Compact Edition, Advanced Edition, Premium Edition

Expert Documentation

Release 7.1 - March 2009

Alcatel·Lucent

Legal notice:

The CE mark indicates that this product conforms to the following Council Directives:
- 89/336/CEE (concerning electro-magnetic compatibility)
- 73/23/CEE (concerning electrical safety)
- 1999/5/CE (R&TTE)

CE

Table of contents

Expert Documentation

Chapter 1
General Presentation

Chapter 2
Hardware : Platform and Interfaces

Chapter 3
User Services

Chapter 4
Voice Mail

Chapter 5
OmniMobility

Chapter 6
VoIP Services

Chapter 7
Private Networks

Chapter 8
General Applications

Chapter 9
Internet Services

Chapter 10
OmniTouch Call Centre Office

Chapter 11
Management Tools

Chapter 12
Maintenance Services

Chapter 13
System Services

Chapter 1

General Presentation

1.1 Overview

1.1.1 CLAUSES

1.2 Main Features

1.2.1 MAIN FEATURES

Alcatel-Lucent OmniPCX Office Communication Server is an "e-communication server", a new "all-in-one" concept combining proven telephony features with data management and access to all the resources of the Internet. This "multi-purpose" server provides a turnkey global communication solution for small and medium-scale businesses with 6 to 200 employees.

For businesses with 6 to 12 employees, the Alcatel-Lucent OmniPCX Office Communication Server range has been expanded to include the Alcatel-Lucent OmniPCX Office Compact Edition

1.2.1.1 Voice:

- Advanced telephony
- Voice mail unit
- Automated Attendant
- Integrated CTI server
- Voice over IP
- Mobility (DECT technology or VoWLAN technology)
- PIMphony (telephony application for PC)
- Multiple Automated Attendant

1.2.1.2 Data:

- LAN switch
- Router and integrated firewall
- DHCP and DNS server
- Information sharing
- Resources sharing

- Remote access server (RAS)

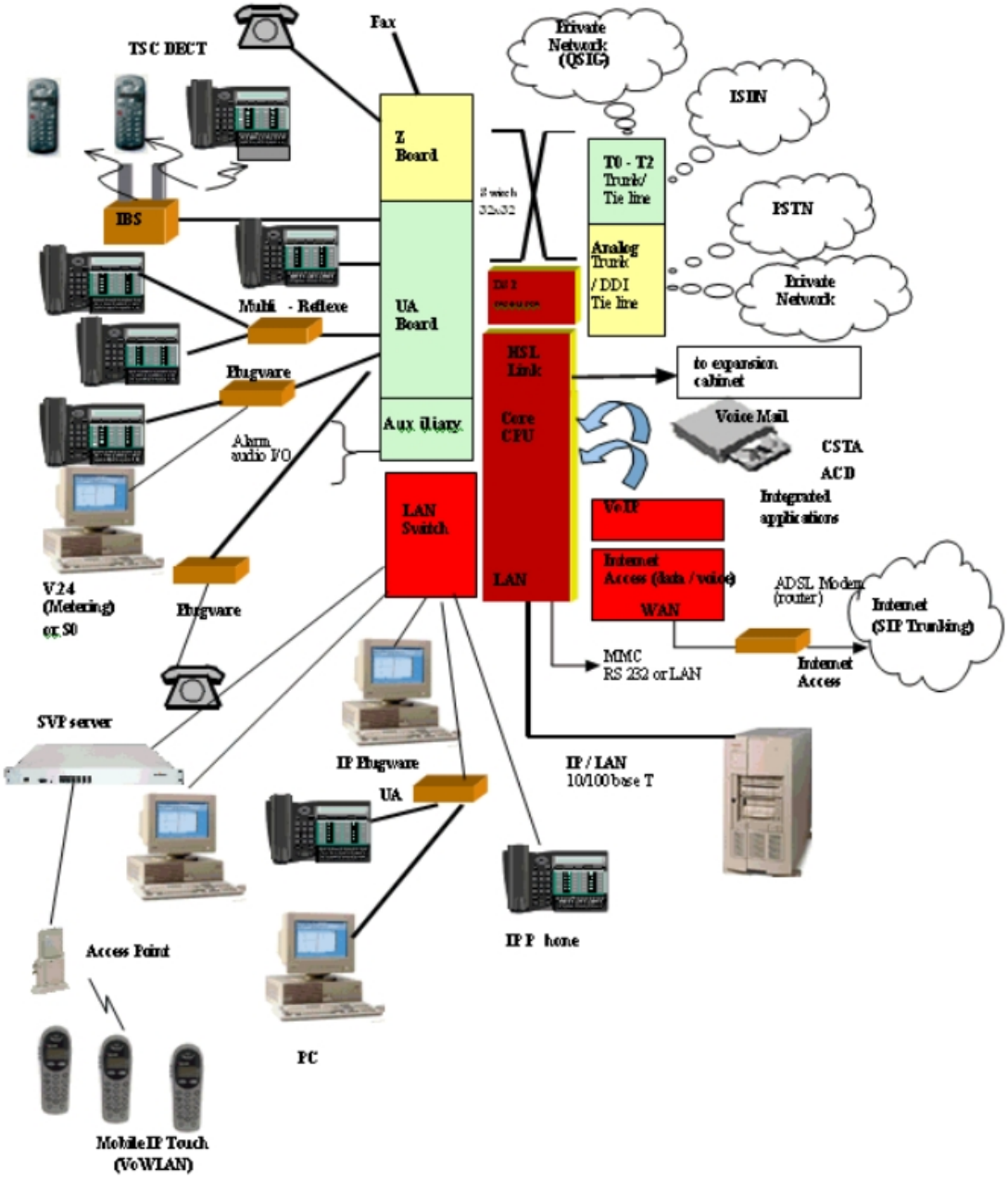
1.2.1.3 Internet:

- Shared access to the Internet (ISDN or xDSL connection)
- Proxy server
- Cache server
- E-mail server

  Note:
  Only for migration from prior releases - For new systems, e-mail server feature requires an Extended Communication Server.

- VPN
- Intranet server

1.2.2 INSTALLATION SUMMARY



1.2.3 HARDWARE DESCRIPTION

In order to cover the entire SME/SMI market segment (6 to 200 users), Alcatel-Lucent OmniPCX Office Communication Server is available in:

- 3 19" rack modules which can be mounted in a rack or placed on a shelf.

- 1 module which is fixed either directly to the wall, or to a wall support (US version).

1.2.3.1 Rack 1 or S or SMALL

- 28 ports
- 1 CPU slot + 2 general-purpose slots (no SLI16 board)
- Power consumption: 1 A (230 V) / 2 A (110 V) - 80 W.
- Dimensions: H = 66 mm (2.6 inches); W = 442 mm (17.4 inches); D = 400 mm (15.76 inches).
- Weight: 6 kg.

1.2.3.2 Rack 2 or M or MEDIUM

- 56 ports
- 1 CPU slot + 5 general-purpose slots
- Power consumption: 1.2 A (230 V) / 2.3 A (110 V) - 120 W.
- Dimensions: H = 110 mm (4.3 inches); W = 442 mm (17.4 inches); D = 400 mm (15.76 inches).
- Weight: 11 kg.

1.2.3.3 Rack 3 or L or LARGE

- 96 ports
- 1 CPU slot + 4 specific general-purpose slots (no UAI16 and MIX boards)
- Power consumption: 1.2 A (230 V) / 2.3 A (110 V) -150 W.
- Dimensions: H = 154 mm (6.1 inches); W = 442 mm (17.4 inches); D = 400 mm (15.76 inches).
- Weight: 13 kg.

Maximum capacity:

The system can be extended by adding one or two modules to the main module. All combinations are possible, with a maximum of 3 modules. The maximum capacity is 236 stations.

1.2.3.4 Alcatel-Lucent OmniPCX Office Compact Edition

- 12 ports.
- 1 CPU slot + 1 MIX slot
- Power consumption: 1.5 A (240 V)
- Dimensions: H = 345 mm; W = 370 mm; D = 65 mm.
- Weight: 5.1 kg.

The following mixed boards are available:

- MIX 244
- MIX 284
- MIX 248
- MIX 448
- MIX 484
- AMIX 444-1
- AMIX 484-1
- AMIX 448-1

Compact Edition 2nd Generation

The Compact Edition 2nd Generation is an evolution of the current CE platform. The Compact Edition 2nd Generation, which is wall-mounted, is special to the Mini-MIX daughter board. This board, which is plugged on a CPU-4 (ASPEN 133 MHZ and 128MB of flash) for call handling, provides 2 Z accesses and 2 T0 accesses.

The Mini-MIX daughter board has been available from Alcatel-Lucent OmniPCX Office Communication Server R5.1 on Compact Edition 2nd Generation providing 100V to CPU slot.

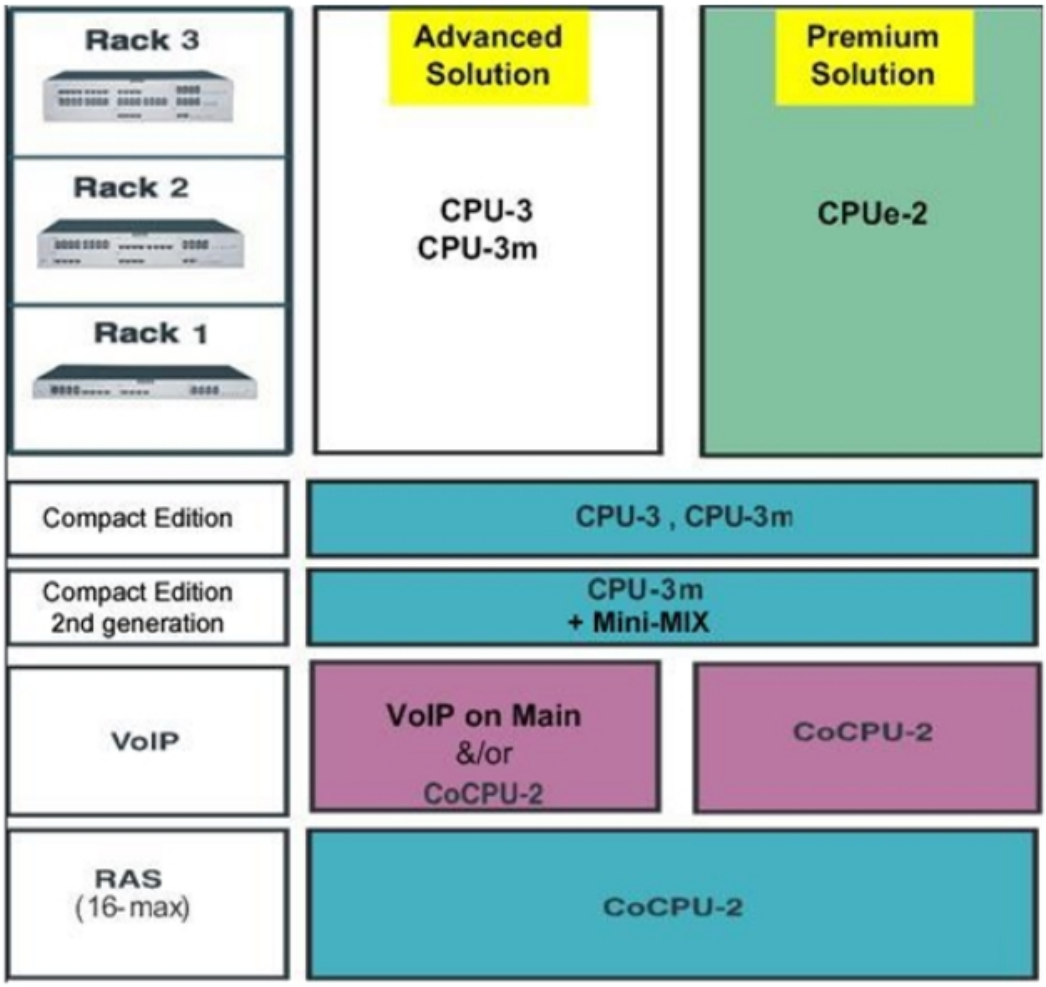
The Mini-MIX led (the previously WAN led) is steady when the Mini-MIX daughter board is detected.

No WAN daughter board can be plugged on a CPU-4 because Internet Access Services are not supported on Aspen CPUs..

1.2.4 PRODUCT LINE-UP

Different solutions exist for each model, depending on the desired level of service: These solutions allow the system to be built up by adding modules, boards, applications and software keys.

1.2.4.1 Applications and CPU boards



1.2.5 BOARDS AND OPTIONS

The following table lists the boards available on Alcatel-Lucent OmniPCX Office Communication Server **Release 7.x** (S, M or L racks).

Board	Function	Optional boards	Connections
APA2 APA4, APA8 APA8	2, 4 or 8 analog trunk line interfaces	GSCLI: Ground Start signalling CLIDSP: CLIP local management	Analog trunk line (TL), TL-PS diversion
ATA2 ATA4	2 or 4 analog trunk line interfaces	MET: pulse meter receivers (phased out)	Analog trunk line (TL), TL-PS diversion
BRA2 BRA4 BRA8	2, 4 or 8 T0 basic accesses		ISDN network ISDN-EFM T0/S0 forwarding box
CPUe	Processing Unit (up to R1.1) - 64MB SDRAM Always equipped with Hard Drive for Release R5.0 and above	HSL1, HSL2: interconnection with add-on modules AFU, AFU-1: (Auxiliary Function Unit) VoIP4-1, VoIP8-1 and VoIP16-1	Lanswitch or Ethernet terminal Please-wait message player Tuner for background music Alarm Doorphone Loudspeaker General call ringer ISDN-EFM T0/S0 forwarding box Pulse metering device OMC
CPU-1 CPU-2	Processing Unit (From R2.0) Processing Unit (From R3.0) 64 MB Flash Memory. Always equipped with Hard Drive for Release R5.0 and above	HSL1, HSL2: interconnection with add-on modules AFU, AFU-1: (Auxiliary Function Unit) VoIP4-1, VoIP8-1 and VoIP 16-1	Lanswitch or Ethernet terminal Please-wait message player Tuner for background music Alarm Doorphone Loudspeaker General call ringer ISDN-EFM T0/S0 forwarding box Pulse metering device OMC
CPU-3	Processing Unit (From R5.0) 128 MB Flash Memory. Always equipped with Hard Drive for R7.0.	HSL1, HSL2: interconnection with add-on modules AFU, AFU-1: (Auxiliary Function Unit) VoIP4-1, VoIP8-1 and VoIP16-1* XMEM128-1 memory extension Xmem_IDE interface for Hard Disk	Lanswitch or Ethernet terminal Please-wait message player Tuner for background music Alarm Doorphone Loudspeaker General call ringer ISDN-EFM T0/S0 forwarding box Pulse metering device OMC

Board	Function	Optional boards	Connections
CPU-3m	From R5.1: Processing Unit 128 MB Flash Memory Always equipped with Hard Drive for R7.0.	Optional Xmem128-1 memory extension Optional VOIP-1 or VOIP-2 Optional Mini-MIX (Exclusive with HSL and SLANX4 daughter boards) Optional AFU–1 Optional HSLx Optional SLanX4	Lanswitch or Ethernet terminal Please-wait message player Tuner for background music Alarm Doorphone Loudspeaker General call ringer ISDN-EFM T0/S0 forwarding box Pulse metering device OMC
CPU-4	From R7.0: Processing Unit 128 MB Flash Memory Optional Hard Drive	Optional Xmem128-1 memory extension Optional VOIP-1 or VOIP-2 Optional Mini-MIX (Exclusive with HSL and SLANX4 daughter boards) Optional AFU–1 Optional HSLx Optional SLanX4	Lanswitch or Ethernet terminal Please-wait message player Tuner for background music Alarm Doorphone Loudspeaker General call ringer ISDN-EFM T0/S0 forwarding box Pulse metering device OMC
CPUe-1 CPUe-2	Processing Unit (From R2.0) Processing Unit (From R3.1) Always equipped with Hard Drive	HSL1, HSL2: interconnection with add-on modules AFU, AFU-1: (Auxiliary Function Unit) WAN: additional Ethernet link	Lanswitch or Ethernet terminal Please-wait message player Tuner for background music Alarm Doorphone Loudspeaker, General call ringer ISDN-EFM T0/S0 forwarding box Pulse metering device OMC
CoCPU CoCPU-1 CoCPU-2	CoProcessing Unit (Up to R1.1) CoProcessing Unit (From R2.0) CoProcessing Unit (From R3.1)	VoIP: (Voice over IP): SLANX4: mini switch (CPU/CPUs - CoCPU link)	Lanswitch or Ethernet terminal
DDI2 DDI4	2 or 4 analog trunk line interfaces with Multiple Subscriber Numbers (MSN)		Analog trunk line with Multiple Subscriber Numbers (MSN)
LanX8 LanX16 LANX16-1 LanX8-2 LANX16-2	8 or 16 port Ethernet 10/100 BT (of which 1 or 2 10/100/1000 BT ports on LANX-2 boards)		@ Phones, Hub, Lanswitch, PC, etc.

Board	Function	Optional boards	Connections
MEX (equipped with an HSL1 board)	Extension module controller		
MIX244 MIX248 MIX284 MIX484 MIX448 MIX044 MIX084 MIX048	0, 2 or 4 T0 basic accesses + 4 or 8 UA interfaces + 4 or 8 Z interfaces		ISDN network, analog Z terminals and Alcatel Reflexes stations or Alcatel-Lucent 9 seriess-sets
AMIX484-1 AMIX448–1 AMIX444–1	4 analog line accesses, 4 or 8 UA interfaces and 4 or 8 Z interfaces	GSCLI: Ground Start signalling CLIDSP: local CLIP management METCLI	PSTN network, analog Z terminals and Alcatel Reflexes stations or Alcatel-Lucent 9 series-sets
PRA-T2 PRA-T1 DASS2 DLT2 T1-CAS T1-CSS PCM R2	PRA -T2, DASS2, DLT2: 30 x 64-Kbps B-channels + 1 x 64-Kbps D-channel; 2048 Kbps. PRA-T1: 23 x 64-Kbps B-channels + 1 x 64-Kbps D-channel; 1544 Kbps. 23 x 64-Kbps B-channels + 1 x 64-Kbps D-channel T1-CAS: 24 x B-channels, including signalling; 1544 Kbps. PCM R2: 30 x 64-Kbps B-channels +1 x 4-Kbps signalling channel; 2048 Kbps.		PRA-T2: ISDN network DASS2: UK public/private network DLT2: Private QSIG network PRA-T1: Hong-Kong ISDN network ISDN (US) T1-CAS: USA public network PCM R2: Public network
SLI4 SLI8 SLI16 SLI4-1 SLI8-1 SLI16-1	4, 8 or 16 Z interfaces		Analog Z terminals
UAI4 UAI8 UAI16 UAI16-1	4, 8 or 16 UA interfaces UAI16-1 board: possibility of powering terminals connected to the 16 interfaces remotely from an external EPS48 power supply		Alcatel Reflexes stations or Alcatel-Lucent 9 series-sets Multi Reflexes 4070 IO/EO DECT base stations EPS48 only on interface 1 of the UAI16-1 board

Remark:

the CPU and MIX boards have the same characteristics as those used by Alcatel-Lucent OmniPCX Office Communication Server.

Note:

***As of Release 6.0, all 16 DSP channels of VoIP16 are taken into account on main CPU.*

1.2.6 SUBSETS COMPATIBILITY

For detailed information, refer to the Technical Communication on this issue.

1.3 Capacity and Limits

1.3.1 CAPACITIES AND LIMITS

The following table gives the capacities provided by the various Alcatel-Lucent OmniPCX Office Communication Server solutions.

	S / e-S	**M / e-M**	**L / e-L**	**XL / e-XL**	**Max. limits**	**CE**	**Compact Edition 2nd Generation**
System							
Type of module	Rack 1	Rack 2	Rack 3	Rack 3 + extension Rack 3	Up to 3 modules	Wall mounted	Wall mounted
Total number of slots (with CPU and MEX boards)	3	6	9	18	27	2	2
Available slots	2	5	8	16	24	1	1
Total number of main CPU boards	1						
Total number of UAI16-1 boards	1	3	4	8	12	1	1
Total number of SLI16 boards	0	2	5	10	12	0	0
Total number of UAI16-1 + MIX boards	2	5	4	8	12	1 (mixed)	1 (mixed)
Total number of CoCPU-1. CoCPU-2 CoProcessing boards	1	2	2	5	6	0	0
VOIP daughter boards	2	3	3	6	6	1	1
XMEM-128 daughter board	1 (plugged into a Aspen CPU)						
Mini-MIX daughter board							1
Hard disk	1					1 (with UPS)	1 (with UPS)

	S / e-S	M / e-M	L / e-L	XL / e-XL	Max. limits	CE	Compact Edition 2nd Generation
Hard disk capacity	20 Gigabytes minimum					20 GB minimum (with battery supplied external power)	20 GB minimum (with battery supplied external power)
Communication ports							
Digital ports	24	56	96	192	200	16	16
Z ports	16	32	80	160	196	8	10
Voice ports (digital + Z)	28	56	96	192	200	12	14
Multi Reflexes 4099 Hubs	6	6	6	12	18	4	4
LAN-Switch boards (LANX-1 and LANX-2)	2	4	8	12	12	1 LANX16	1 LANX16
Available LAN switch Ethernet ports	28	56	112	168	168	1	1
Analog NDDI trunks	8	16	32	64	72	4	4
Analog DDI trunks	0	16	32	64	72	0	0
Primary T1 + T2 + DLT2 access	1	3	3	6	9	1	1
Basic T0 + DLTO access	8	10				8	8
ISDN access (T0 + T2 + T1 + DLTO + DLT2)	10					8	8
T1 CAS access (US only)	1	3	3	5	5	1	1
PCM R2 boards	1	1	1	2	3	0	0
IP trunks	24	40	40	88	96	8	8
Total trunk lines and B channels (LR, SDA, T1. T2. T0. IP)	34	90	120	120	120	16	16
Terminals + Work stations							
Directory numbers (*)	250						
Digital terminals (***) + simple terminals (Z)	28	56	96	192	236	20	20
Digital terminals (***)	24	56	96	192	236	16	16

	S / e-S	**M / e-M**	**L / e-L**	**XL / e-XL**	**Max. limits**	**CE**	**Compact Edition 2nd Generation**
Analog terminals (Z)	16	32	80	160	196	8	8
Mobile terminals (**)	120						
IP subscribers (Alcatel-Lucent 8 series + PIMphony IP)	55	120		200		55	55
Virtual terminals	200						
IP PIMphony media Advanced	55						
IP PIMphony media Premium		120		200			
H.323 PC client	55	120		150		55	55
PIMphony clients with integrated CTI server	75 Alcatel-Lucent OmniPCX Office Advanced Edition CS solutions 200 Alcatel-Lucent OmniPCX Office Premium Edition CS solutions					75	75
TAPI 2.0 server-session	75 Alcatel-Lucent OmniPCX Office Advanced Edition CS solutions 200 Alcatel-Lucent OmniPCX Office Premium Edition CS solutions					75	75
TAPI 2.0 server-monitoring	75 Alcatel-Lucent OmniPCX Office Advanced Edition CS solutions 400 Alcatel-Lucent OmniPCX Office Premium Edition CS solutions					150	150
PIMphony Unified	75						
TAPI 2.1 server-session	25						
TAPI 2.1 server-monitoring	236						
CSTA server-session	25						
CSTA server-monitoring	236						
Digital terminal options							
Add-on modules (max. 3/port)	10	40	60	120	136	8	8
S0. Z and V24 interfaces	12	24	42	48	48	4	4
V24 metering interface	1						
DECT bases (full wireless configurations)							

	S / e-S	M / e-M	L / e-L	XL / e-XL	Max. limits	CE	Compact Edition 2nd Generation
Remotely supplied, splitterless DECT bases	4	4	4	8	12	3	3
Remotely supplied DECT bases with splitter	16	48	60	60	60	16	16
Remotely supplied DECT bases with and without splitter	20	52	60	60	60	16	16
Remotely supplied DECT bases (remotely supplied + local supply)	23	55	60	60	60	NA	NA
Call server							
Voice mail ports	8					8	8
Voice mail storage capacity	60 minutes (basic) 4 hours (with XMEM-128) 200 hours (with Hard Disk)						
Simultaneous call recordings (only with hard disk)	3						
Preannouncement	from 4 to 8						
Languages	from 2 to 4						
Directory entries	5000 (including collective speed dial numbers)						
Collective speed dial numbers	2200						
System on-hold music	16 seconds						
Customizable on-hold music	up to 2 minutes without hard disk up to 10 minutes with hard disk						
Multiple EDN per S0	98						
Entries in ARS table	3000						
Account codes	250						
Metering tickets	up to 1000 tickets						
NMC tickets with hard disk	up to 30.000 records						
Groups (hunting + broadcasts + pick-ups)	50 with maximum of 32 users per group						
Attendant groups	8 with maximum of 8 operator stations per group						
Conference	3 simultaneously						

	S / e-S	M / e-M	L / e-L	XL / e-XL	Max. limits	CE	Compact Edition 2nd Generation
Meet Me Conference	6 party conference, limit = 1						
Call Centre							
Agents declared	32						
Agents active	10 without hard disk 32 with hard disk						
Groups of agents	8						
Assistant agent	10 (Alcatel-Lucent OmniPCX Office Advanced Edition CS solution) 32 (Alcatel-Lucent OmniPCX Office Premium Edition CS solution)						
Supervisor	1 (Alcatel-Lucent OmniPCX Office Advanced Edition CS solution) 4 (Alcatel-Lucent OmniPCX Office Premium Edition CS solution)						
e-server							
Shared Internet access	128 kbps/s (2 B channels (ISDN) 10 Mbps/s (ADSL modem or external router					NA	NA
WCA users	25					NA	NA
WCA nomadic users	25					NA	NA
Internet users	200					NA	NA
Simultaneous Internet accesses	Depends on available bandwidth (e.g.: up to 20 over a 128 Kbps/s link)					NA	NA
Web page cache capacity	1.5 GB					NA	NA
E-mailboxes	200					NA	NA
E-mail storage capacity	10 GB					NA	NA
Intranet web server capacity	200 MB					NA	NA
File server	4 GB					NA	NA
Simultaneous PPTP teleworkers	50					NA	NA
LAN to LAN networking	50					NA	NA
ISDN RAS							
RAS on Main CPU	2 x 64 kbps/s with HD						
RAS with CoCPU-1 /CoCPU-2	16 x 64 kbps/s					NA	NA

(*): Subscriber numbers include all terminals and virtual users, 13 auxiliary ports (VMU, Internet access, Remote access), main operator terminal number.

(**): Make sure that radio base dimensioning is adapted to mobile sets number.

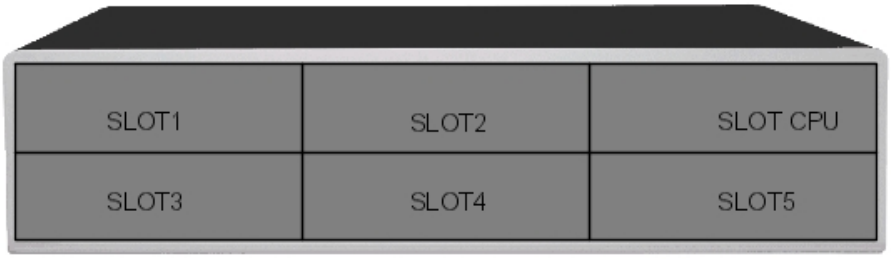
(***): Numbers indicated include digital terminals connected to Multi Reflexes 4099 Hubs.

1.3.1.1 BOARDS IMPLEMENTATION

1.3.1.1.1 Rack 1

BOARDS	SLOTS 1-2	CPU SLOT
CPU-1. CPUe-1. CPU-2. CPUe-2. CPU-3. CPU-3m, CPU-4	No	Mandatory
MIX x/y/z	Yes	No
AMIX-1 x/y/z	Yes	No
UAI4. UAI8. UAI16. UAI16-1	Yes	No
SLI4. SLI8. SLI4-1. SLI8-1	Yes	No
SLI16. SLI16-1	No	No
PRA-T2. PRA-T1. DASS2. DLT2. T1-CAS, PCM R2	Yes	No
APA4. APA8	Yes	No
DDI2. DD14	No	No
BRA2. BRA4. BRA8	Yes	No
CoCPU-1. CoCPU-2	Yes	No
LANX8. LANX16. LANX16-1. LANX8-2. LANX16-2	Yes	No

1.3.1.1.2 Rack 2

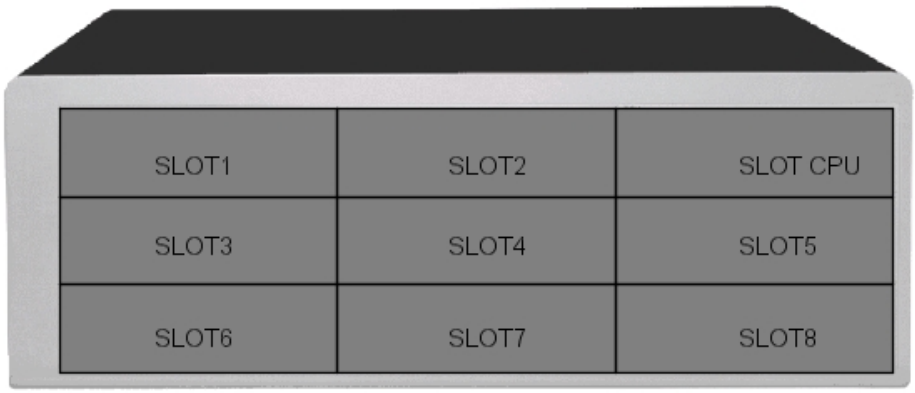


BOARDS	SLOTS 1-2-3-4-5	CPU SLOT
CPU-1. CPUe-1. CPU-2. CPUe-2. CPU-3. CPU-3m, CPU-4	No	Mandatory
MIX x/y/z	Yes	No

BOARDS	SLOTS 1-2-3-4-5	CPU SLOT
AMIX-1 x/y/z	Yes	No
UAI4. UAI8. UAI16. UAI16-1	Yes	No
SLI4. SLI8. SLI16. SLI4-1. SLI8-1. SLI16-1	Yes	No
PRA-T2. PRA-T1. DASS2. DLT2. T1-CAS, PCM R2	Yes	No
APA4. APA8	Yes	No
DDI2. DD14	Yes	No
BRA2. BRA4. BRA8	Yes	No
CoCPU-1. CoCPU-2 (Slots 2. 4. 5 only)	Yes	No
LANX8. LANX16. LANX16-1. LANX8-2. LANX16-2	Yes	No

1.3.1.1.3 Rack 3

Caution:
The VoIP4-1. VoIP8-1 and VoIP16-1 boards implemented on a CPU board consume a hardware resource used for slot 8 of the module. In this case, it is impossible to add a board other than a LANXxx board in slot 8.



BOARDS	SLOT 1	SLOTS 2-3-4	SLOTS 5-6-7-8	CPU SLOT
CPU-1. CPUe-1. CPU-2. CPUe-2. CPU-3. CPU-3m, CPU-4	No	No	No	Mandatory
MIX x/y/z	Yes	Yes	No	No
AMIX-1 x/y/z	Yes	Yes	No	No
UAI4. UAI8	Yes	Yes	Yes	No

BOARDS	SLOT 1	SLOTS 2-3-4	SLOTS 5-6-7-8	CPU SLOT
UAI16. UAI16-1	Yes	Yes	No	No
SLI4. SLI8. SLI16. SLI4-1. SLI8-1. SLI16-1	Yes	Yes	Yes	No
PRA-T2. PRA-T1. DASS2. DLT2. T1-CAS, PCM R2	Yes	Yes	Yes	No
APA4	Yes	Yes	Yes	No
APA8	Yes	No	Yes	No
DDI2. DD14	Yes	Yes	Yes	No
BRA2. BRA4. BRA8	Yes	Yes	Yes	No
CoCPU-1. CoCPU-2	No	Yes	Yes	No
LANX8. LANX16. LANX16-1. LANX8-2. LANX16-2	Yes	Yes	Yes	No

1.3.1.2 Alcatel-Lucent OmniPCX Office Compact Edition

BOARDS	PER SLOT	CPU SLOT
CPU-2. CPU-3. CPU-3m, CPU-4	No	Mandatory
MIX x/y/z	Yes	No
AMIX-1 x/y/z	Yes	No
Mini-MIX (available only for Compact Edition 2nd Generation with CPU-3m or CPU-4)	Yes	No

1.3.2 POWER SUPPLY LIMITS

The following tables give the detailed power consumption of the different items (boards and terminals) and the limit not to be exceeded for each model (all values are expressed in W).

The maximum budget at the charger level is also indicated for each model and you just have to add the values for all items present in the system. The configuration will be within the power

supply limits if the total obtained is less than or equal to the maximum budget allowed for the type of rack used:

Maximum budget (Alcatel-Lucent OmniPCX Office Advanced Edition CS)

- Alcatel-Lucent OmniPCX Office Compact Edition = 30 W
- Rack 1 = 34.33 W
- Rack 2 = 52.81 W
- Rack 3 = 79.62 W

Maximum budget (Alcatel-Lucent OmniPCX Office Premium Edition CS)

- Rack 1 = 46.28 W
- Rack 2 = 67 W
- Rack 3 = 92 W

BOARDS AND TERMINALS	**RACK 3**	**RACK 2**	**RACK 1 / Alcatel-Lucent OmniPCX Office Compact Edition**
CPU boards			
CPU/CoCPU	6.39	5.16	5.14
CPUe/CoCPU@	7.09	5.73	5.71
(Co)CPU-1-2	7.09	5.73	5.71
CPU-3. CPU-3m, CPU-4			5.71 (only with Compact Edition 2nd Generation)
CPUe-1. CPUe-2	15.95	16.86	17.03
MEX	1.60	1.32	1.30
Daughter boards			
Mini-MIX	Forbidden	Forbidden	0.8 (only with Compact Edition 2nd Generation)
XMEM/XMEM-1/XMEM-128	0.13	0.10	0.10
VOIP 16-1	2.17	1.74	1.74
VOIP 8-1	1.26	1.01	1.01
VOIP 4-1	0.81	0.65	0.65
HSL	0.38	0.30	0.30
WAN/Integrated T1	0.91	0.73	0.73
2.5" Hard disk	2.61	2.33	2.17
S-LANX4	2.01	1.62	1.62
AFU/AFU-1	0.64	0.55	0.61
Trunk boards			
BRA 8	1.09	0.97	0.90
BRA 4	0.64	0.56	0.53

BOARDS AND TERMINALS	RACK 3	RACK 2	RACK 1 / Alcatel-Lucent OmniPCX Office Compact Edition
BRA 2	0.38	0.33	0.31
PRA T2/T1 - DASS2 - DLT2 - T1-CAS - PCM R2	0.41	0.33	0.33
ATA 4	1.42	1.42	1.13
ATA 2	0.78	0.78	0.62
Metering	0.07	0.06	0.06
APA 8	2.27	2.19	1.82
APA 4	1.41	1.34	1.14
METCLI (4 interfaces)	0.46	0.43	0.38
GSCLI (4 interfaces)	0.11	0.10	0.09
CLIDSP	0.51	0.41	0.41
DDI 4	9.31	10.25	FORBIDDEN
DDI 2	4.65	5.12	FORBIDDEN
Datacom boards			
LANX 8/LANX 8-2	4.53	3.64	3.64
LANX 16	8.56	6.88	6.88
LANX 16-1/LANX 16-2	8.12	9.38	9.61
Mixed boards			
4T0/8UA/4Z	3.00	2.9	2.76
4T0/4UA/8Z	3.45	3.45	3.29
2T0/4UA/4Z	2.16	2.13	2.03
2T0/8UA/4Z	2.74	2.65	2.52
2T0/4UA/8Z	3.2	3.2	3.05
8UA/4Z	2.48	2.39	2.33
4UA/8Z	3.01	2.96	2.92
4UA/4Z	1.91	1.86	1.82
4AT/8UA/4Z	2.45	2.52	2.62
4AT/4UA/8Z	3.35	3.48	3.57
4AT/4UA/4Z	2.43	2.49	2.56
Extension boards			
UAI 16	2.39	2.21	2.10
UAI 16-1	1.66	1.73	1.77
UAI 8	1.38	1.32	1.27
UAI 4	0.88	0.87	0.85
SLI 16/SLI 16-1	4.76	5.00	FORBIDDEN
SLI 8/SLI 8-1	2.39	2.51	2.39

BOARDS AND TERMINALS	RACK 3	RACK 2	RACK 1 / Alcatel-Lucent OmniPCX Office Compact Edition
SLI 4/SLI 4-1	1.21	1.26	1.20
Terminals			
Alcatel-Lucent 9 series/Reflexes (UA) station	0.39	0.45	0.46
Add-on module	0.21	0.24	0.25
Multi Reflexes 4099	0.52	0.61	0.62
CTI/AP option	0.79	0.92	0.94
V24 option	0.79	0.92	0.94
S0 option	1.07	1.23	1.26
4070 (IBS) remotely supplied from the PCX	2.52	2.90	2.98
Analog terminal	0.19	0.21	0.22

Note:

When using an option with CTI, the consumption value must be added; example for a rack 3:

- 4093 (V24+CTI) = 0 + 0.79 = 0.79 W
- 4094 (S0 + CTI) = 1.07 + 0.79 = 1.86 W

When using an SLI extension board or an MIX board, the number of analog sets that can be connected must be added even if they are not connected; e.g. for a rack 3:

- SLI16 = 4.64 +(16 x 0.21) = 8 W
- MIX484 = 2.99 + (4 x 0.21) = 3.83 W

When using a UAI16-1 extension board, a "power splitter" option can be added to port 1 (in parallel with the UA set) that makes it possible to feed all the subscribers and base stations connected to this same board. They will then be deducted from the power budget; e.g. for a rack 3:

- either a UAI16-1 with 10 UA sets and 3 IBS without the "power splitter" option = 13.12 W, or 1.66 + (10 x 0.39) + (3 x 2.52) = 13.12 W
- either a UAI16-1 with 10 UA sets and 3 IBS without the "power splitter" option = 1 W, or -1 + (10 x 0.39) + (3 x 2.52) = 13.12 W

The consumption budget for Alcatel-Lucent OmniPCX Office Premium Edition CS solutions can only be used if CPUe-1/CPUe-2 boards are used. 2nd generation Racks offer a higher performance power supply with a higher consumption budget per Rack. However, the CPU, CPUe, CPU-1. CPU-2. CPU-3. CPU-3m and CPU-4 boards cannot detect these different 1G and 2G Racks and therefore cannot include them when calculating power consumption.

The consumption budget can be read via the labelled addresses below:

- PowBudMain for the main cabinet value
- PowBudMex1 for the value of add-on module 1
- PowBudMex2 for the value of add-on module 2

Note that the IBS value = 0W (local power) in the labelled addresses. This is because the system cannot detect whether the IBSs are powered locally or self-powered. To avoid being

restricted by power limits in a case where the IBS would use a local power supply it doesn't count them.

1.4 Compliance with Standards

1.4.1 COMPLIANCE WITH STANDARDS

1.4.1.1 SAFETY DECLARATION

Compliance with IEC 60950-1 1st Edition standards

Interface classification	Interface location
TNV-3	- Z interface (SLI board) - Z interface for digital station (AP board) - Analog trunk line interface (ATA board)
SELV	- Digital station interface (UAI board or Multi Reflexes 4099 option) - 4070 IO/EO base station interface (UAI board) - T0/DLT0 interface (BRA board) - T2/T1 interface (PRA board) - S0 interface (S0 board) - Please-wait or background music interface (CPU/CPUe board) - Alarm interface (CPU/CPUe board) - General bell interface (CPU/CPUe board) - Door phone interface (CPU/CPUe board) - Loudspeaker interface (CPU/CPUe board) - V24 interface (CPU/CPUe board) - CTI interface for digital station (CTI or V24/CTI board) - 10/100 base T Ethernet interface (CPU/CPUe or CoCPU/CoCPU@ board) - 4070 IO/EO base station (inputs-outputs) - 4097 CBL UA/DECT adapter

SELV: Safety Extra Low Voltage

TNV-3: Telecommunication Network Voltage

To maintain safety levels, it is essential to connect circuits of the same type and to ensure that all means of connection comply with the constraints indicated for each circuit type.

1.4.1.2 ESSENTIAL REQUIREMENTS

This product complies with the core requirements of European Community R&TTE Directive 1999/5/EC.

Electromagnetic compatibility:

- EN55022 Ed.1998 + A1: 2000 + A2: 2003 class B: Limits and methods of measuring the characteristics of radioelectric disturbances produced by information technology equipment.
- EN55024 Ed.1998 + A1: 2001 + A2: 2003: Information technology equipment: immunity characteristics.
- EN61000-3-2 Ed.2000 + A2: 2005: Electromagnetic compatibility: harmonic current emission limits.

- EN61000-3-3 Ed.1995 + A1: 2001: Electromagnetic compatibility: voltage fluctuation and flicker limits in low voltage networks.

Safety:

- IEC 60950-1 1st Edition: Safety of information technology equipment.

1.5 Environment Compatibility

1.5.1 EQUIPMENT COMPATIBILITY

On the new generation Alcatel-Lucent OmniPCX Office Communication Server, it is possible to re use some equipment and terminals from the Alcatel-Lucent OmniPCX Office Communication Server range.

1.5.1.1 TERMINAL COMPATIBILITY ON THE Alcatel-Lucent OmniPCX Office Communication Server

1.5.1.1.1 Compatible Digital Sets

- The complete Alcatel-Lucent 9 series range: Alcatel-Lucent 4019 Digital Phone, Alcatel-Lucent 4029 Digital Phone, Alcatel-Lucent 4039 Digital Phone.
- The complete line 3G: 4035 (Advanced), 4020 (Premium), 4010 (Easy), and 4004 (First), 4097 CBL.
- All sub-devices behind Alcatel Reflexes: 4083 ASM, 4084 IS, 4084 ISW, 4085 AB, 4091, 4093 ASY, 4094 ISW, 4095 AP.
- **From release 5 onwards, sub-devices CTI 4091 support only the UA protocol. SPI for TAPI interface is not implemented anymore**.
- Four different sub-devices are available (R500) for the line Alcatel-Lucent 9 series (Alcatel-Lucent 4019 Digital Phone, Alcatel-Lucent 4029 Digital Phone, Alcatel-Lucent 4039 Digital Phone):
  - AP Interface Module for connecting analog terminals, faxes and modems,
  - S0 Interface Module for connecting ISDN terminals through the UA link,
  - V24/CTI Interface Module: see module V24/CTI Interface Module - Hardware description .

- Multi Reflexes 4099 for using up to 3 digital sets through one digital link.

These sub-devices are compatible with the current range of terminals.
Because new hardware and software have been designed, AP Interface Module, S0 Interface Module and V24/CTI Interface Module can manage messages with more than 24 bytes (which is the limit in the existing sub-devices).
Hardware and software associated with Multi Reflexes 4099 have not changed but a mechanical box has been included in this sub-device.

1.5.1.1.2 Compatible IP Terminals

- Line Alcatel-Lucent 8 series: Alcatel-Lucent IP Touch 4008 Phone, Alcatel-Lucent IP Touch 4018 Phone, Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone, Alcatel-Lucent IP Touch 4068 Phone.
- Line Alcatel-Lucent IP Touch 8 series phone Extended Edition: Alcatel-Lucent IP Touch 4008 phone Extended Edition, Alcatel-Lucent IP Touch 4018 phone Extended Edition, Alcatel-Lucent IP Touch 4028 phone Extended Edition, Alcatel-Lucent IP Touch 4038 phone Extended Edition, Alcatel-Lucent IP Touch 4068 phone Extended Edition

1.5.1.1.3 Compatible Mobile Terminals

- Terminals DECT 2G: 4073 GS, 4074 GB, GBEx, GH, GI and SGAP.
- Terminals DECT Mobile 100 and 200.
- DECT Reflexes terminals with 4097 CBL.
- Alcatel-Lucent 300 DECT Handset and Alcatel-Lucent 400 DECT Handset handsets.
- Intelligent base station 4070 IO/EO (IBS) and gain antennas.
- Alcatel-Lucent Mobile IP Touch 300 and Alcatel-Lucent Mobile IP Touch 600
- Alcatel-Lucent IP Touch 310 WLAN Handset and Alcatel-Lucent IP Touch 610 WLAN Handset

1.5.1.2 INCOMPATIBLE HARDWARE PARTS ON Alcatel-Lucent OmniPCX Office Communication Server

- The complete range of Alcatel Reflexes 1G (first generation).
- Mobile DECT sets 4075, 4074 B, 4074 Bex, 4074 H.
- Base station DECT RBS 4070 IA and 4070 EA.
- The complete range 160 sets.
- The complete range 4120 (900B) sets.
- Voice mail of Alcatel OmniTouch Call Center Office in release 1.0.
- Fast IP Reflexes and e-Reflexes sets

Chapter 2

Hardware : Platform and Interfaces

2.1 CompactEdition and S, M, L Racks

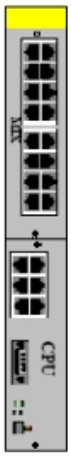
2.1.1 Hardware description

2.1.1.1 Alcatel-Lucent OmniPCX Office Compact Edition AND RACK S/M/L MODULES

2.1.1.1.1 Alcatel-Lucent OmniPCX Office Compact Edition

Alcatel-Lucent OmniPCX Office Compact Edition is a wall-mounted version. It provides 2 slots (1xCPU slot+1xMIX slot).

The Alcatel-Lucent OmniPCX Office Compact Edition rack is not expandable and cannot be used as satellite.



2.1.1.1.2 Compact Edition 2nd Generation

The Compact Edition 2nd Generation, available since R5.1, is an evolution of the current CE.

It is distinguished by the **Mini-MIX** daughter board which is plugged into the **CPU-3m** or CPU-4 board and provides two additional Z (Analog Extension)ports and two additional TO (ISDN Basic Rate) accesses.

2.1.1.1.3 RACK S (SMALL)

The RACK S module (formerly known as RACK 1) mainly consists of a plastic frame.

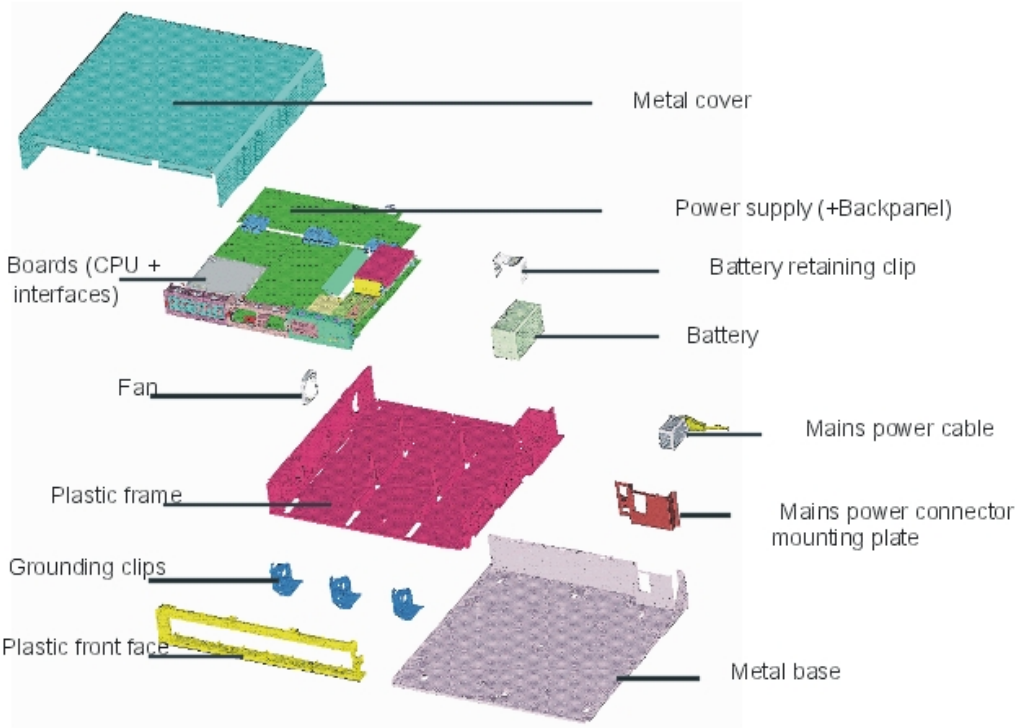
The plastic frame receives all the parts for attaching the power supply board, the fans, the battery and the mains power connector, and everything needed to facilitate the routing of the

cables.

There is no backplane board: the metric connectors are on the power supply module.

The enclosure consists of 3 parts: metal cover and base, plastic front face.

Access to the fans, the power supply module and the battery is gained by disconnecting the mains cable and removing the top metal cover (it is vital to remove all the boards before opening the cover).

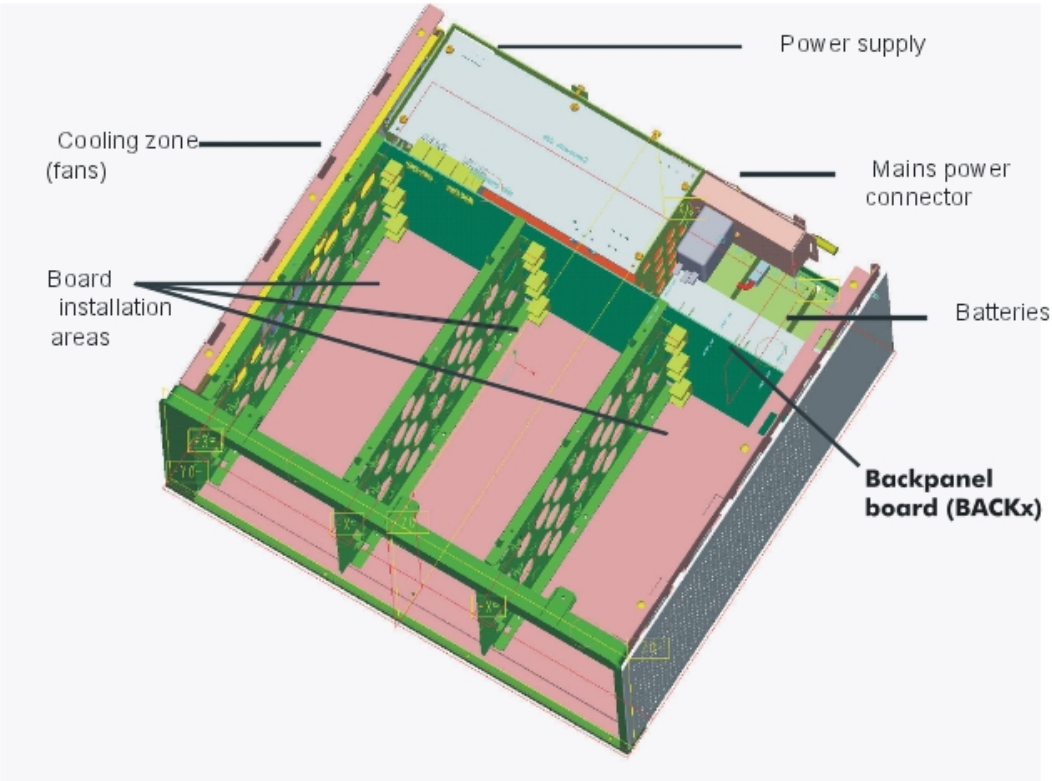


2.1.1.1.4 RACK M (MEDIUM) AND RACK L (LARGE)

The frame consists of a "U"-shaped sheath closed on the top by a riveted plate. The boards are guided by 2 rails for RACK M (formerly known as RACK 2), or 3 rails for RACK L (formerly known as RACK 3), riveted vertically to the frame.

The enclosure consists of a metal top part, two metal side parts and a plastic front face.

Access to the fans, the power supply module and the batteries is gained by disconnecting the power cable and unscrewing the backplane.



2.2 Boards

2.2.1 CPU-1/CPU-2/CPU-3/CPU-3m/CPU-4

2.2.1.1 Hardware description

2.2.1.1.1 CPU Overview

The CPU-1 board is based on the new tracking of the ASPEN CPU board and has the following characteristics: 133 MHz processor, 32 MB NAND Flash, 64 MB SDRAM, DSP 5410.

The CPU-2 board has the same main characteristics as the CPU-1 board, except that the 32 MB NAND Flash memory is replaced by a 64 MB NAND Flash memory.

The CPU-3 board has the following characteristics: 133 MHz processor, 128 MB NAND Flash, 64 MB SDRAM.

The CPU-3m board is fitted with a 133 MHz processor, a 128 MB NAND Flash memory and 64 MB of SDRAM.

The CPU-4 board is fitted with a 133 MHz processor, a 128 MB NAND Flash memory and 128 MB of SDRAM.

2.2.1.1.2 Daughter Boards

The CPU-1/CPU-2/CPU-3/CPU-3m/CPU-4 boards can be equipped with the following daughter boards:

- **HSL** (High Speed Link): module interconnections. This daughter board is not compatible with the Mini-Mix daughter board.
- **XMEM, XMEM-1, XMEM128-1** (eXpansion MEMory): memory extension. This daughter board is not compatible with the VoIP daughter board.
  This daughter board includes a 2.5" hard drive connector:
  - Use a flat cable to connect a PATA hard disk
  - Use a P2SATA-AXV daughter board to connect a SATA hard disk
- **AFU, AFU-1** (Auxiliary Function Unit): supporting auxiliary functions such as general bell, doorphone, audio In, audio Out, etc. The AFU-1 board is required for the connection of the ISDN-EFM box (T0/S0 forwarding)
- **VoIP, VoIP-1** (Voice over IP): Gateway H.323 with integrated Gatekeeper function or SIP Gateway. Supports management of CODECs and DSPs for IP telephony and IP Trunk (IP trunk lines) applications

  Caution:
  The VoIP-X boards implemented on a CPU board consume a hardware resource used for slot 8 of the module. In this case, it is impossible to add a board other than a LANXxx board in slot 8.
  This daughter board includes a 2.5" hard drive connector:
  - Use a flat cable to connect a PATA hard disk
  - Use a P2SATA-AXV daughter board to connect a SATA hard disk to a VoIP daughter board
  - Use a P2SATA-AV1 daughter board to connect a SATA hard disk to a VoIP-1 daughter board
- **Mini-MIX** (only for Compact Edition): this daughter board provides two Z (analog) ports and two T0 accesses. This daughter board is available on CPU-3m and CPU-4 only. This daughter board is not compatible with an HSL board.

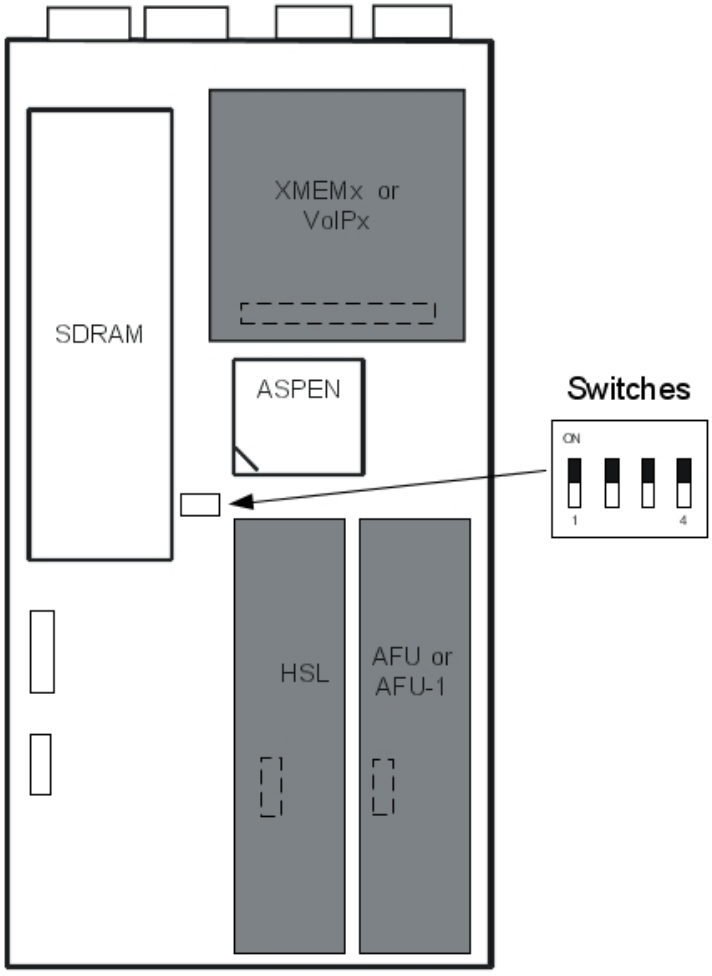


Figure 2.4 : Daughter Board Position on CPU-1, CPU-2 or CPU-3

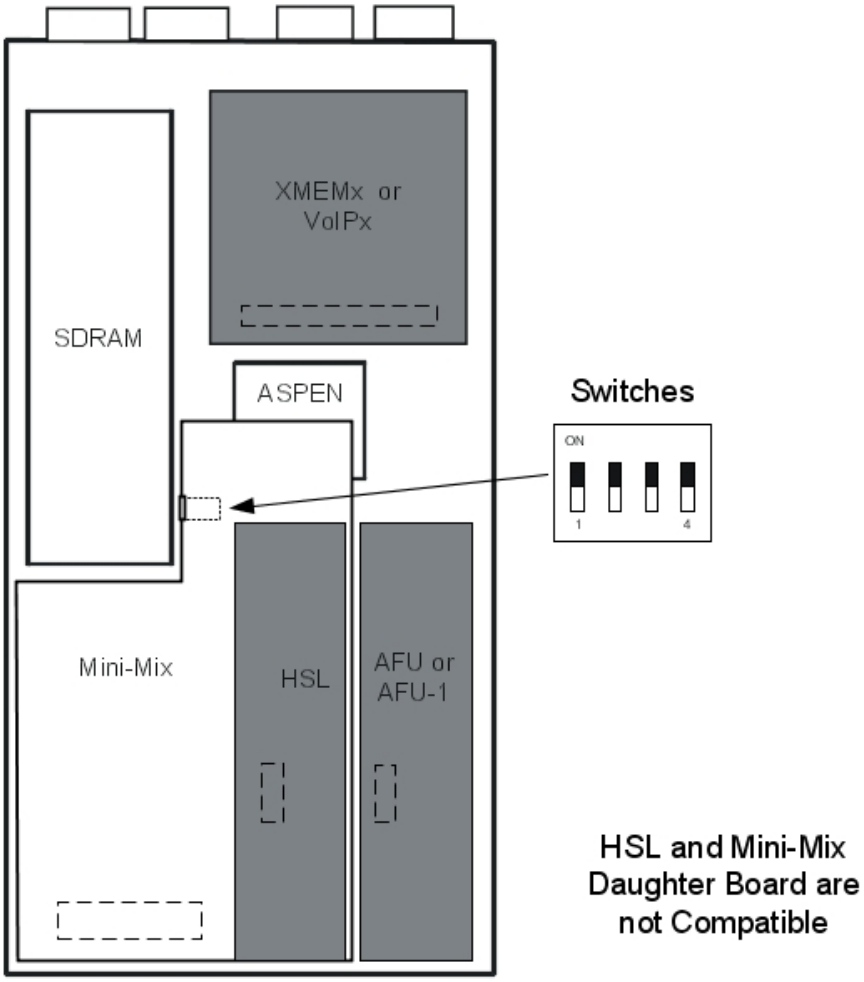


Figure 2.5 : Daughter Board Position on CPU-3m or CPU-4

2.2.1.2 Hardware configuration

2.2.1.2.1 Meaning of the LED Indications

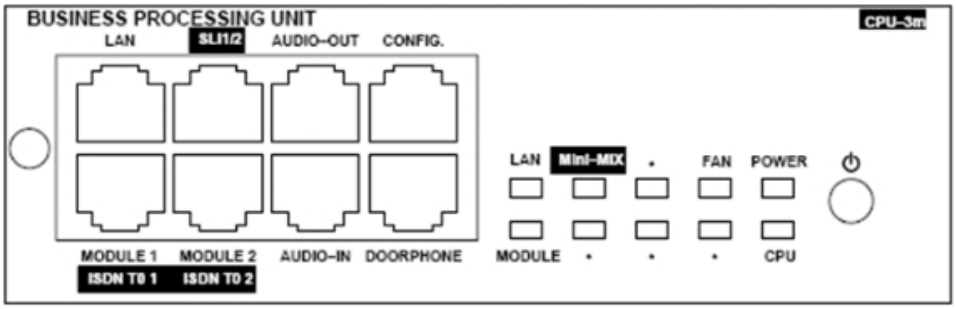


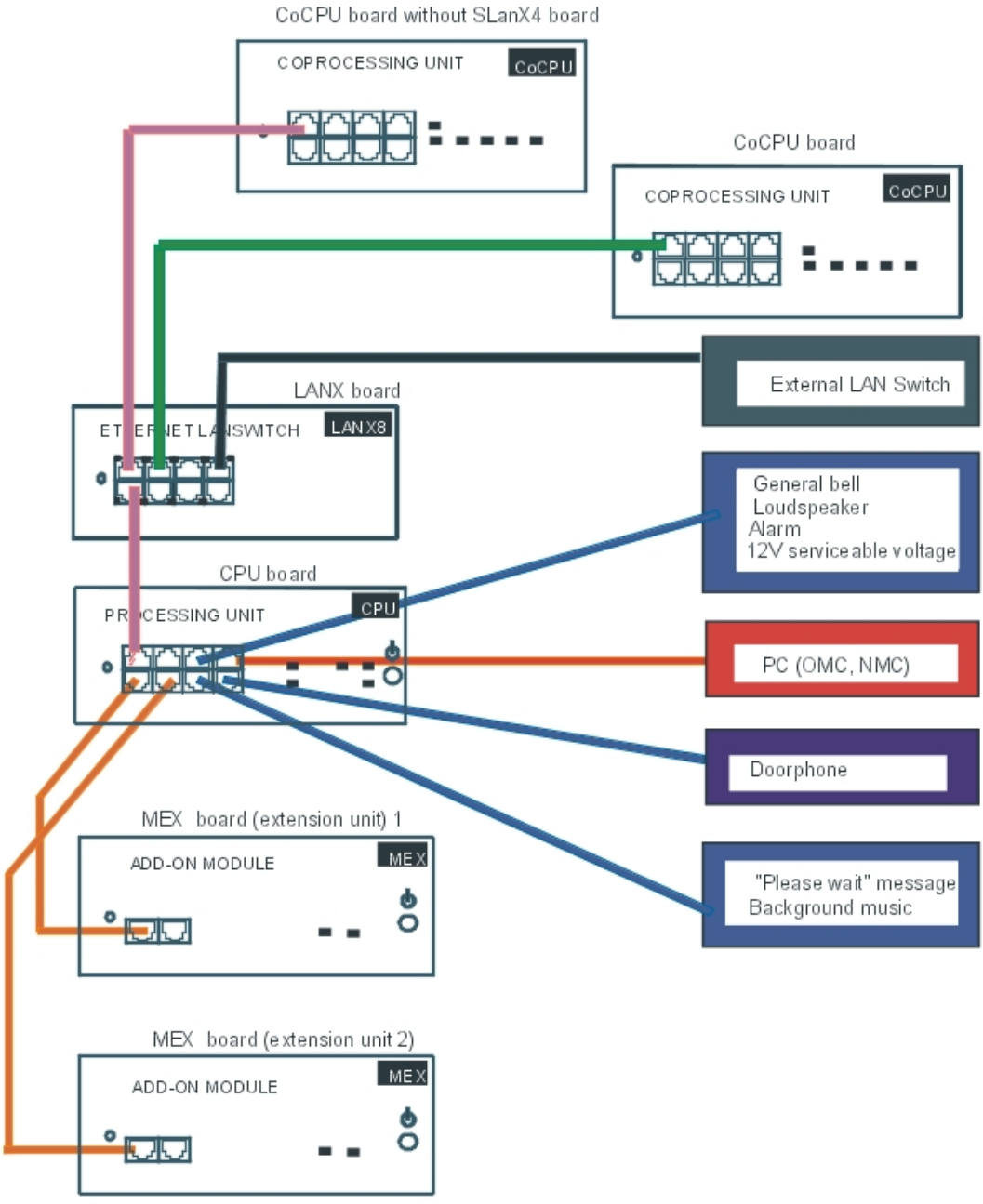
Figure 2.6 : CPU Front Panel

table 2.1 : LED Meaning for a Main CPU

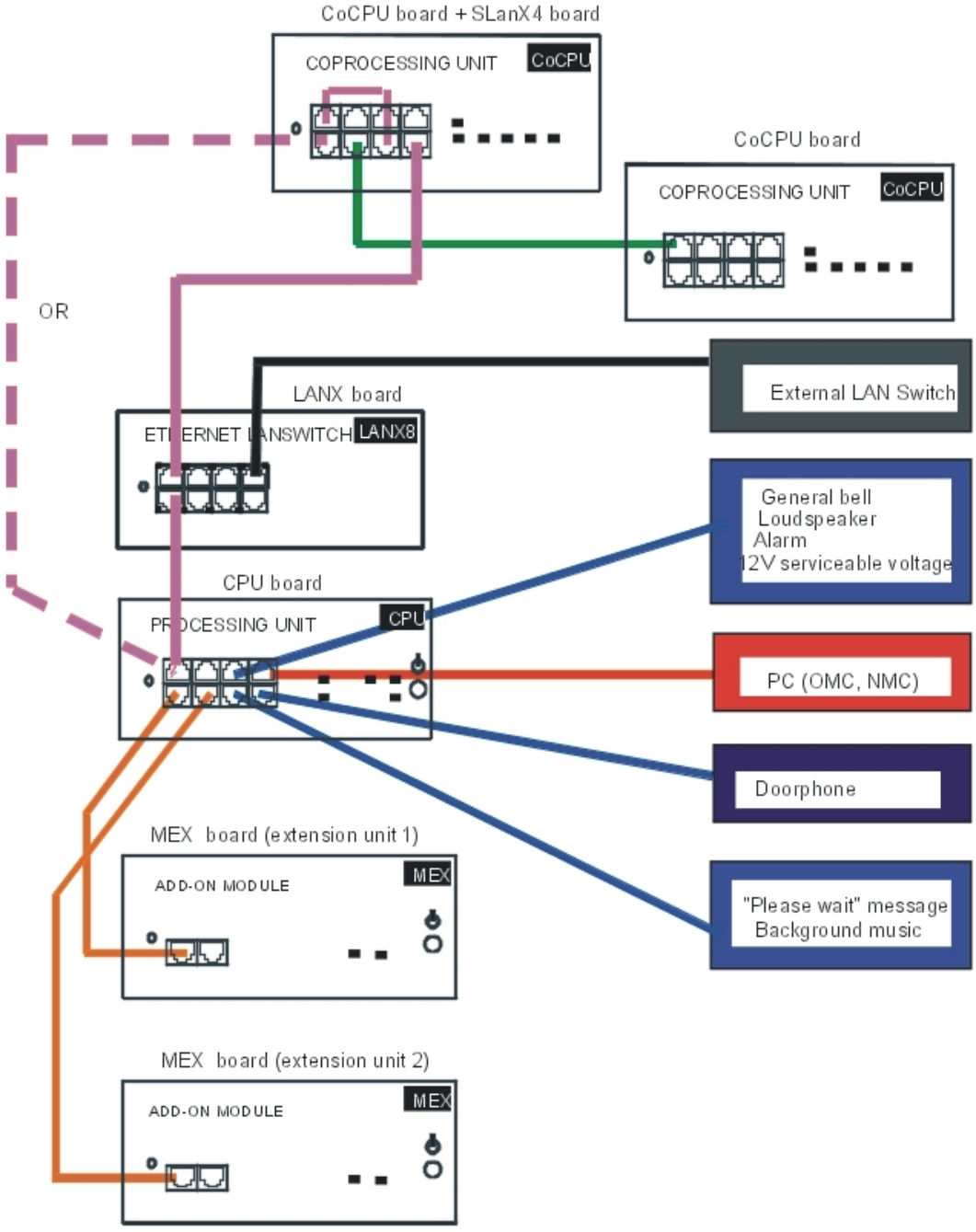
Name	**Colour**	**Function**
CPU	Green	CPU functioning LED (flashing)
POWER	Red/Green	Power status LED: - Mains operation: steady green LED - Battery operation: steady yellow LED - Idle: flashing red LED
FAN	Red/Green	Fan status LED: - Both fans functioning: steady green LED - 1 or both fans down: steady red LED
LAN	Green	LAN functioning LED (flashes when there is traffic)
Mini-MIX	Green	Detection of Mini-MIX board in a Compact Edition 2nd Generation
MODULE	Green	Presence of HSL board

2.2.1.2.2 GENERAL CONNECTION DIAGRAM

Configuration without SLANX4 (recommended configuration)



Configuration with SLANX4



2.2.1.3 External connections

2.2.1.3.1 Output Port

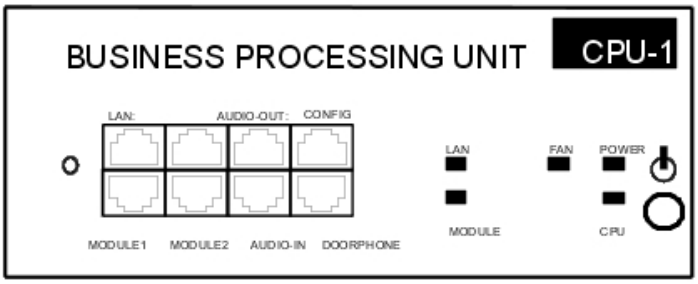


Figure 2.9 : CPU-1

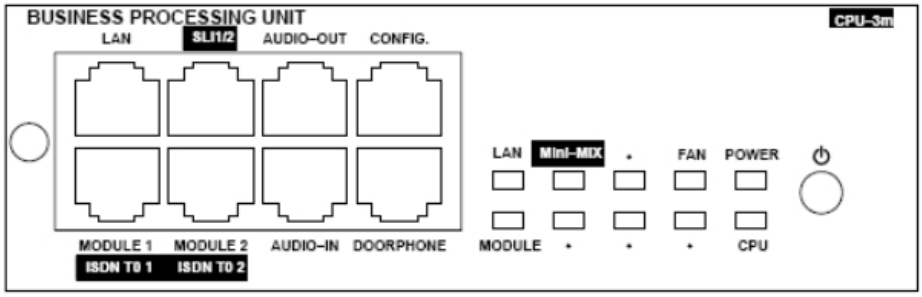


Figure 2.10 : CPU-3m or CPU–4

Available functions:

- **LAN**: 10/100 base T Ethernet port (MDI-II/straight)
- **AUDIO-OUT**: loudspeaker, alarm and general bell interfaces; 12V output
- **AUDIO-IN**: please-wait message and background music interfaces
- **DOORPHONE**: doorphone interfaces
- **CONFIG**: RS232 for MMC, NMC and PPP connections
- **MODULE1**: HSL link to add-on module 1 (if HSL daughter board present)

- **MODULE2**: HSL link to add-on module 2 (if HSL daughter board present)
- **ISDN T0 1**: T0 access 1 if Mini-Mix daughter board present (CPU-3m or CPU-4 only)
- **ISDN T0 2**: T0 access 2 if Mini-Mix daughter board present (CPU-3m or CPU-4 only)
- **SLI1/2**: access to analog terminals 1 and 2 (if Mini-Mix daughter board present on CPU-3m or CPU-4)

table 2.2 : Socket Connections

RJ45 pin	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
LAN	TX+	TX-	RX+			RX-		
SLI 1/2 (CPU-3m and CPU-4 only)			ZA1	ZB1			ZA2	ZB2
AUDIO-OUT	Audio Out A	Audio Out B	Alarm A	CenRg A	CenRG B	Alarm B	Grd	+12 V
CONFIG	CTS	DSR	RX	Ground	Ground	TX	DTR	RTS
MODULE1	TX+	TX-	RX+			RX-		
MODULE2	TX+	TX-	RX+			RX-		
AUDIO-IN	Audio In A	Audio In B	Audio Ctrl A			Audio Ctrl B		
DOORPHONE			DoorPh B1	DoorPhA1	DoorPhA2	DoorPhB2		
ISDN T0 1 (CPU-3m and CPU-4 only)			TX+	RX+	RX+	TX+		
ISDN T0 2 (CPU-3m and CPU-4 only)			Tx+	RX+	Rx-	Tx-		

2.2.1.3.2 Connecting a PATA Hard Disk

The PATA hard disk is connected to the XMEM (or VOIP) daughter board via a flat cable.

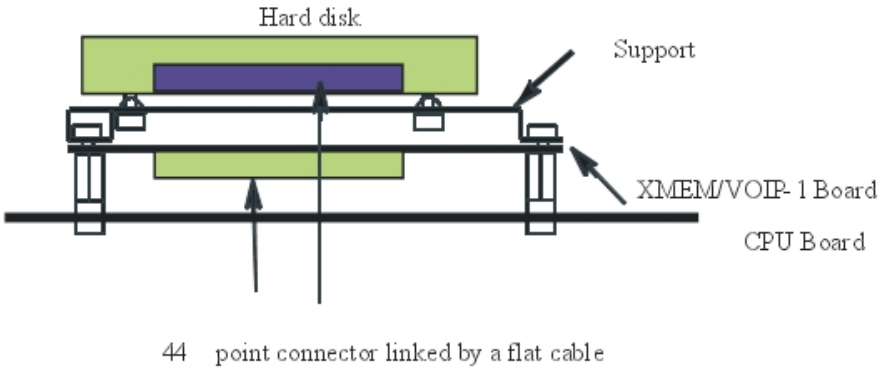


Figure 2.11 : PATA Hard Disk Connection

Hard disks are fitted using an XMEM (XMEM, XMEM-1, or XMEM128-1) or VOIP (VOIP or VOIP-1) daughter board.

Important:

Before performing an installation, take anti-static precautions (wristband, heelpiece, etc.) when handling the hard disk. Electrostatic discharges can shorten the life of the disk.

When going into stand-by mode, wait for red Power LED to stop flashing before you remove the CPU board from the module. Extracting the disk before the switch to standby is completed can destroy part of the disk or damage its contents. Never handle the hard disk until the motor has stopped completely (about 4 seconds after the red Power LED stops flashing).

2.2.1.3.3 Connecting a SATA Hard Disk

The SATA hard disk is connected to the XMEM or VOIP daughter board via the P2SATA-AXV (or P2SATA-AV1) daughter board.

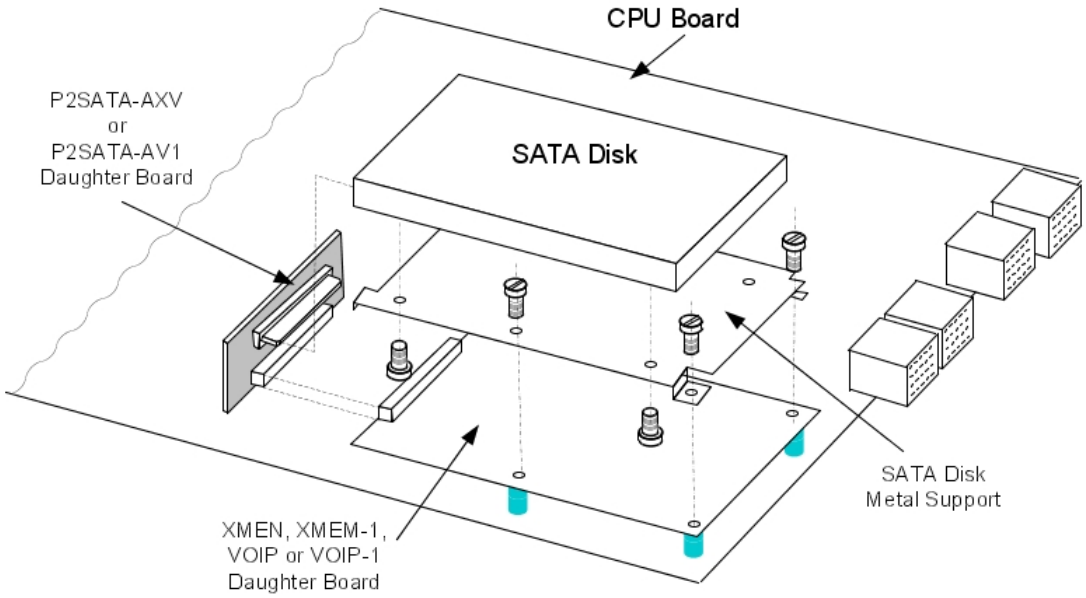


Figure 2.12 : SATA Hard Disk Connection

The P2SATA-AXV is used to connect to the XMEM, the XMEM-1 or the VOIP daughter boards.

The P2SATA-AV1 is used to connect to the VOIP-1 daughter board.

Caution:

Before performing an installation, take anti-static precautions (wristband, heelpiece, etc.) when handling the hard disk. Electrostatic discharges can shorten the life of the disk.

When going into stand-by mode, wait for the red Power LED to stop flashing before removing the CPU board from the module. Extracting the disk before the switch to standby is completed can destroy part of the disk or damage its contents. Never handle the hard disk until the motor has stopped completely (about 4 seconds after the red Power LED stops flashing).

2.2.1.3.4 Connecting a Music-on-Hold Message Player

This is connected via the **Audio CTRL** output (control contact open when idle) and the **Audio In** input of the AUDIO-IN connector.

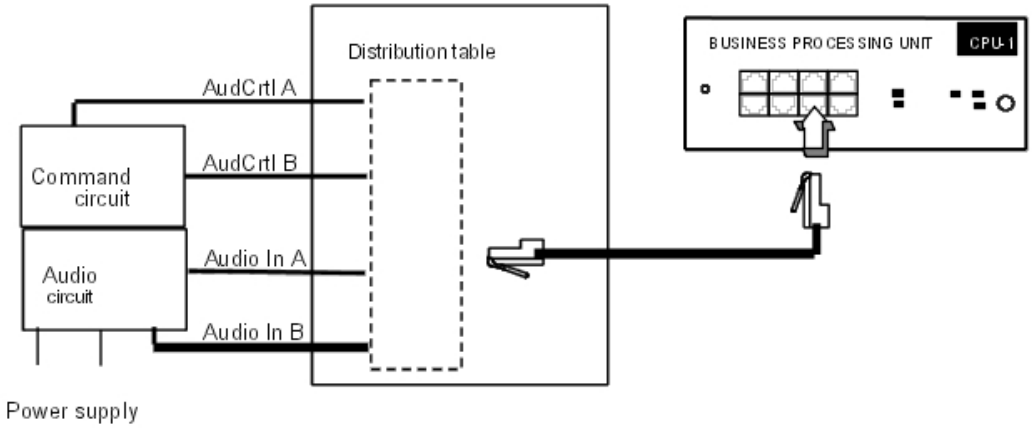


Figure 2.13 : Music-On-Hold Message Player Connection

Audio input characteristics:

- Input impedance 600 Ohms

Contact properties (same characteristics for the alarm and doorphone control contacts):

- Max. power 10 W
- Max. voltage 60 V
- Max. current 500 mA

2.2.1.3.5 Connecting a Source for Background Music

This is connected via the **Audio In** input of the AUDIO-IN connector.

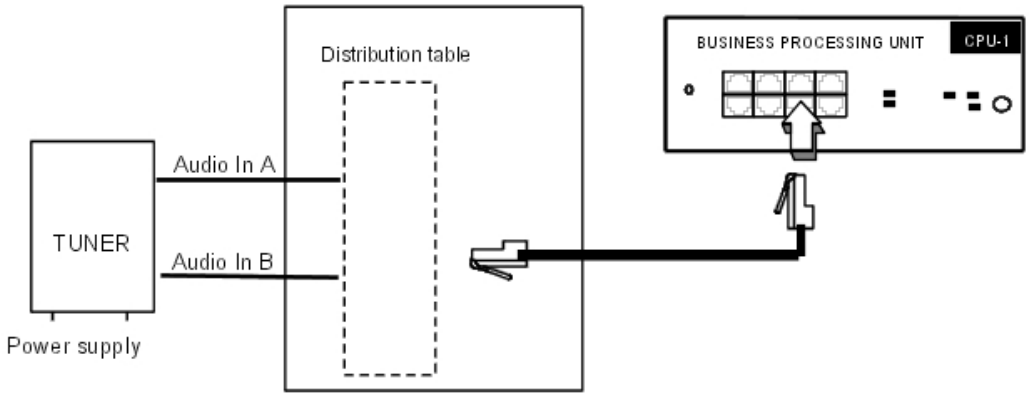


Figure 2.14 : Background Music Connection

Audio input characteristics:

- Input impedance: 600 Ohms
- Input level: access + 4.7 dBr or + 15 dBr

2.2.1.3.6 Connecting an Alarm

The alarm is activated under the same conditions as TL forwarding (power outage or software command).

This is connected via the **Alarm** output (control contact closed when idle) of the AUDIO-OUT connector.

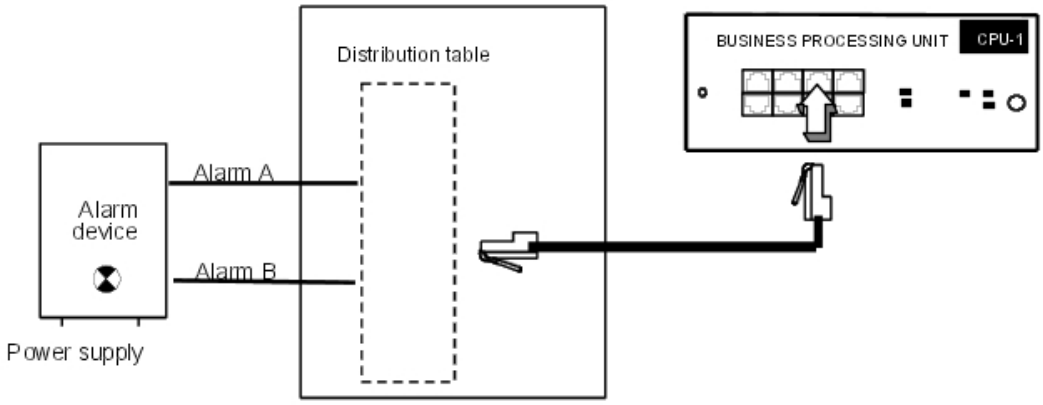


Figure 2.15 : Alarm Connection

2.2.1.3.7 Connecting a Doorphone

The doorphone interface comprises an intercom and an optional door strike that works in conjunction with an electrical supply provided through a suitable low voltage transformer, for example a SELV (Safety Extra Low Voltage) transformer.

It is connected via the **DoorPhA** and **DoorPhB** outputs (control contacts remain open when idle) of the DOORPHONE connector.

Connecting an NPTT doorphone

- A single doorphone with doorstrike may be connected to the system.
- The system also allows for the connection of 2 doorphones without doorstrikes.

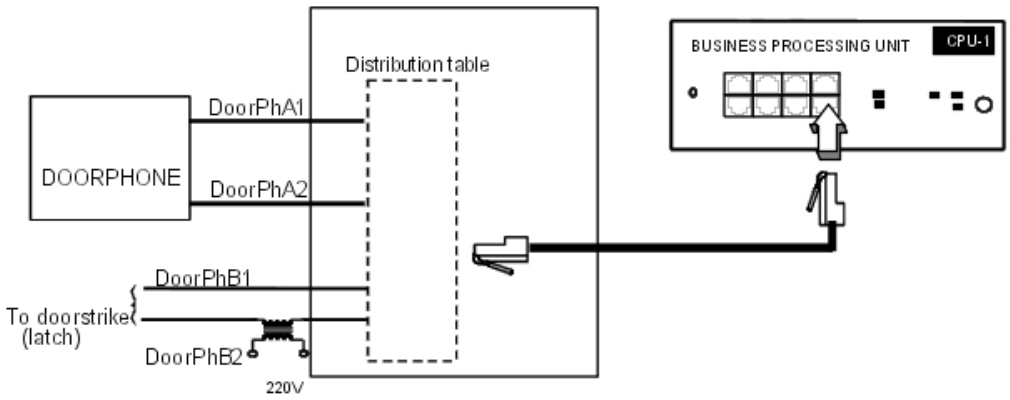


Figure 2.16 : Doorphone Connection

Connecting Telemini and Universal Doorphones

These doorphones only require the use of an analog (Z) station interface.

- Several of these doorphones can be connected to the system; the limit is determined by the maximum number of analog stations the system can support.
- A system cannot have TELEMINI and UNIVERSAL doorphones at the same time.

2.2.1.3.8 Connecting a General Bell

The general bell is connected via the **CenRg** output of the AUDIO-OUT connector.

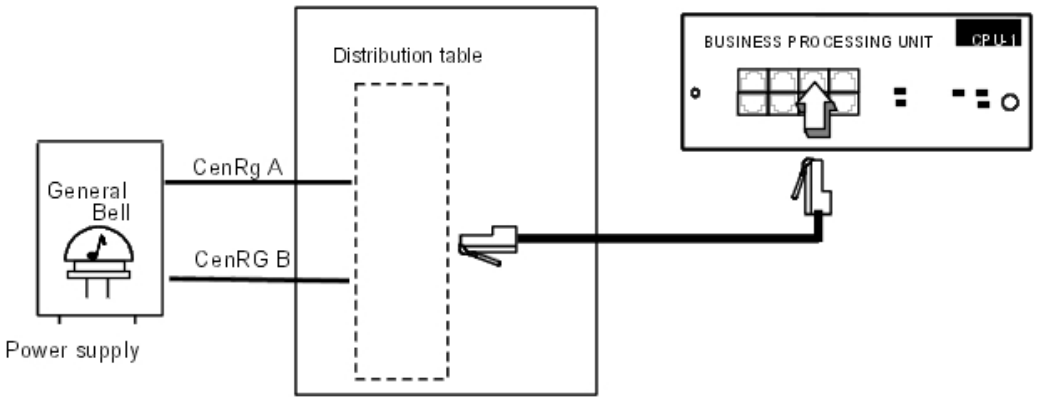


Figure 2.17 : General Bell Connection

2.2.1.3.9 Connecting a Speaker System

A compatible speaker system may be connected via the **Audio Out** output of the AUDIO-OUT connector.

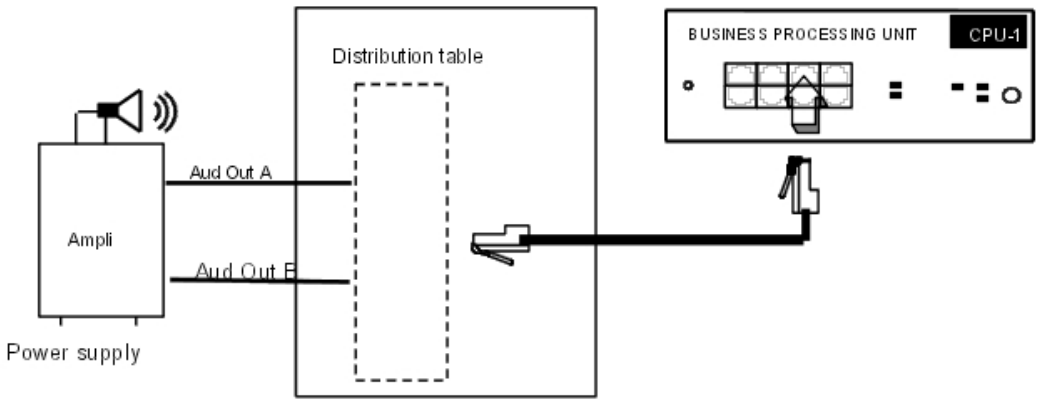


Figure 2.18 : Speaker System Connection

- Output impedance: <500 Ohms
- Output level: access + 3 dBr

2.2.1.3.10 Using the 12V Output

The **Ground** and **+ 12V** outputs on the AUDIO-OUT connector allow for the connection of an external 12V device with a maximum energy consumption of 150 mA (Rack 1 and Rack 2) or 300 mA (Rack 3).

2.2.1.3.11 Z and T0 Accesses

The **Mini-MIX** daughter board is used with **CPU-3m** or **CPU-4** on Compact Edition 2nd Generation.

It provides two T0 and two Z accesses.

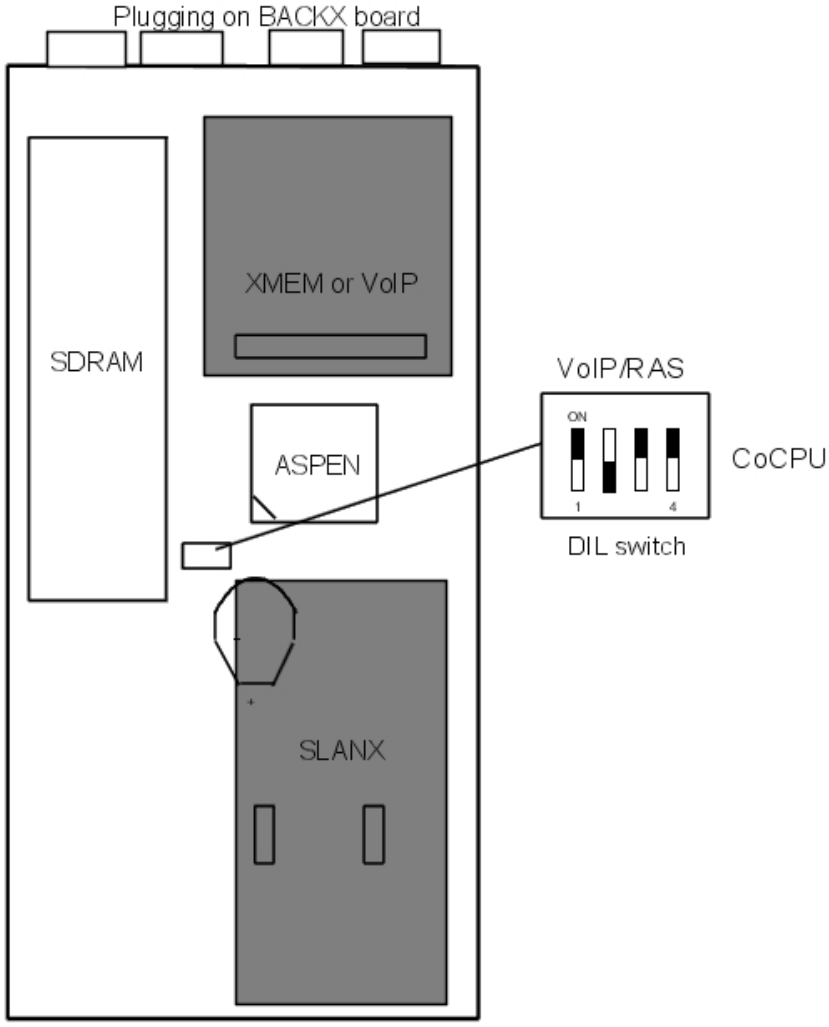
The numbering for the Mini-MIX accesses is the following:

- Slot 80 EN 1 for the first T0 access
- Slot 80 EN 2 for the second T0 access
- Slot 80 EN 9 for the first Z port
- Slot 80 EN 10 for the second Z port

2.2.2 CoCPU

2.2.2.1 Hardware description

The CoCPU (CoProcessing Unit) boards enable applications such as Voice over IP (VoIP) and Remote Access Server (RAS).



2.2.2.1.1 DAUGHTER BOARDS

The CoCPU (CoCPU-1 and CoCPU-2) boards can be equipped with the following daughter boards:

- VoIP/VoIP-1 (Voice Over IP): Gateway H323 with integrated Gatekeeper function; supports the management of CODECs and DSPs for IP telephony and IP Trunk (IP trunk lines) applications.
- SLANX (LANX Switch): 4 LAN Switch ports.

DAUGHTER BOARDS	**CoCPU**
VoIP/VoIP-1	YES
SLANX4	YES
HARD DISK	NO

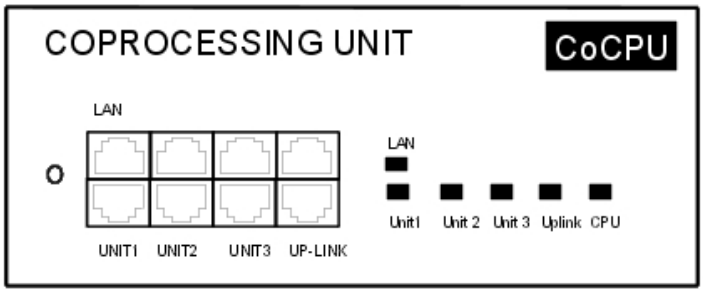
CoCPU without VoIP daughter board is a RAS CoCPU.

2.2.2.1.2 SDRAM CAPACITY

Capacity	CoCPU	CoCPU-1/CoCPU-2
SDRAM32	YES	NO
SDRAM64	NO	YES
SDRAM128	NO	NO

2.2.2.2 Hardware configuration

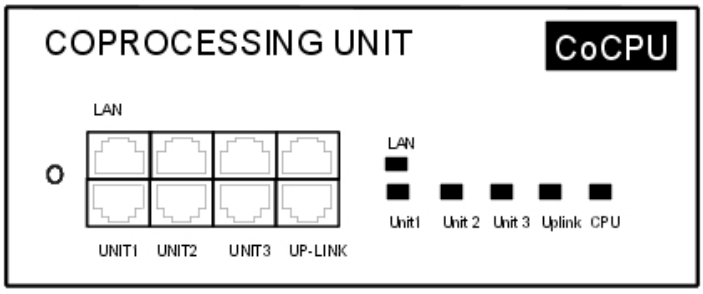
2.2.2.2.1 MEANING OF THE LED INDICATIONS



Name	Colour	Function
CPU	Green	CPU functioning LED (flashing)
LAN	Green	LAN functioning LED (flashes when there is traffic)
UNITS 1 - 4 UPLINK	Green	LAN switch interfaces 1 to 4 functioning LED (flashes when there is traffic)

2.2.2.3 External connections

2.2.2.3.1 OUTPUT PORTS (FACEPLATE)



Available functions:

- LAN : 10/100 base T Ethernet port (MDI-II/straight)

- UNIT1, UNIT2, UNIT3: Ports on integrated LAN switch (MDI-X/crossover).
- UPLINK: integrated LAN switch uplink port (MDI-II/straight).

RJ45 pin	1	2	3	4	5	6	7	8
LAN outputs	TX+	TX-	RX+			RX-		
Uplink outputs	TX+	TX-	RX+			RX-		
Unit 1 to 3 outputs	RX+	RX-	TX+			TX-		

2.2.2.3.2 CONNECTION

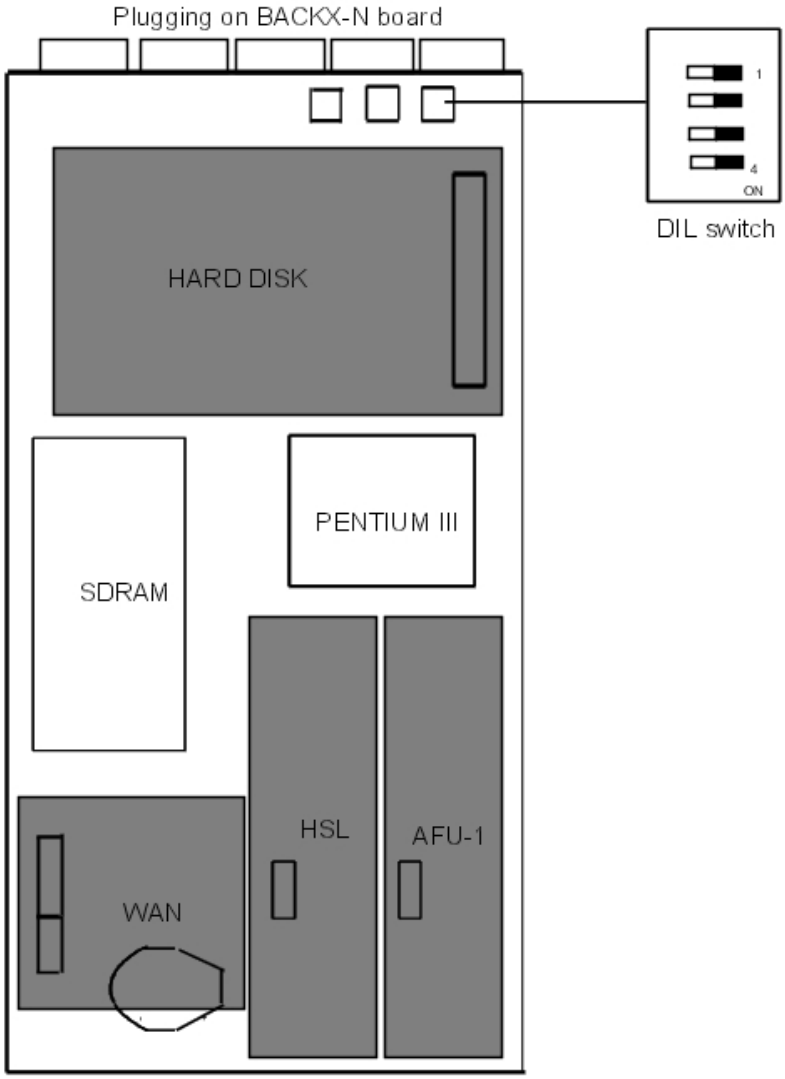
The CoCPU boards are connected either to the CPU board (LAN port) or to a LAN switch port. See also the General Diagram in the section on CPU-CPUe boards.

2.2.3 CPUe-1/CPUe-2

2.2.3.1 Hardware description

The CPUe-1/CPUe-2 boards (Central Processing Units) are based on the Pentium III LP (Low Power) processor.

They have the following characteristics: 700 MHz processor, 32 MB NAND Flash, 256 MB SDRAM, DSP 5410 and 5402, RMA.



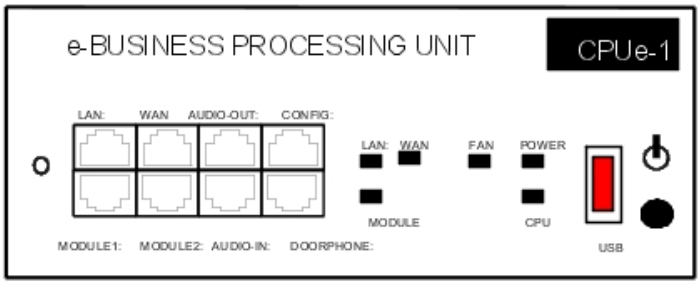
2.2.3.1.1 DAUGHTER BOARDS

The CPUe-1/CPUe-2 boards can be equipped with the following daughter boards:

- HSL (High Speed Link): module interconnections
- WAN/EtherWAN: Ethernet link allowing the connection of an external DSL modem or an external router
- Data-T1: for an Integrated T1 (voice/data) connection
- AFU-1 (Auxiliary Function Unit): support for auxiliary functions: general bell, doorphone, audio In, audio Out, etc.; this board also allows the connection of a forwarding T0/S0 ISDN-EFM box.
- HARD DISK: 2.5" hard disk.

2.2.3.2 Hardware configuration

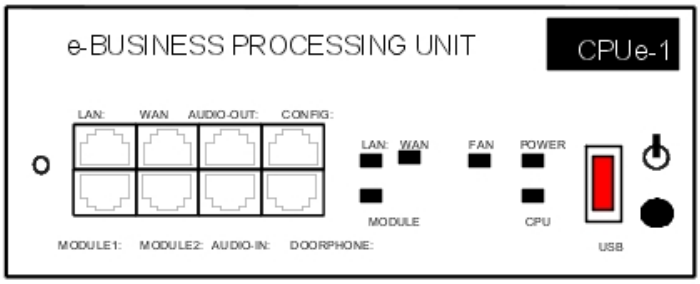
2.2.3.2.1 MEANING OF THE LED INDICATIONS



Name	Color	Function
CPU	Green	CPU functioning LED (flashing)
POWER	Red/Green	- Mains operation: steady green LED - Battery operation: steady yellow LED - Idle: flashing red LED - System shutdown: steady red LED
FAN	Red/Green	- Both fans functioning: steady green LED - 1 or both fans down: steady red LED
LAN	Green	LAN functioning LED (flashes when there is traffic)
MODULE	Green	Presence of HSL board
WAN	Green	LED showing correct WAN operation (flashes when there is traffic); LED used if an ADSL modem/cable modem is connected.

2.2.3.3 External connections

2.2.3.3.1 OUTPUT PORTS (FACEPLATE)



Available functions:

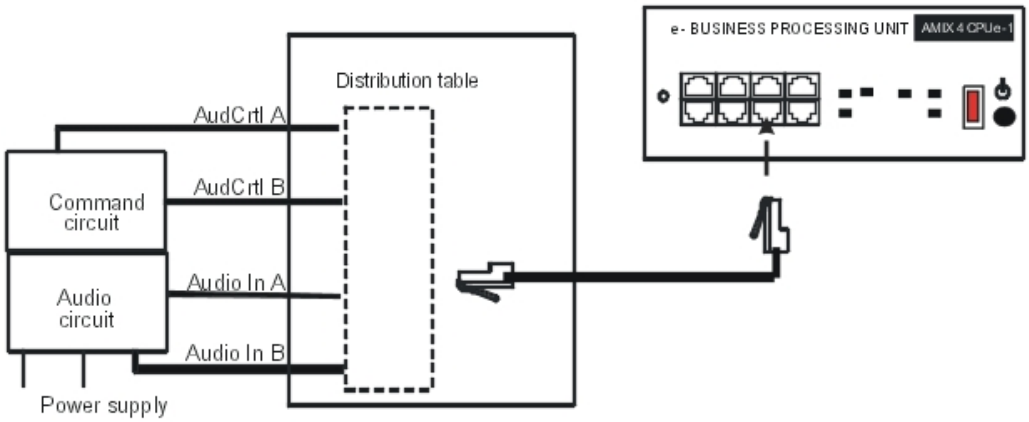
- LAN : 10/100 base T Ethernet (MDI-II/straight)
- WAN: 10/100 base T Ethernet (MDI-II/straight); connection to an ADSL modem
- AUDIO-OUT: loudspeaker, alarm and general bell interfaces; 12V output

- AUDIO-IN: please-wait message and background music interfaces
- DOORPHONE: doorphone interfaces
- CONFIG: RS232 for MMC, NMC and PPP connections
- MODULE1: HSL link to add-on module 1
- MODULE2: HSL link to add-on module 2
- USB: USB connector (not used in the current state of the product)

RJ45 pin	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
LAN outputs	TX+	TX-	RX+			RX-		
AUDIO-OUT outputs	Audio Out A	Audio Out B	Alarm A	CenRg A	CenRg B	Alarm B	Ground	+12 V
CONFIG outputs	CTS	DSR	RX	Ground	Ground	TX	DTR	RTS
MODULE1 outputs	TX+	TX-	RX+			RX-		
MODULE2 outputs	TX+	TX-	RX+			RX-		
AUDIO-IN outputs	Audio In A	Audio In B	Audio Ctrl A			Audio Ctrl B		
DOORPHONE outputs			Door PHB1	DoorPHA1	DoorPHA2	Door PHB2		
USB outputs (not used)	0V	D0-	D0+	GND:	Ground	Ground	Ground	Ground

2.2.3.3.2 CONNECTING A MUSIC-ON-HOLD MESSAGE PLAYER

This is connected via the **AudioCTRL** output (control contact open when idle) and the **Audio In** input of the AUDIO-IN connector.



Audio input characteristics:

- Input impedance 600 Ohms

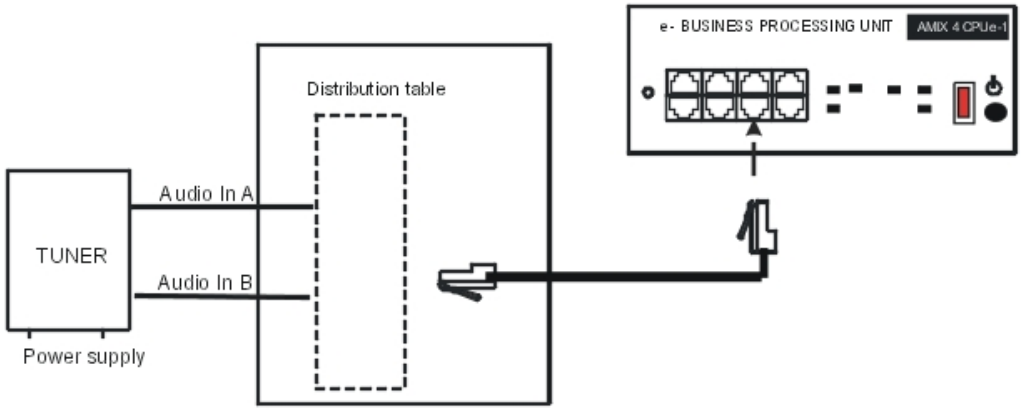
Contact properties (same characteristics for the alarm and doorphone control contacts):

- Max. power 10 W

- Max. voltage 60 V
- Max. current 500 mA

2.2.3.3.3 CONNECTING A SOURCE FOR BACKGROUND MUSIC

This is connected via the **Audio In** input of the AUDIO-IN connector.



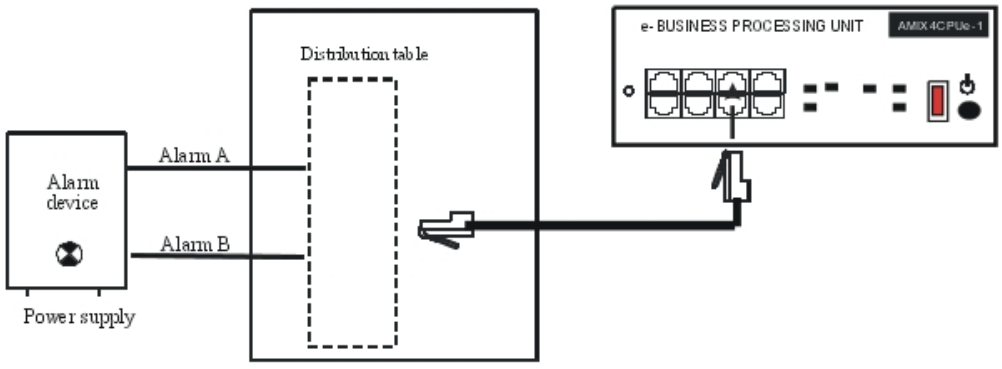
Audio input characteristics:

- Input impedance: 600 Ohms
- Input level: access + 4.7 dBr or + 15 dBr

2.2.3.3.4 CONNECTING AN ALARM

The alarm is activated under the same conditions as TL forwarding (power outage or software command).

This is connected via the **Alarm** output (control contact closed when idle) of the AUDIO-OUT connector.



2.2.3.3.5 CONNECTING A DOORPHONE

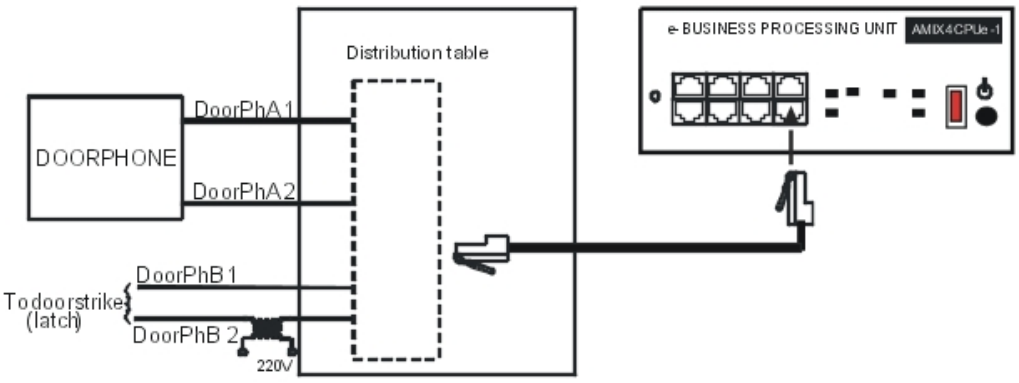
The doorphone interface comprises an intercom and an optional door strike that works in conjunction with an electrical supply provided through a suitable low voltage transformer, for

example a SELV (Safety Extra Low Voltage) transformer.

It is connected via the **DoorPHA** and **DoorPHB** outputs (control contacts open when idle) of the DOORPHONE connector.

Connecting an NPTT doorphone

- A single doorphone with doorstrike may be connected to the system.
- The system also allows the connection of 2 doorphones without doorstrikes.



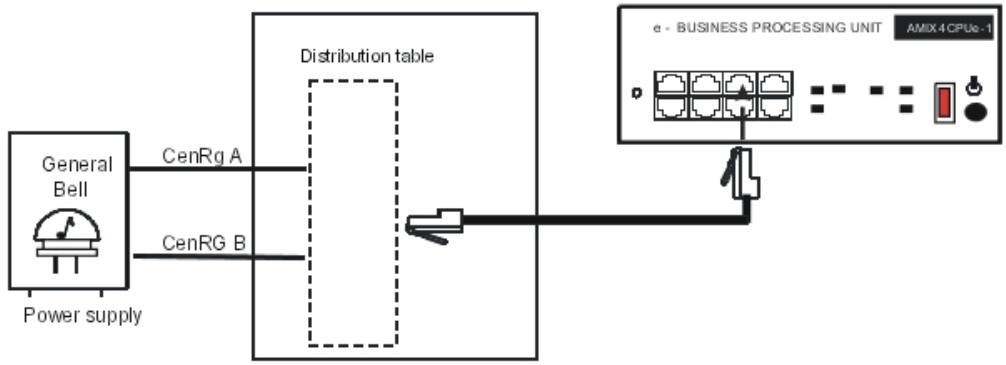
Connecting Telemini and Universal Doorphones

These doorphones only require the use of an analogue (Z) station interface.

- Several of these doorphones can be connected to the system; the limit is determined by the maximum number of analogue stations the system can support.
- A system cannot have TELEMINI and UNIVERSAL doorphones at the same time.

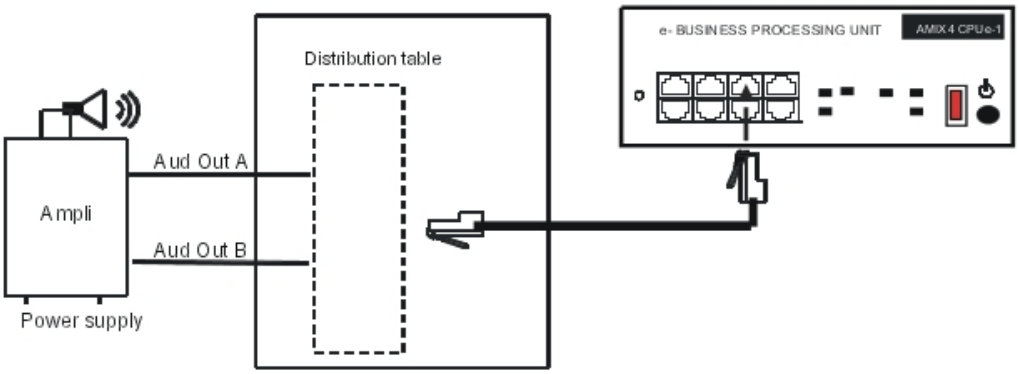
2.2.3.3.6 CONNECTING A GENERAL BELL

The general bell is connected via the **CenRg** output of the AUDIO-OUT connector.



2.2.3.3.7 CONNECTING A SPEAKER SYSTEM

A compatible speaker system may be connected via the **Audio Out** output of the AUDIO-OUT connector.



Audio output characteristics:

- Output impedance: < 500 Ohms
- Output level: access + 3 dBr

2.2.3.3.8 USING THE 12V OUTPUT

The **Ground** and **+ 12V** outputs on the AUDIO-OUT connector allow for the connection of an external 12V device with a maximum energy consumption of 150 mA (Rack 1 and Rack 2) or 300 mA (Rack 3).

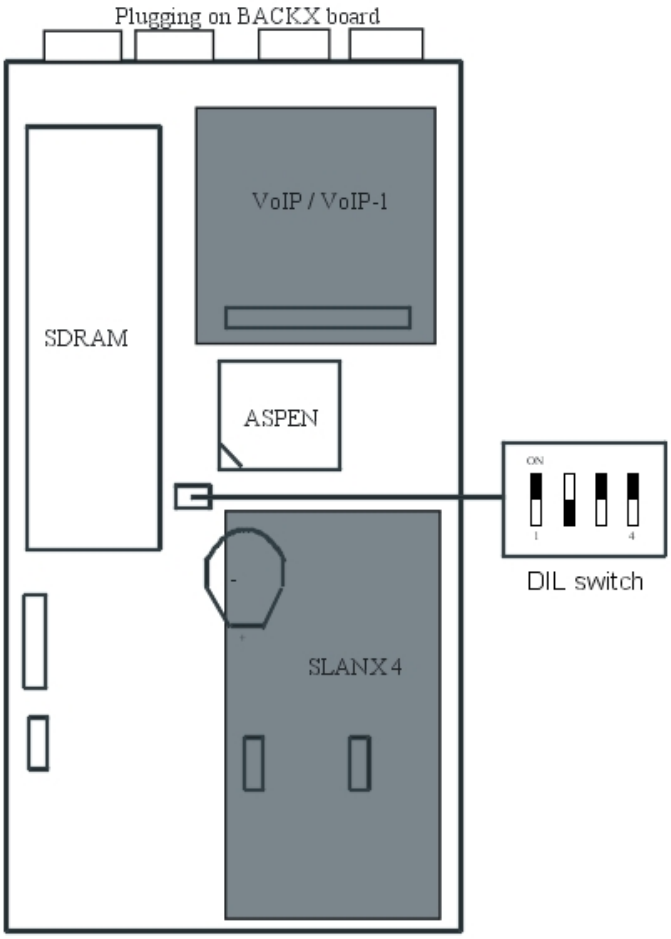
2.2.4 CoCPU-1/CoCPU-2

2.2.4.1 Hardware description

The CoCPU-1 and CoCPU-2 boards (Central CoProcessing Units) have the following characteristics:

- 133 MHz Aspen processor
- 32 MB NAND Flash
- 64 MB SDRAM
- DSP 5410 and 5402

They are necessary when using one of the two following functionalities: VoIP or RAS (no simultaneous use).



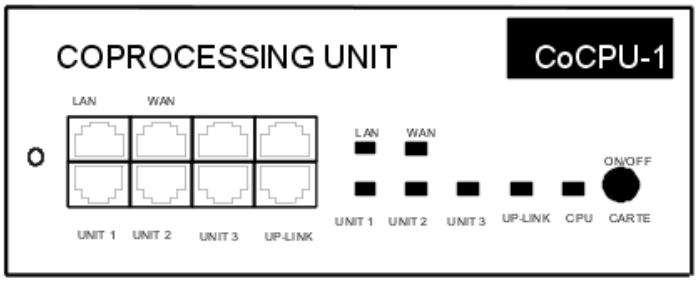
2.2.4.1.1 DAUGHTER BOARDS

The CoCPU-1/CoCPU-2 boards can be equipped with the following daughter boards:

- VoIP/VoIP-1: (Voice over IP): Gateway H323 with integrated Gatekeeper function; supports the management of CODECs and DSPs for IP telephony and IP Trunk (IP trunk lines) applications.
- SLANX (Switched LANX): 4 LAN switch ports.

2.2.4.2 Hardware configuration

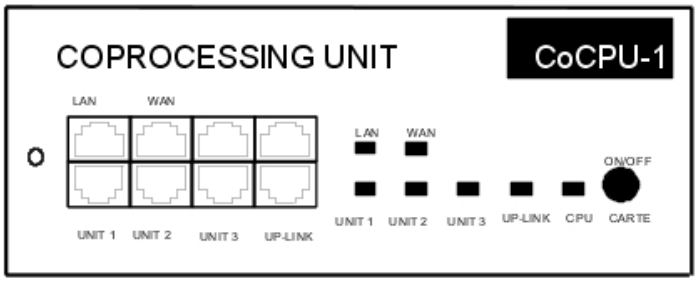
2.2.4.2.1 MEANING OF THE LED INDICATIONS



Name	Color	Function
CPU	Green	CPU functioning LED (flashing)
LAN	Green	LAN functioning LED (flashes when there is traffic)
WAN	Green	Not used
UNITS 1 - 4 UPLINK	Green	LAN switch interfaces 1 to 4 functioning LED (flashes when there is traffic)

2.2.4.3 External connections

2.2.4.3.1 OUTPUT PORTS (BOARD STIFFENER)



Available functions:

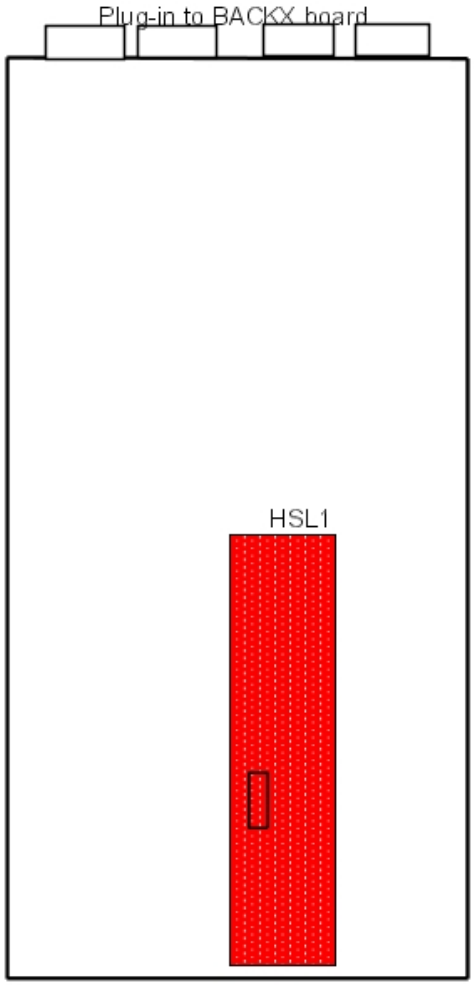
- LAN : 10/100 base T Ethernet port (MDI-II/straight)
- WAN : 10/100 base T Ethernet port (MDI-II/straight); ADSL modem connection
- UNIT1, UNIT2, UNIT3 : ports on integrated LAN switch (MDI-X/crossover)
- UPLINK : Integrated LAN switch uplink port (MDI-II/straight).

RJ45 pin	1	2	3	4	5	6	7	8
LAN/WAN outputs	TX+	TX-	RX+			RX-		
Uplink outputs	TX+	TX-	RX+			RX-		
Unit 1 to 3 outputs	RX+	RX-	TX+			TX-		

2.2.5 MEX

2.2.5.1 Hardware description

The MEX board (Module EXpansion) performs the controller functions in the add-on modules.

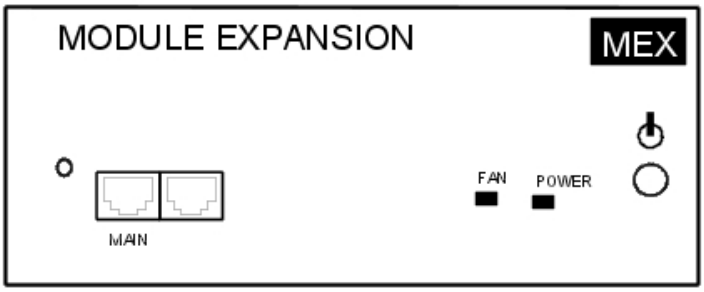


2.2.5.1.1 DAUGHTER BOARD

The MEX board is equipped with an HSL1 (High Speed Link) board for interconnecting with the basic module.

2.2.5.2 Hardware configuration

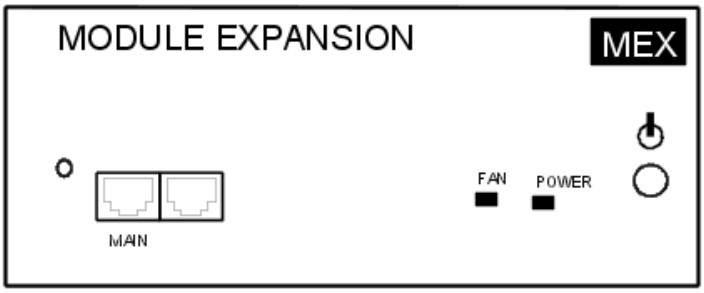
2.2.5.2.1 MEANING OF THE LED INDICATIONS



Name	Colour	Function
POWER	Red/Green	- Mains operation: steady green LED - Battery operation: steady yellow LED - Idle: flashing red LED
FAN	Red/Green	- Both fans functioning: steady green LED - 1 or both fans down: steady red LED

2.2.5.3 External connections

2.2.5.3.1 OUTPUT PORTS (FACEPLATE)



Available functions:

- MAIN: HSL to basic module (cable max. length: 5 metres).

RJ45 pin	1	2	3	4	5	6	7	8
MAIN outputs	TX+	TX-	RX+			RX-		

2.2.5.3.2 CONNECTION

The MEX board is connected to the **MODULE 1** or **MODULE 2** connector on the CPU/CPUe board. See also the General Diagram in the section on CPU-CPUe boards.

2.2.6 BRA

2.2.6.1 Hardware description

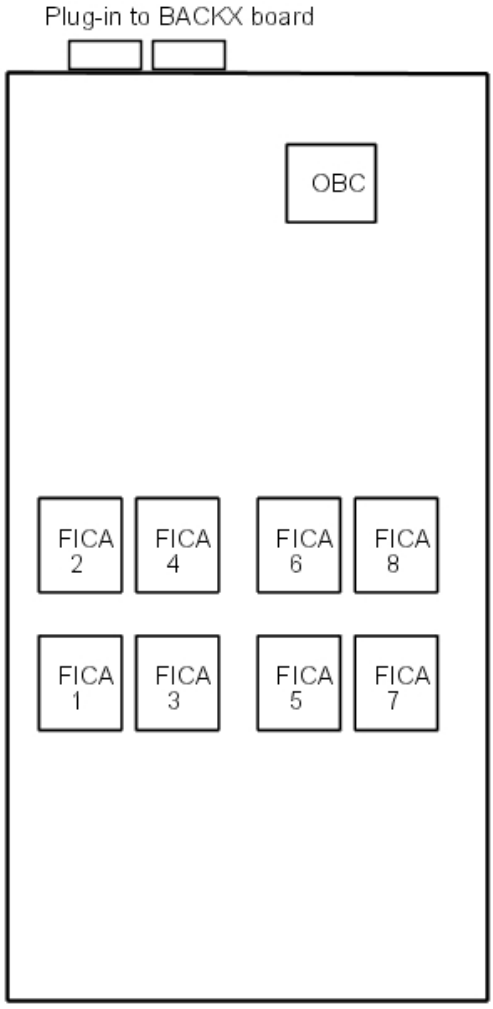
The BRA board The BRA (Basic Rate Access) board provides the basic access points (2 x 64-Kbps B-channels + 1 x 16-Kbps D-channel per access) for connecting the system to the ISDN digital public network (point-to-point or multipoint T0 link) and, starting with version R2.0, to a private network (point-to-point DLT0 link); 3 versions are offered:

- BRA2: 2 T0 accesses
- BRA4: 4 T0 accesses
- BRA8: 8 T0 accesses

With OMC it is possible to define the operating mode access by access: T0 (ISDN) or DLT0 (QSIG). If the choice is DLT0 (QSIG), the following operating mode may be defined: master = Network (NT), slave = User(TE)

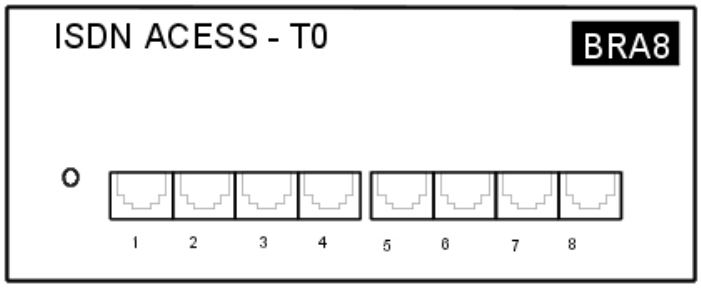
Note:

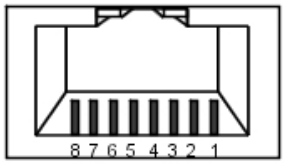
Configuration in T0/DLT0 is done by access pairs; if an access (04-001-01 for example) is configured in DLT0, the 2nd one (04-002-01) must also be configured in DLT0.



2.2.6.2 External connections

2.2.6.2.1 OUTPUT PORTS (BOARD STIFFENER)





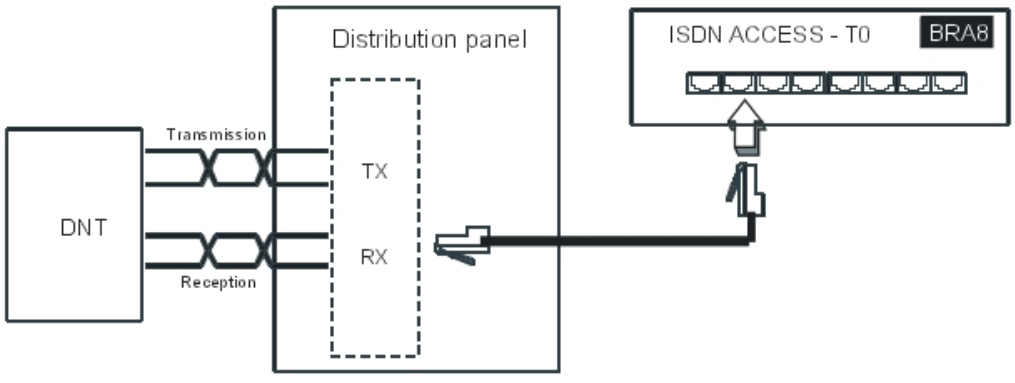
Female RJ45, front

RJ45 pin	1	2	3	4	5	6	7	8
Outputs			TX+	RX+	RX-	TX-		

2.2.6.2.2 CONNECTING A T0 ACCESS

The Alcatel-Lucent OmniPCX Office Communication Server system can be installed near the digital network termination or at a certain distance (up to 350 m), as required.

Connection without T0/S0 forwarding



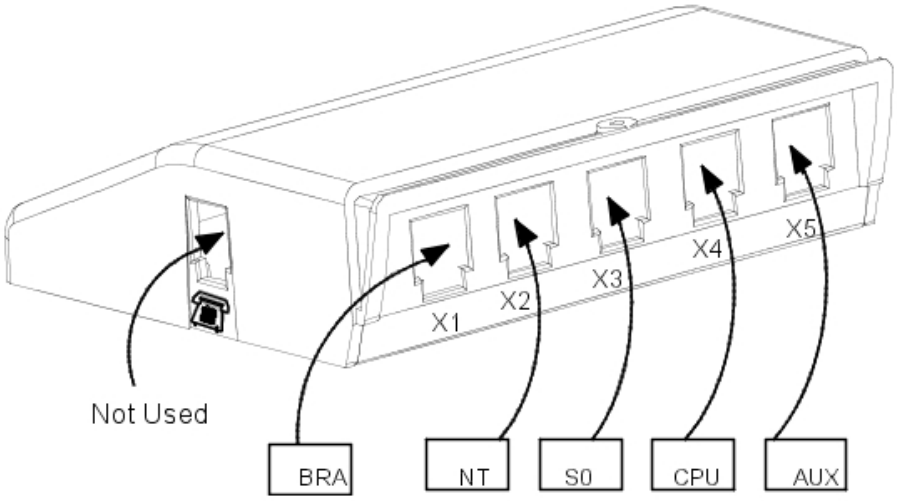
Connection with T0/S0 forwarding

In the event of a loss of tension or CPU malfunction, the ISDN-EFM box allows a T0 access to be forwarded directly to a S0 station.

Note:

The AFU-1 board (daughter board of the CPU board) must be equipped so as to detect a loss of tension.

Description of the ISDN-EFM box

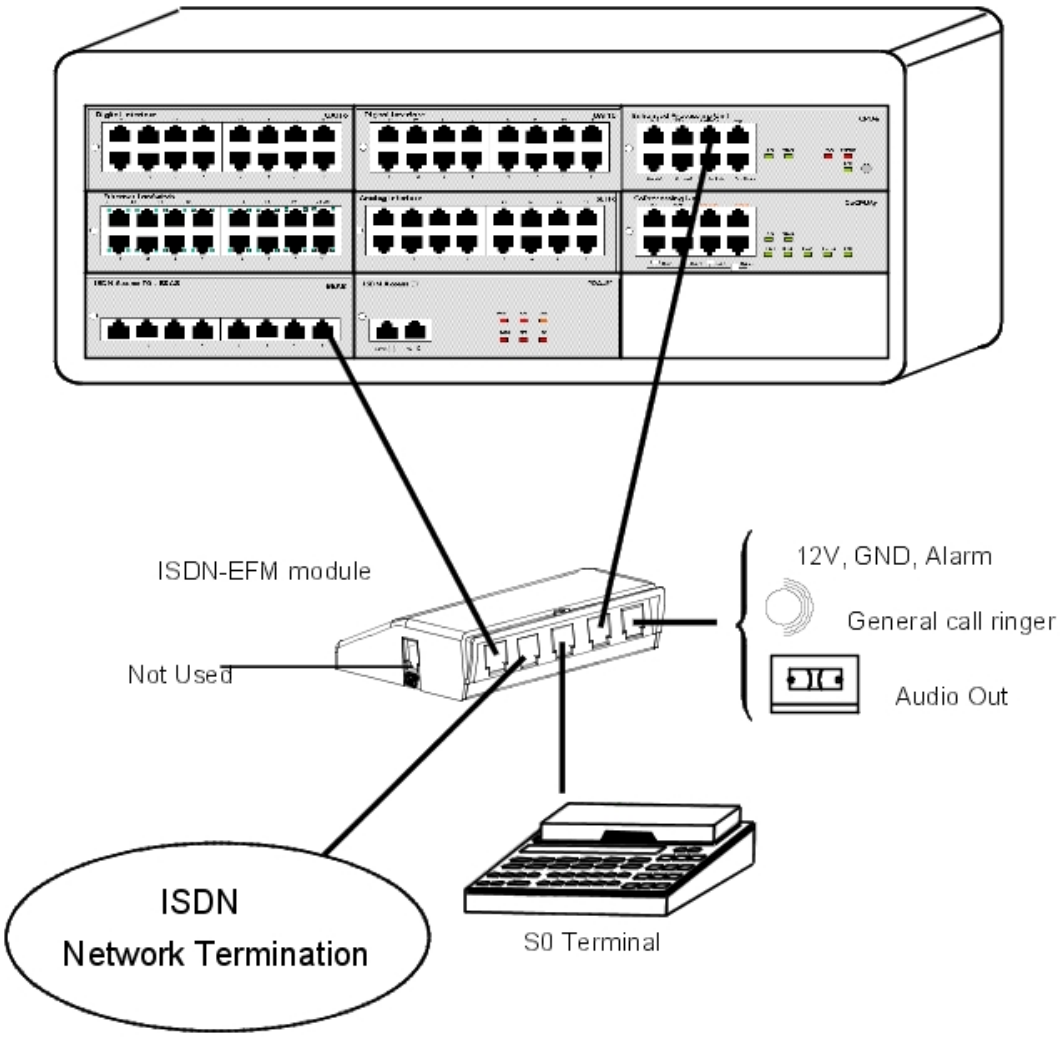


Connections

The ISDN-EFM box must be installed as close as possible to the system (3 m maximum). All the box connections are made with straight RJ45-RJ45 cables.

Output connectors functions:

- BRA: connection of T0 access to be forwarded.
- NT: Connection of ISDN network termination.
- S0: connection of forwarding S0 station.
- CPU: connection to the CPU board's AUDOUT connector.
- AUX: connection of Audio out, Alarm, General bell and 12 V use auxiliaries; since AUX is a copy of the CPU board's AUDOUTde connector, check the sheet of the CPU board in use for connection recommendations.



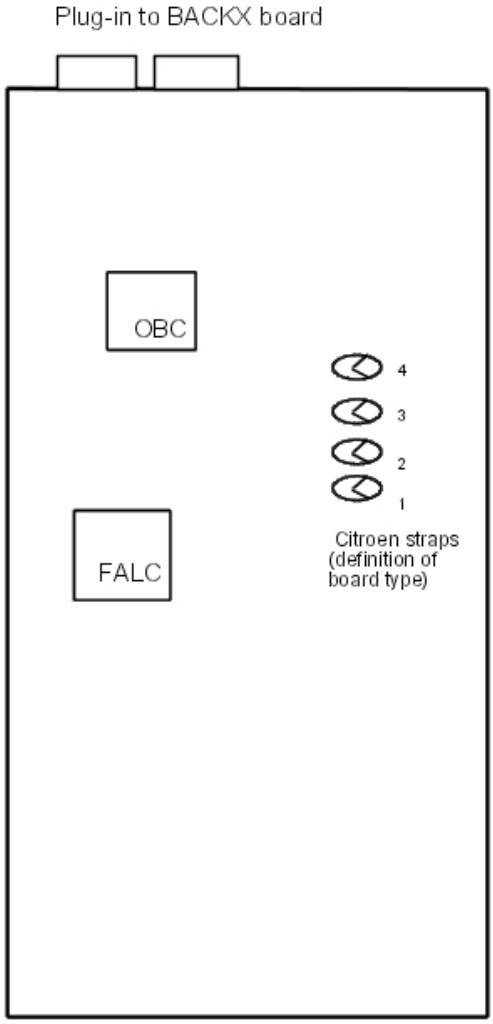
2.2.7 PRA

2.2.7.1 Hardware description

The PRA board (Primary Rate Access) board provides 1 primary access for connecting the Alcatel-Lucent OmniPCX Office Communication Server system to the ISDN digital public network or to private networks:

- PRA-T2, DASS2, DLT2: 30 x 64-Kpbs B-channels + 1 x 64-Kbps D-channel; 2048 Kbps.
- PRA-T1: 23 x 64-Kbps B-channels + 1 x 64-Kbps D-channel; 1544 Kbps
- T1-CAS: 24 x B-channels, including signalling; 1544 Kbps.
- PCM R2: 30 x 64 Kbps B-channels + 1 x 4 Kbps signalling channel; 2048 Kbps.

There are several connection options: T2 120-ohm symmetrical pairs and T1 100-ohm symmetrical pairs. A coaxial 75-ohm connection is available using an external adapter kit.



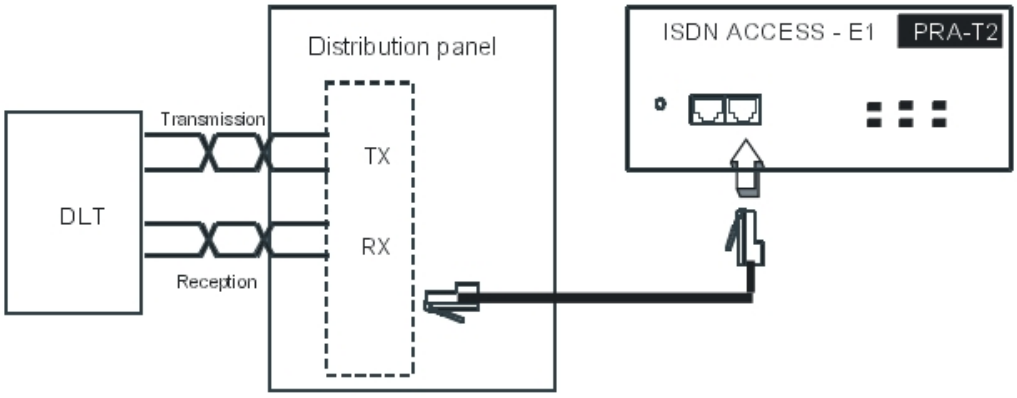
2.2.7.2 Hardware configuration

2.2.7.2.1 BOARD TYPE DEFINITION (CITROEN STRAPS)

The board type is defined by the Citroën strap solder:

- T2 (ex-factory) :no solders
- T1 : solder on strap 1
- T1-CAS : solders on straps 2 and 3
- DLT2 : solder on strap 2
- DASS2 : solder on strap 3
- PCM R2 : solder on strap 4

2.2.7.2.2 CONNECTION (120- OHM SYMMETRICAL PAIRS)



The PRA board is connected to a digital line termination (DLT) by 2 reinforced symmetrical pairs.

Cable impedance: 120 Ohms +/- 20% between 200 kHz and 1 MHz; 120 Ohms +/- 10% at 1 MHz.

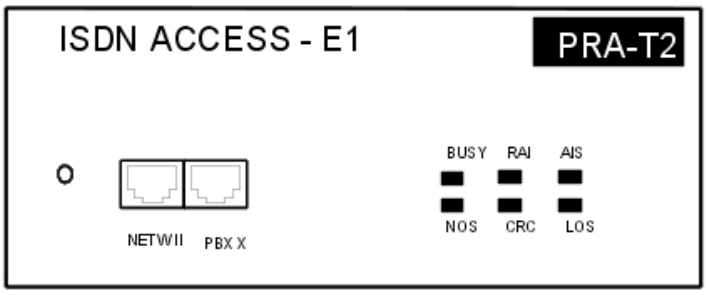
We recommend using an L120-series cable (or the L204 equivalent).

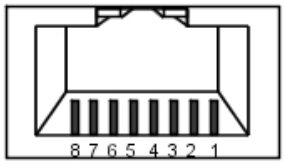
The distance T2-DLT is limited by the amount of loss between the DLT and T2, which must not exceed 6 dB at 1024 kHz.

2.2.7.3 External connections

2.2.7.3.1 OUTPUT PORTS (BOARD STIFFENER)

T2 board example





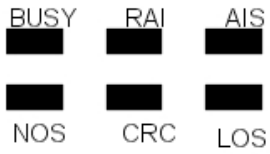
Female RJ45, front

RJ45 pin	1	2	3	4	5	6	7	8
NETW outputs	RX+	RX-		TX+	TX-			
PBX outputs	TX+	TX-		RX+	RX-			

NETW: connection to public network DLT.

PBX: network operation (QSIG).

2.2.7.3.2 ALARM LEDS



T2 Name	T1 Name	Feature
BUSY	BUSY	B-channels busy (red LED lights up if at least 1 B-channel is busy)
RAI (ATD)	RAI	Remote frame alarm (red LED lights up on alarm)
AIS (SIA2M)	AIS	Too many "1's in the 2-Mbit binary train (red LED lights up on alarm)
NOS (MS)	NSIG	Absence of 2-Mbit signal (red LED lights up on alarm)
CRC (TE)	CRC	CRC error (red LED lights up on alarm)
LOS (PVT)	NSYN	Loss of frame alignment (red LED lights up on alarm)

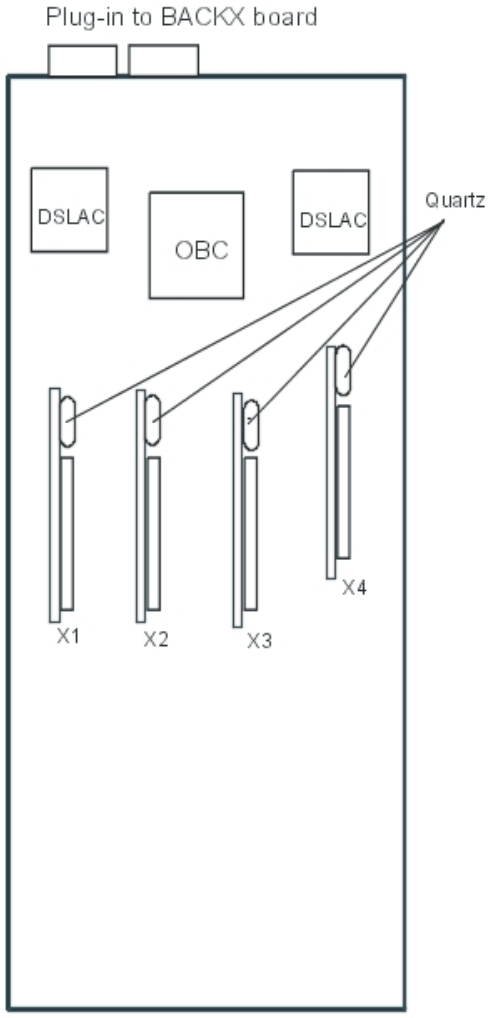
In parentheses: French abbreviations

2.2.8 ATA

2.2.8.1 Hardware description

The ATA (Analog Trunk Access) board serves to connect analog trunk lines (TL). 2 board versions are available:

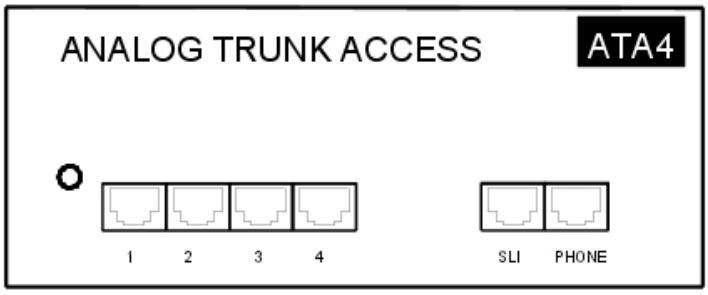
- ATA-2: 2 trunk lines
- ATA-4: 4 trunk lines

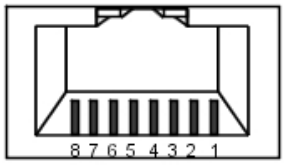


X1, X2, X3, X4 : plug-in connectors for MET daughter boards (pulse meter receivers); by referring against the quartz implanted on the MET daughter boards, the set up of these boards must follow the layout above.

2.2.8.2 External connections

2.2.8.2.1 OUTPUT PORTS (BOARD STIFFENER)



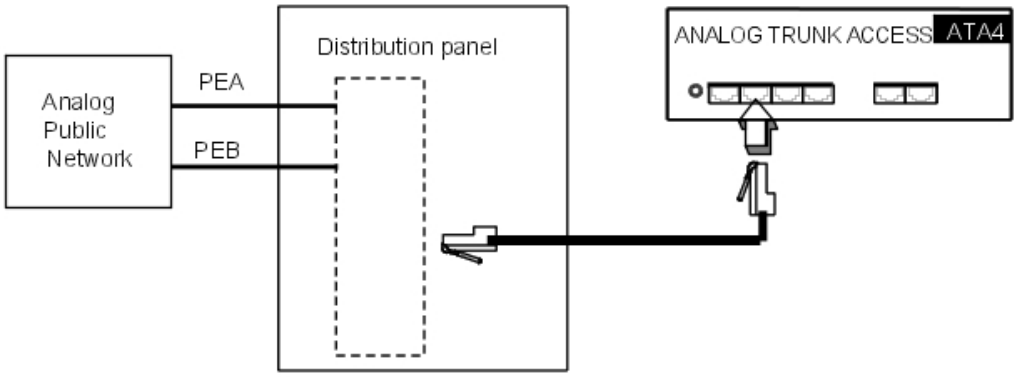


Female RJ45, front

RJ45 pin	1	2	3	4	5	6	7	8
Outputs 1 to 4				PEA	PEB			
SLI outputs				ZA	ZB			
PHONE outputs				ZSETA	ZSETB			

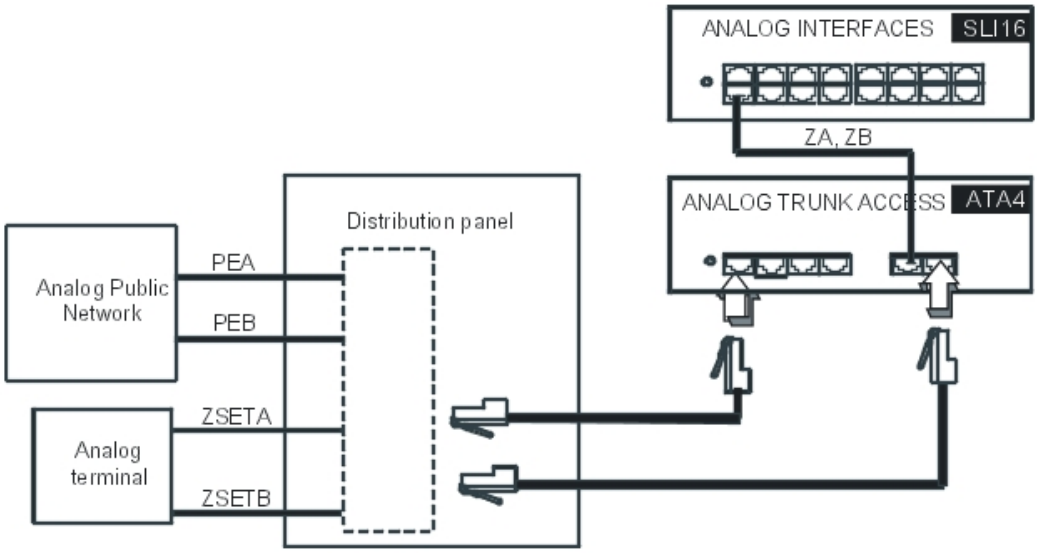
2.2.8.2.2 CONNECTING A TL

Without TL forwarding



With TL forwarding

In the event of a power cut or CPU failure, this solution forwards the analog line connected to device 1 on the ATA board to another analog set in the system.



2.2.9 ATA for UK Protocols

2.2.9.1 Overview

2.2.9.1.1 ADAPTATION TO UK PROTOCOLS

In accordance with the UK analogue public network, 2 types of ATA boards are available:

- ATA board (2 or 4 equipments) equipped with polarity inversion detectors.
- ATA LCG board (2 or 4 equipments) equipped with calibrated power failure detectors.

Protocol	Board type		Supported functionality	
	ATA	ATA LCG	Detection release of remote	Detection disconnect of remote
"Loop calling unguarded clear" protocol	YES	YES	NO	NO
"Loop calling guarded clear" protocol	NO	YES	YES	NO
IP protocol	YES	NO	NO	YES

2.2.10 MIX

2.2.10.1 Hardware description

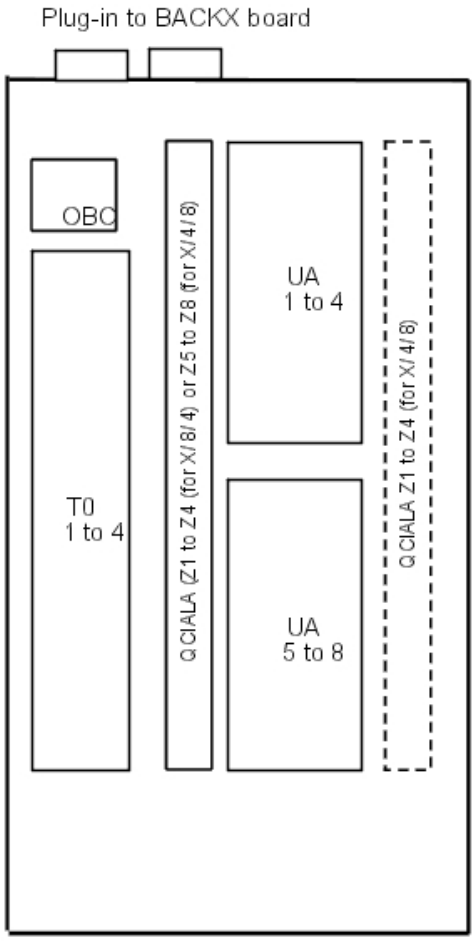
The MIX (Mixed Lines) board serves to connect ISDN basic accesses (T0), digital stations (UA) and 2-wire analog terminals (Z). 6 board versions are available:

- MIX244: 2 T0 accesses, 4 UA interfaces and 4 Z interfaces
- MIX484: 4 T0 accesses, 8 UA interfaces and 4 Z interfaces
- MIX448: 4 T0 accesses, 4 UA interfaces and 8 Z interfaces

- MIX044: 4 UA interfaces and 4 Z interfaces
- MIX084: 8 UA interfaces and 4 Z interfaces
- MIX048: 4 UA interfaces and 8 Z interfaces
- MIX248: 2 T0 accesses, 4 UA interfaces and 8 Z interfaces
- MIX284: 2 T0 accesses, 8 UA interfaces and 4 Z interfaces

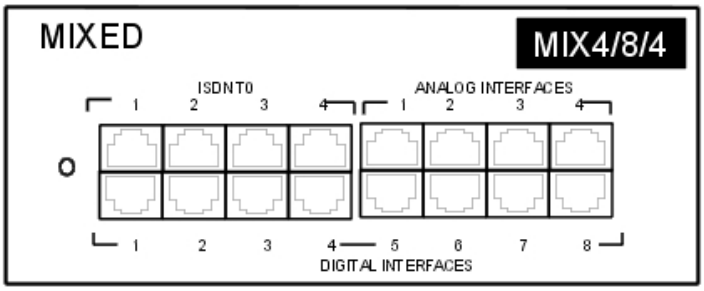
Note:
Contrary to the BRA board, the MIX board's T0 accesses cannot be configured as DLT0 Network. Only DLTO User is allowed in QSIG mode.

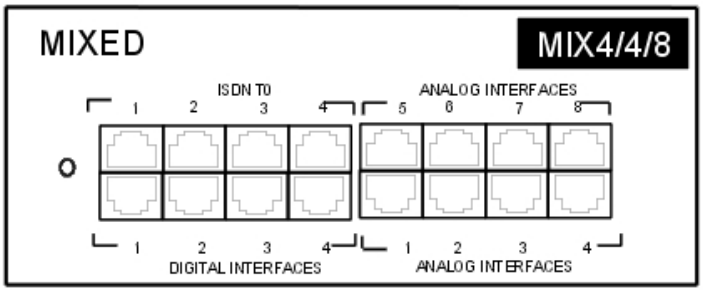
Example: MIX484 board

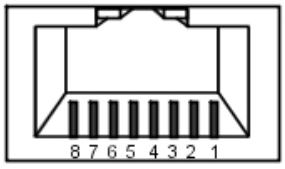


2.2.10.2 External connections

2.2.10.2.1 OUTPUT PORTS (FACEPLATE)







Female RJ45, front

RJ45 pin	1	2	3	4	5	6	7	8
Z outputs				ZA	ZB			
UA outputs				L1	L2			
T0 outputs			TX+	RX+	RX-	TX-		

2.2.10.2.2 CONNECTING AN ANALOG STATION (Z)

Follow the rules in the "SLI board" section.

2.2.10.2.3 CONNECTING A DIGITAL STATION

Follow the rules in the "UAI board" section.

2.2.10.2.4 CONNECTING A T0 BASIC ACCESS

Follow the rules in the "BRA board" section.

2.2.11 Mini-MIX

2.2.11.1 Basic description

The Mini–MIX daughter board, available since R510 on Compact Edition 2nd Generation is an optional daughter board plugged on the CPU-3m or CPU-4 board.

It has the following features:

Two T0 (ISDN Basic Rate Access) interfaces

Two Z (SLI Analog Extension Access) interfaces

One local OBC to handle initialization and low level signalling

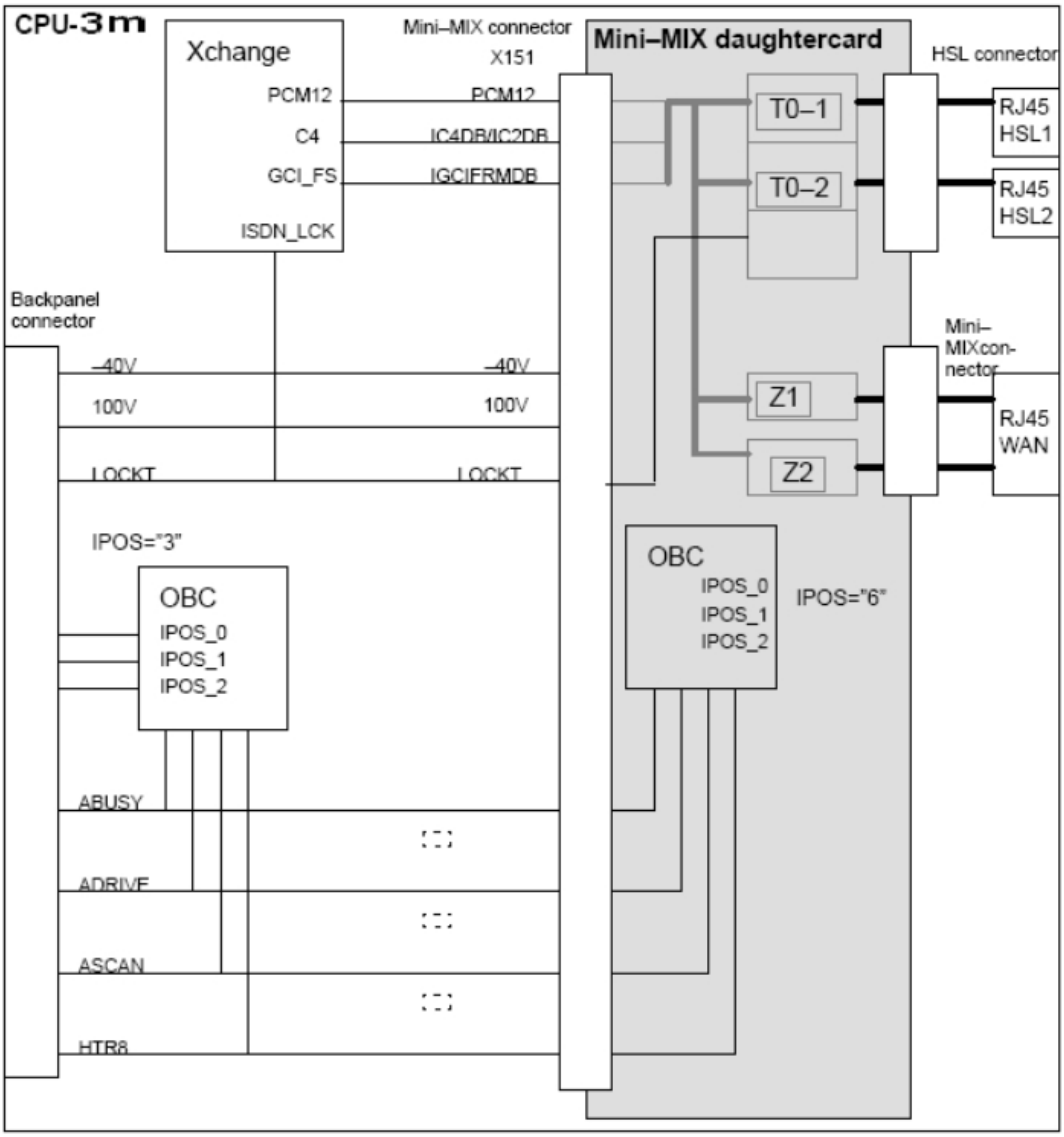


Figure 2.57 : The Mini-MIX daughter board

The Mini–MIX is detected via ASL (just like a peripheral board).

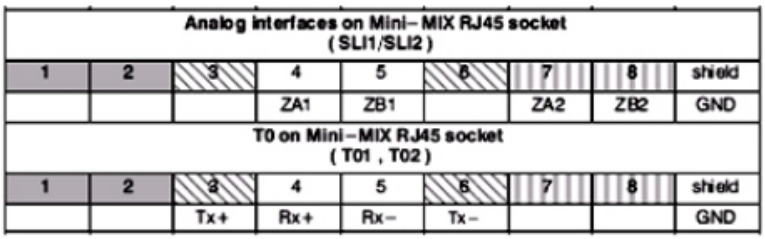
The Mini–MIX is located on position “6” (fixed) of ASL0. Position “6” of ASL0 is not used on the CE , S and M models.

The Mini–MIX drives the Mini–MIX led (previously WAN led) on the front stiffener.

LED “ON” indicates that:

- the Mini–MIX daughter board is present and accepted by the mixed board licence,

- the Backpanel supports 100V distribution (PSTYPE=”0”).



Analog interfaces on Mini–MIX RJ45 socket (SLI1/SLI2)								
1	2	3	4	5	6	7	8	shield
			ZA1	ZB1		ZA2	ZB2	GND
T0 on Mini–MIX RJ45 socket (T01 , T02)								
1	2	3	4	5	6	7	8	shield
		Tx+	Rx+	Rx–	Tx–			GND

Figure 2.58 : RJ45 Assignment Table

Inter–connections between the Mini–MIX and the CPU–3m (or CPU-4) are made through 2BergStak connectors (already used for daughter boards AFU, HSL, etc.)

The Mini–MIX is dedicated to the new CE product (evolution to IP product).

The CE cabinet must be equipped with the new BACKXS, which provides +100V to the CPU slot.

2.2.12 AMIX-1

2.2.12.1 Hardware description

The AMIX-1 (Analogue Mixed Line) board is used to connect the analogue public network (PSTN) to the PBX. It has the following characteristics:

- 4 analogue line accesses
- a maximum of 8 UA interfaces
- a maximum of 8 Z interfaces
- an OBC system interface supporting AT, Z and UA signalling
- protection features
- the PFCT (Power Failure Cut Through) feature which allows a local analogue set to connect directly to a network line in the event of a power cut or a software failure

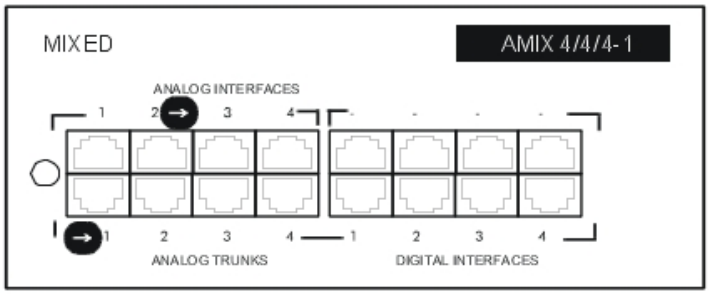
Note:
The AMIX-1 board is required to connect the Alcatel-Lucent OmniPCX Office Compact Edition modules to the analogue public network (PSTN). It can be used for modules 1, 2 and 3.

The AMIX-1 board can take the following 2 daughter boards:

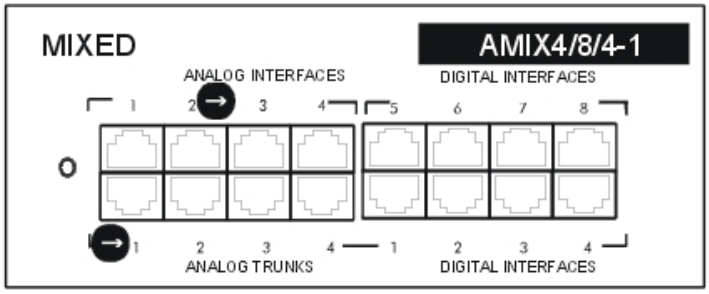
- GSCLI
- CLIDSP

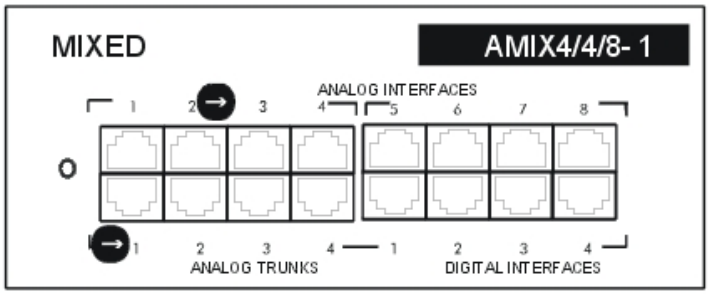
2.2.12.2 External connections

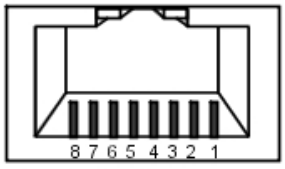
2.2.12.2.1 OUTPUT PORTS (FACEPLATE)



: indicates the assignment ports for the PFCT (Power Failure Cut Through) feature: the Z2 plug is connected to a Z set, the AT1 plug to the PSTN.







Female RJ45, front

RJ45 pin	1	2	3	4	5	6	7	8
AT outputs				AT_B_RING	AT_A_TIP			
UA outputs				UA_a	UA_b			
Z outputs				Z_a	Z_b			

2.2.12.2.2 CONNECTING AN ANALOG STATION (Z)

For more information, refer to the SLI board document.

2.2.12.2.3 CONNECTING ADIGITAL STATION

For more information, refer to the UAI document.

2.2.13 UAI

2.2.13.1 Hardware description

The UAI board allows the connection of digital stations (UA). Two board versions are available:

- boards without external power supply capability:
  - UAI4: 4 UA interfaces
  - UAI8: 8 UA interfaces
  - UAI16: 16 UA interfaces
- boards with external power supply capability:
  - UAI16-1: 16 UA interfaces

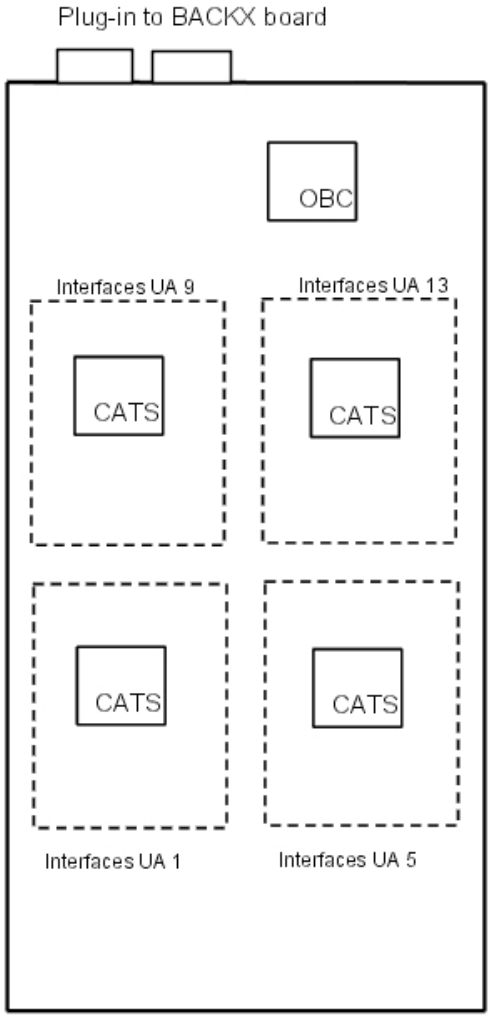
2.2.13.1.1 Differences between the two boards

The UAI16-1 board is equipped with 2 ASICs OSIRIS while the UAI4/8/16 boards are equipped with ASICs CATS (one ASIC OSIRIS replaces 2 ASICs CATS).

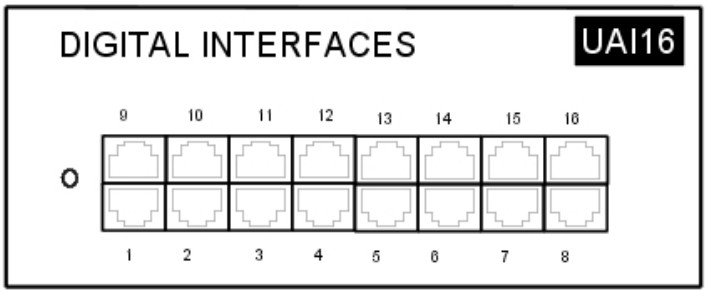
The system software detects whether the board is equipped with CATS or OSIRIS; if the ASIC OSIRIS is detected, the software can also detect whether the board is connected to an external power supply.

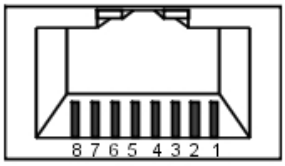
The UAI-16 board allows to remotely supply the terminals connected to the 16 interfaces from a EPS48 external power supply connected to interface 1 using an external adaptation power cable (splitter).

2.2.13.1.2 BOARDS UAI4, UAI8 and UAI16



Output ports (Faceplate)

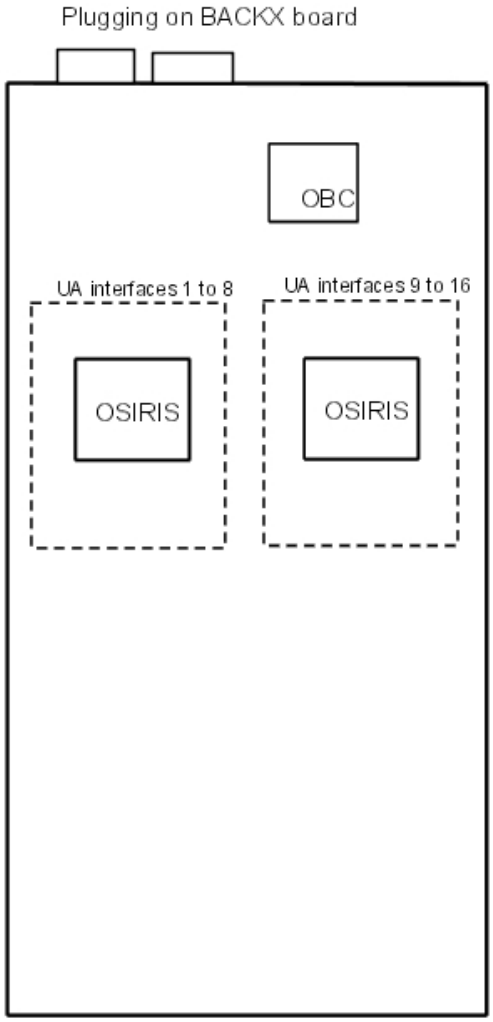




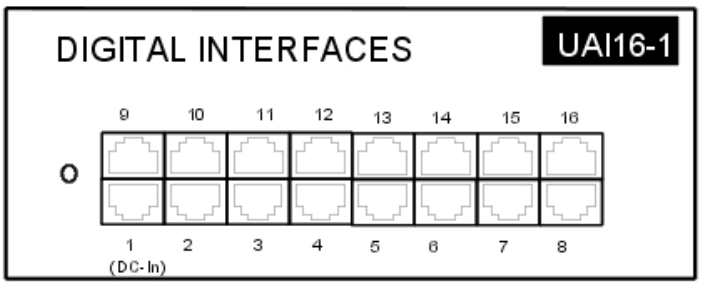
Female RJ45, front

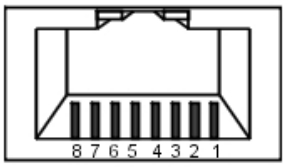
RJ45 pin	1	2	3	4	5	6	7	8
Sorties				L1	L2			

2.2.13.1.3 UAI16-1 board



Output ports (Faceplate)





Female RJ45, front

RJ45 pin	1	2	3	4	5	6	7	8
Outputs 1				L1	L2		0V	+48 V
Outputs 2 to 16				L1	L2			

2.2.13.2 External connections

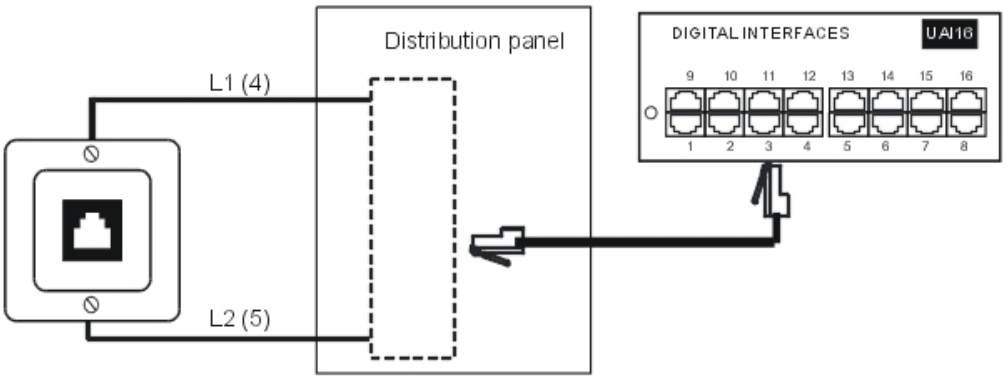
2.2.13.2.1 CONNECTING A DIGITAL STATION

Connection without external power supply

The terminals are equipped with a cable and a self-acting switch that plugs into the wall socket. Each terminal is connected up by a pair of 0.5 or 0.6 mm diameter wires.

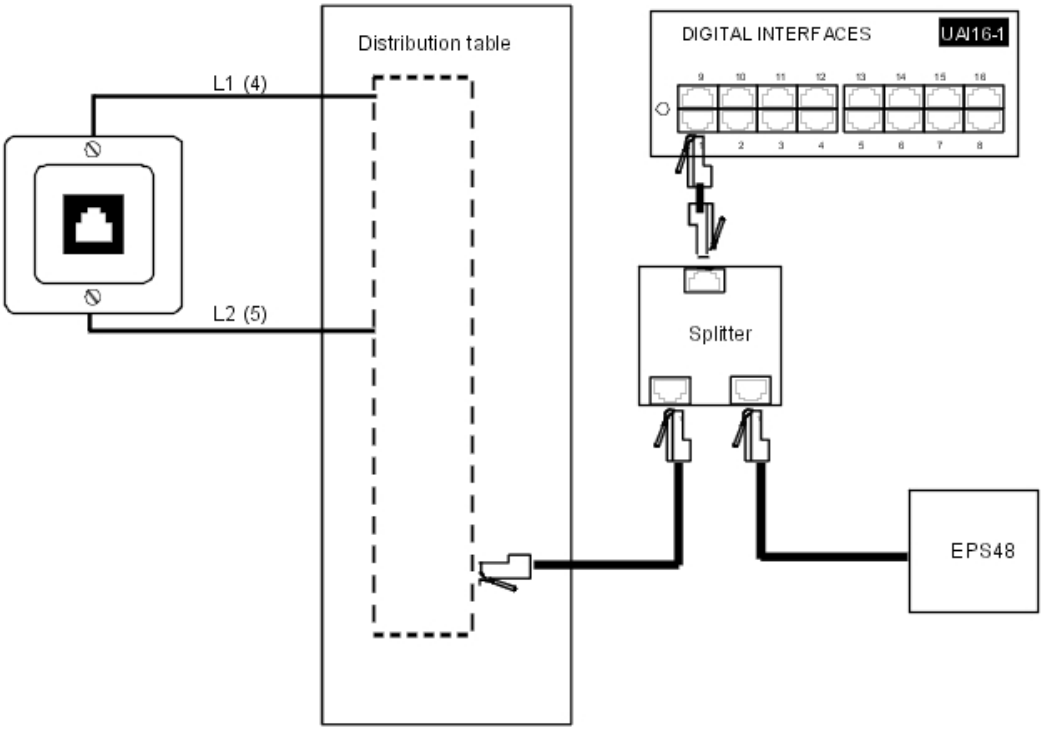
System - Digital station distances:

- 0.5 mm SYT type cable: 800 m (station without option) or 600 m (station with S0 or Z option)
- 0.6 mm 278 type cable: 1,200m (station without option) or 850m (station with S0 or Z option)



Connection with external power supply

A splitter allows the separation of the UA peripheral connection and the EPS48 external power supply.



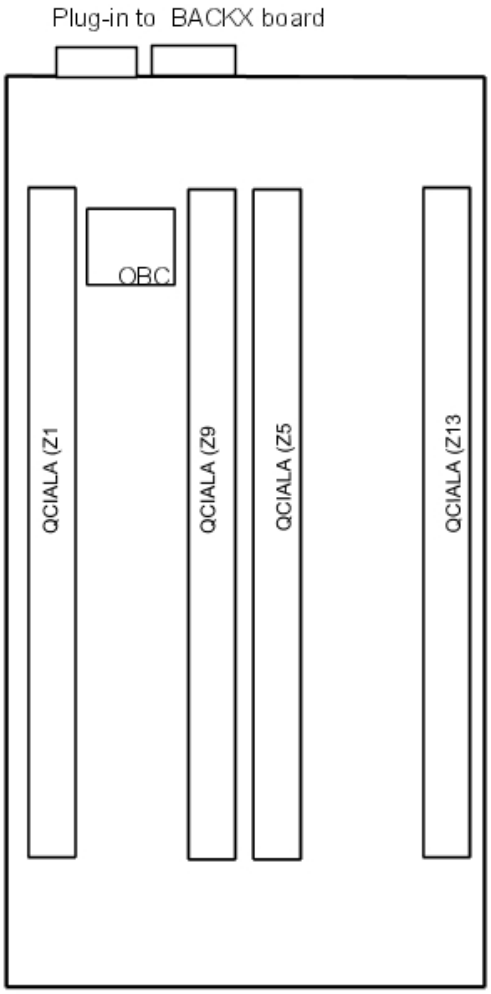
2.2.14 SLI

2.2.14.1 Hardware description

The SLI or SLI-1 board (Single Line) allows the connection of 2-wire analog terminals (Z). 3

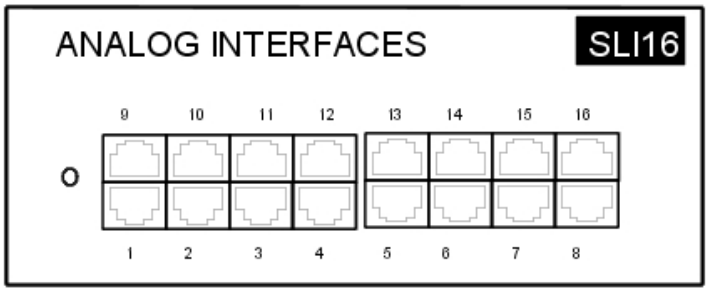
board versions are available:

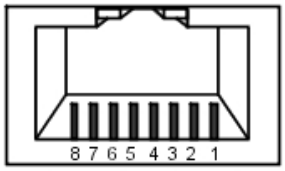
- SLI4: 4 Z interfaces
- SLI8: 8 Z interfaces
- SLI16: 16 Z interfaces



2.2.14.2 External connections

2.2.14.2.1 OUTPUT PORTS (BOARD STIFFENER)



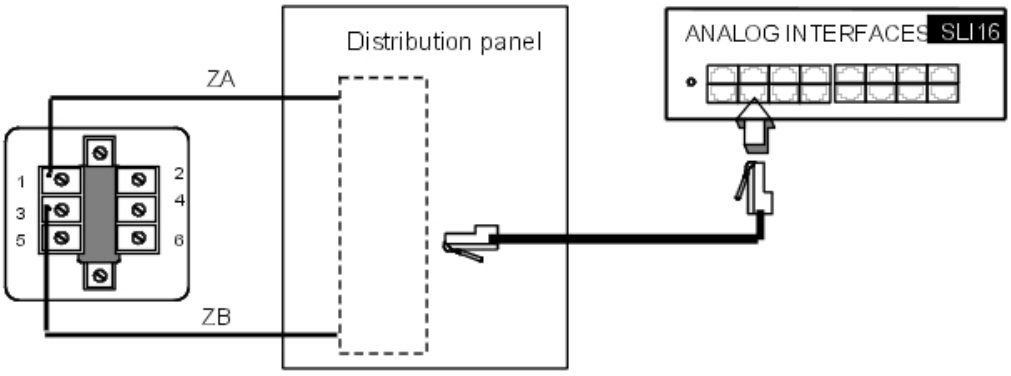


Female RJ45, front

RJ45 pin	1	2	3	4	5	6	7	8
Outputs				ZA	ZB			

2.2.14.2.2 CONNECTING AN ANALOG Z STATION

The terminals are equipped with a cable and a self-acting switch that plugs into the wall socket. Each set is connected up with a pair of 0.5 or 0.6-mm wires (the maximum distance with 0.5-mm cabling is 1.3 km).

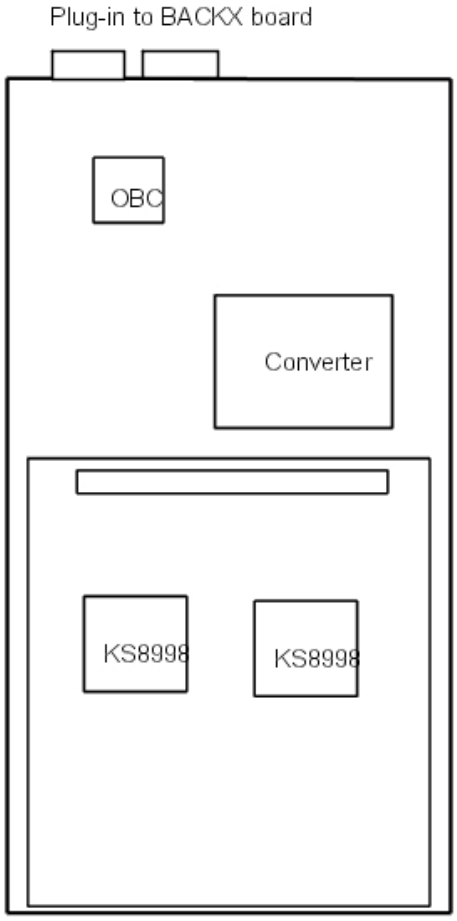


2.2.15 LANX

2.2.15.1 Hardware description

The LanX board (Ethernet LAN Switch) serves to connect Ethernet terminals (IEEE 802.3 compatible). 3 board versions are available:

- **LanX8**
  8 10/100 BT Ethernet ports (ports 1 to 7: MDI-X/crossover; Uplink: MDI-II/straight link)
- **LanX16**
  16 10/100 BT Ethernet ports (ports 1 to 15: MDI-X/crossover; Uplink: MDI-II/straight link)
- **LANX16-1**
  16 10/100 BT Ethernet ports (ports 1 to 15: MDI-X/crossover; Uplink: MDI-II/straight link); low consumption. Contrary to the LANX8 and LANX16 boards that are seen by the system as CPU boards, this LanX16-1 board, under a 40 V tension, is seen as an interface board (such as UAI, SLI, etc.) and thus allows the limit number of usable boards to be increased; in order to find out the limit values by module type, see the "Capacities and limits" sheet.

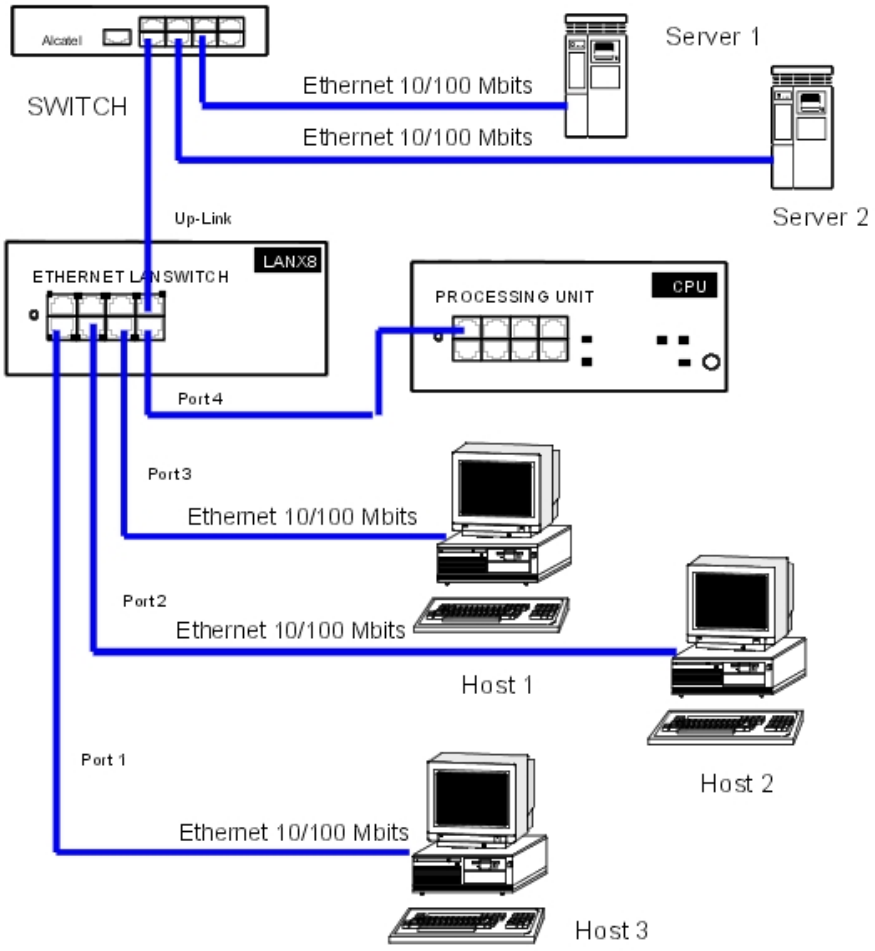


2.2.15.1.1 LANX-2 boards

The LanX8-2 and LanX16-2 are second generation boards integrating respectively 1 or 2 Ethernet Gigabit ports for a Lanswitch/Layer 2 configuration. Any port can be used as an Uplink, as all the ports are auto MDI/MDIX.

2.2.15.2 Configuration examples

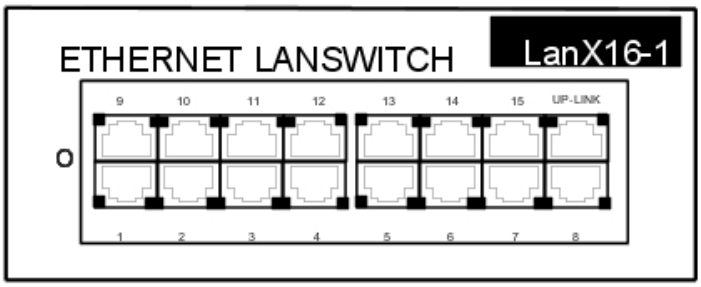
2.2.15.2.1 CONFIGURATION EXAMPLE

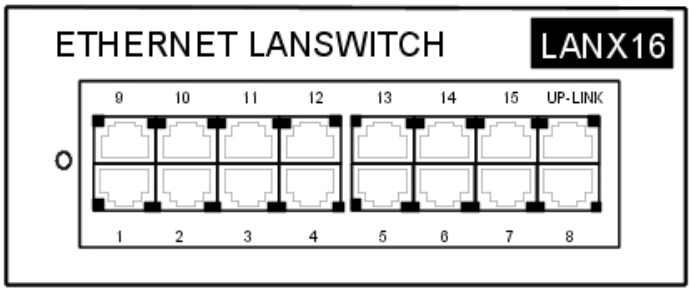


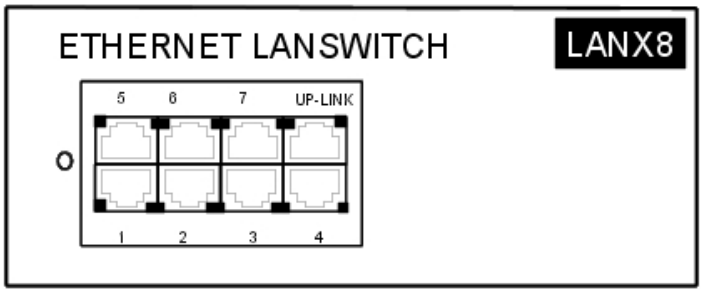
2.2.15.3 External connections

2.2.15.3.1 OUTPUT PORTS (BOARD STIFFENER)

LANX boards

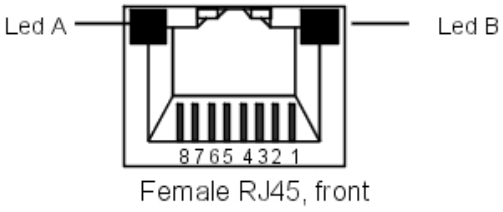






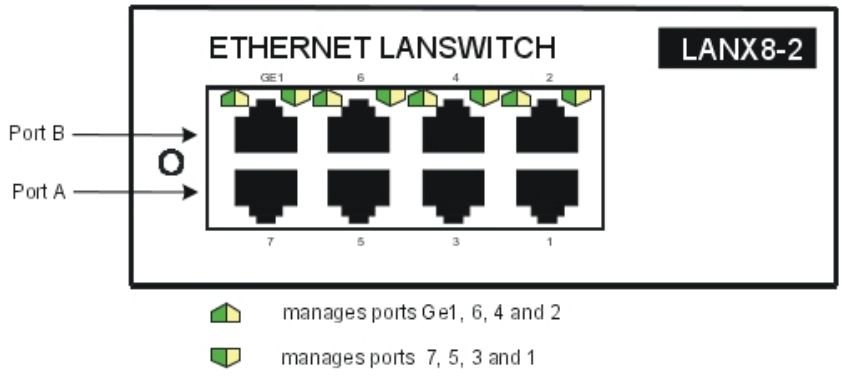
Each category-5 RJ45 connector has 2 green LEDs:

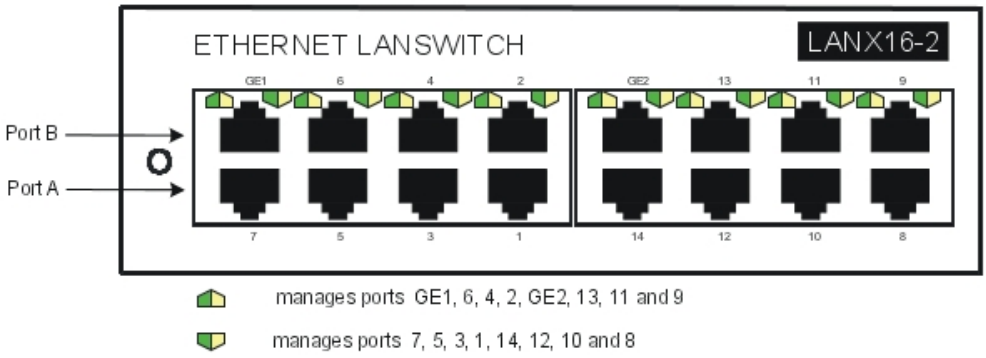
- LED A = link status and activity:
  - LED off: link disconnected
  - LED steady: link connected
  - LED flashing: link active
- LED B = full duplex/collision:
  - LED out: half Duplex
  - LED steady: full Duplex
  - LED flashing: collision:



RJ45 pin	1	2	3	4	5	6	7	8
Port outputs (ports 1 to 15)	RX+	RX-	TX+			TX-		
Up-Link output	TX+	TX-	RX+			RX-		

LANX-2 board





Unlike the first generation boards, the LEDs of the A and B ports are both located at the top of the board. The LED display is as follows:

- Green LED (left) = link status and activity:
  - LED off: link disconnected
  - LED steady: link connected
  - LED flashing: link active
- Yellow LED (right) = speed:
  - off: low speed (10 or 100 Mb for Gigabit port, 10 Mb for the other ports)
  - on: high speed (1 Gb for Gigabit port, 100 Mb for the other ports)

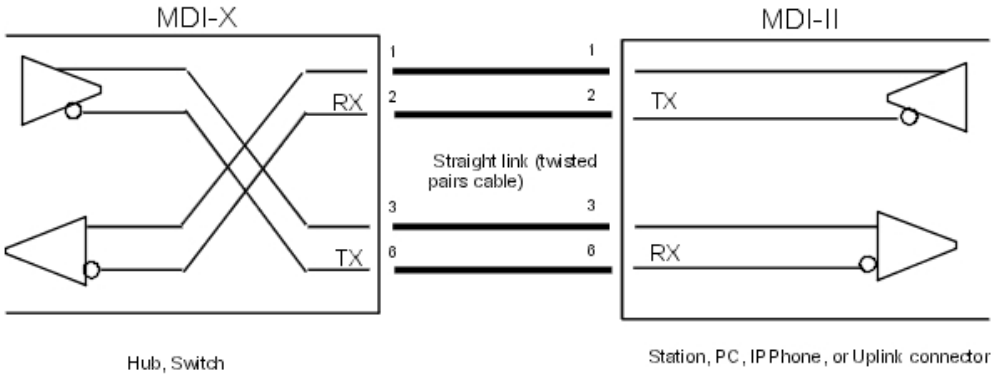
LANX-2 board

RJ45 pin	1	2	3	4	5	6	7	8
Ports 1 to 14	RX+	RX-	TX+			TX-		
GE1, GE2	TR0+	TR0-	TR1+	TR2+	TR2-	TR1-	TR3+	TR3-

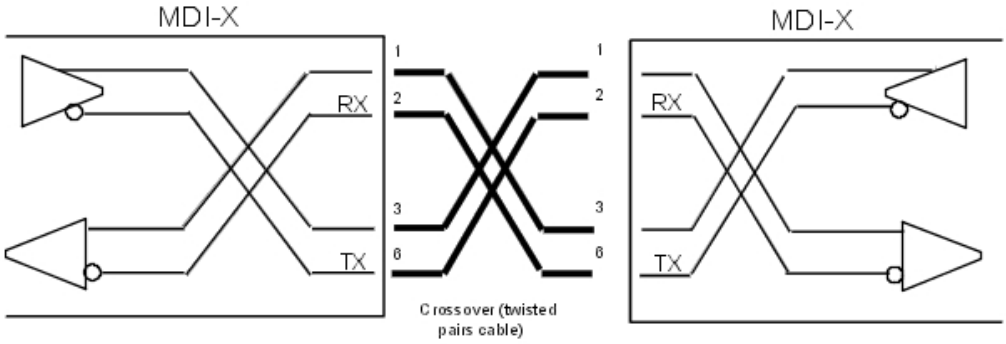
- Port 1 to 14: 10/100 BT ports.
- GE1, GE2: 10/100/1000 BT ports.

2.2.15.3.2 CONNECTION PRINCIPLES

Basic 10/100 BT connection



MDI-X to MDI-X connection



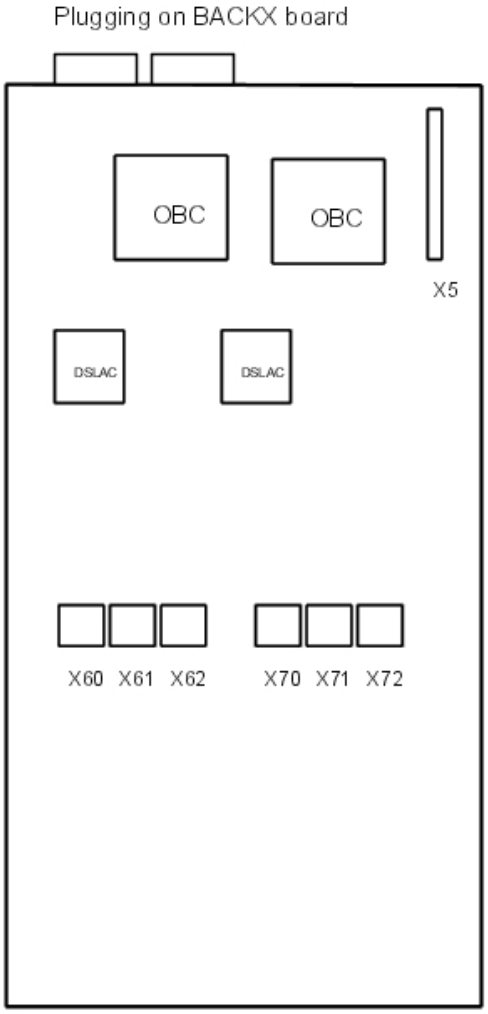
2.2.16 APA

2.2.16.1 Hardware description

The APA boards can only be used on systems running a software version posterior to R2.0.

The APA board (Analogue Public Access) allows the connection of analogue trunk lines (LR). Two board versions are available:

- APA-4: 4 TL interfaces
- APA-8: 8 TL interfaces



X5: CLIDSP daughterboard plugging connector (detection of CLIP signal).

X60, X61, X62, X70, X71, and X72: GSCLI daughterboards plugging connectors (Ground Start signalling).

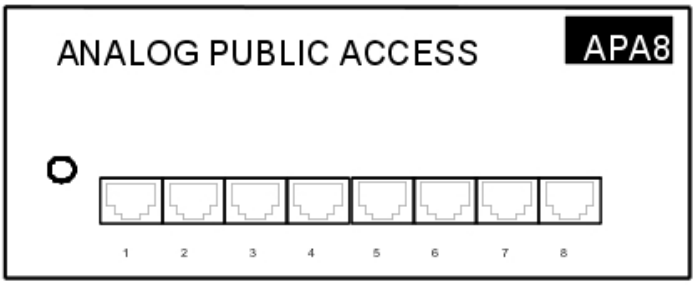
2.2.16.1.1 CLIDSP BOARD EQUIPMENT

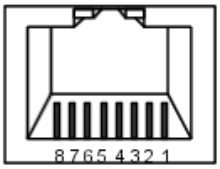
The signal needed to manage the CLIP (Calling Line Identification Presentation) is generated at the CPU board level except in the following cases, which require a CLIDSP board (to be installed on connector X5 of the board): US, UK and all countries using only Dual Tone (DT-AS) as alert signal.

The CLIDSP board will also be necessary to detect the CLIP in the on-hook state (later phase).

2.2.16.2 External connections

2.2.16.2.1 OUTPUT PORTS (FACEPLATE)





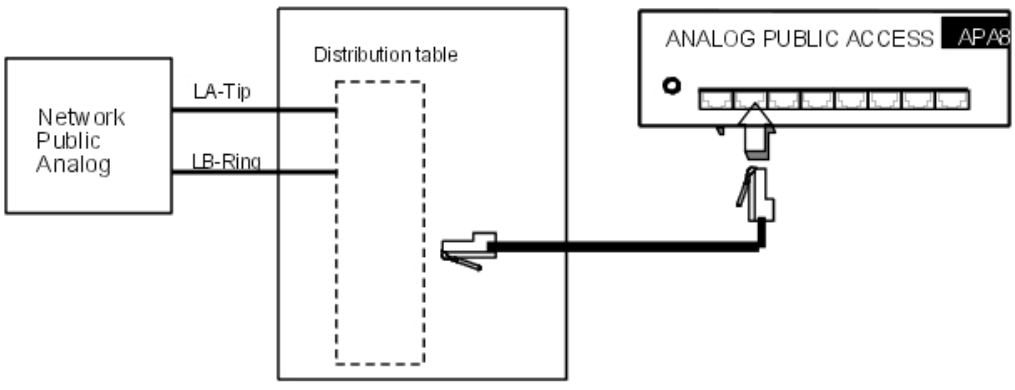
Front panel female RJ45

RJ45 pin	1	2	3	4	5	6	7	8
Output1	ZSETB	ZSETA		LB-Ring	LA-Tip		ZB	ZA
Outputs 2 to 8				LB-Ring	LA-Tip			

Note:
Z set B1 and Z set A1: connection to Z set for cut-through functionality. ZB1 and ZA1: connection to a Z access for cut-through functionality.

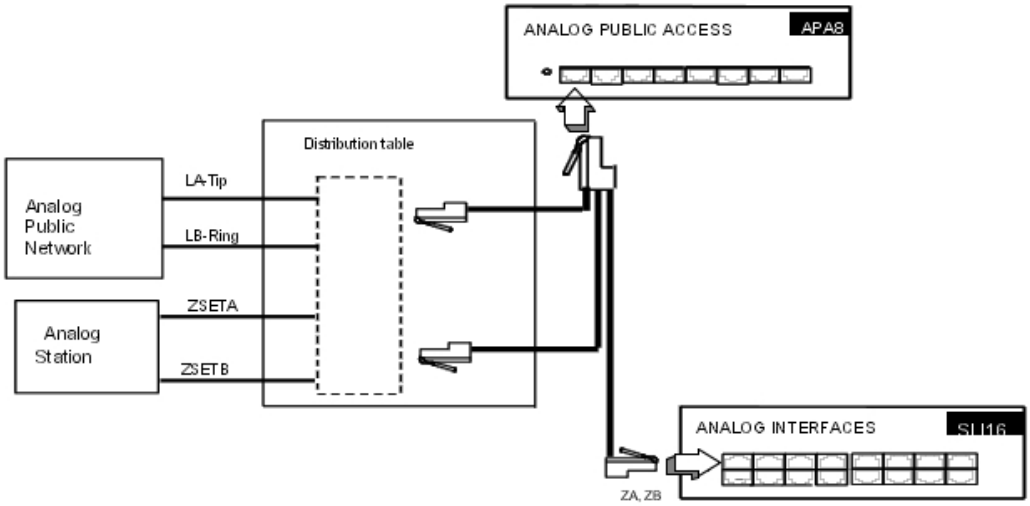
2.2.16.2.2 CONNECTING A TL

Without TL forwarding



With LR forwarding

In the event of power failure or CPU malfunction, this solution allows connection of the analogue line (connected to the APA board's equipment 1) to an analogue station.



Note:

US connection features

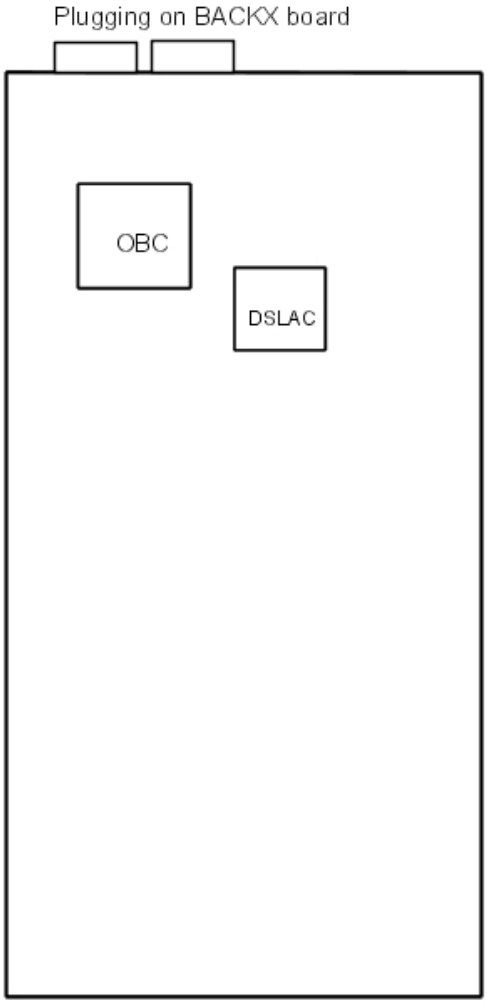
- **APA board equipped with Ground Start signalling:** Ring is connected to the network's + polarity while Tip is connected to the - (ground if using conventional battery).
- **APA board equipped with Loop Start signalling:** In case of conventional battery, Tip is normally connected to the network equipment's ground and Ring to the network's - polarity. Nevertheless, maintenance operations may temporarily or permanently inverse these polarities: the connection of each of the battery's terminals to the earth cannot be ensured. In the case of va riable battery, no terminal is connected to ground: the Tip and Ring outputs are variable.

2.2.17 DDI

2.2.17.1 Hardware description

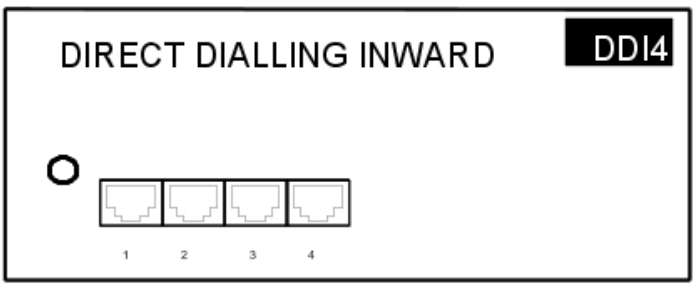
The DDI board (Direct Dialling Inward) allows the connection of analogue trunk lines with Multiple Subscriber Numbers. 2 board versions are available:

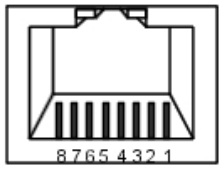
- DDI-2: 2 SDA interfaces
- DDI-4: 4 SDA interfaces



2.2.17.2 External connections

2.2.17.2.1 OUTPUT PORTS (BOARD STIFFENER)

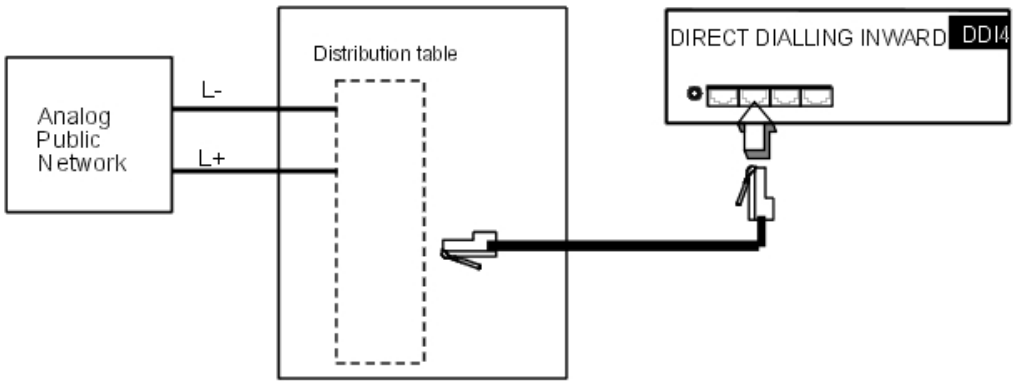




Front panel female RJ45

RJ45 pin	1	2	3	4	5	6	7	8
Outputs				L-	L+			

2.2.17.2.2 CONNECTING AN SDA LINE



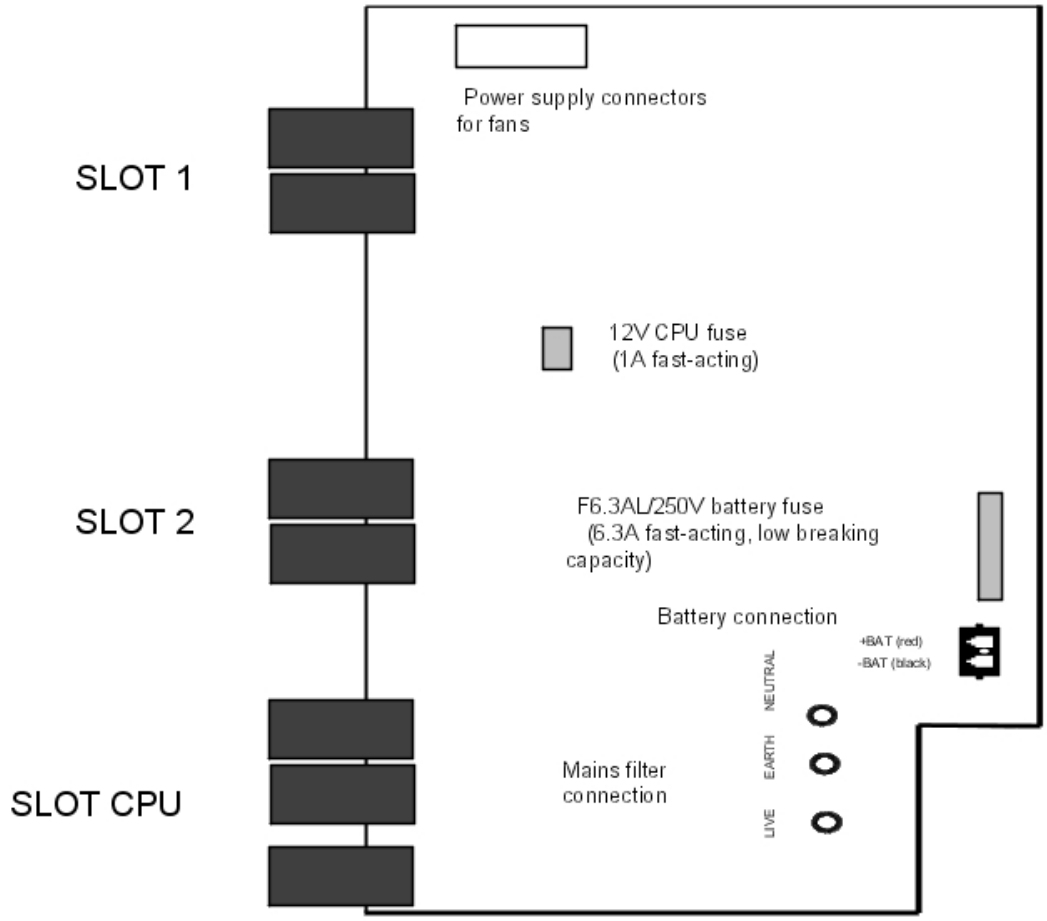
2.2.18 Power Supplies

2.2.18.1 Hardware description

Power supplies of the PSxN family are mandatory when the system is equipped with a PIII CPU board.

2.2.18.1.1 POWER SUPPLY PS1/PS1N

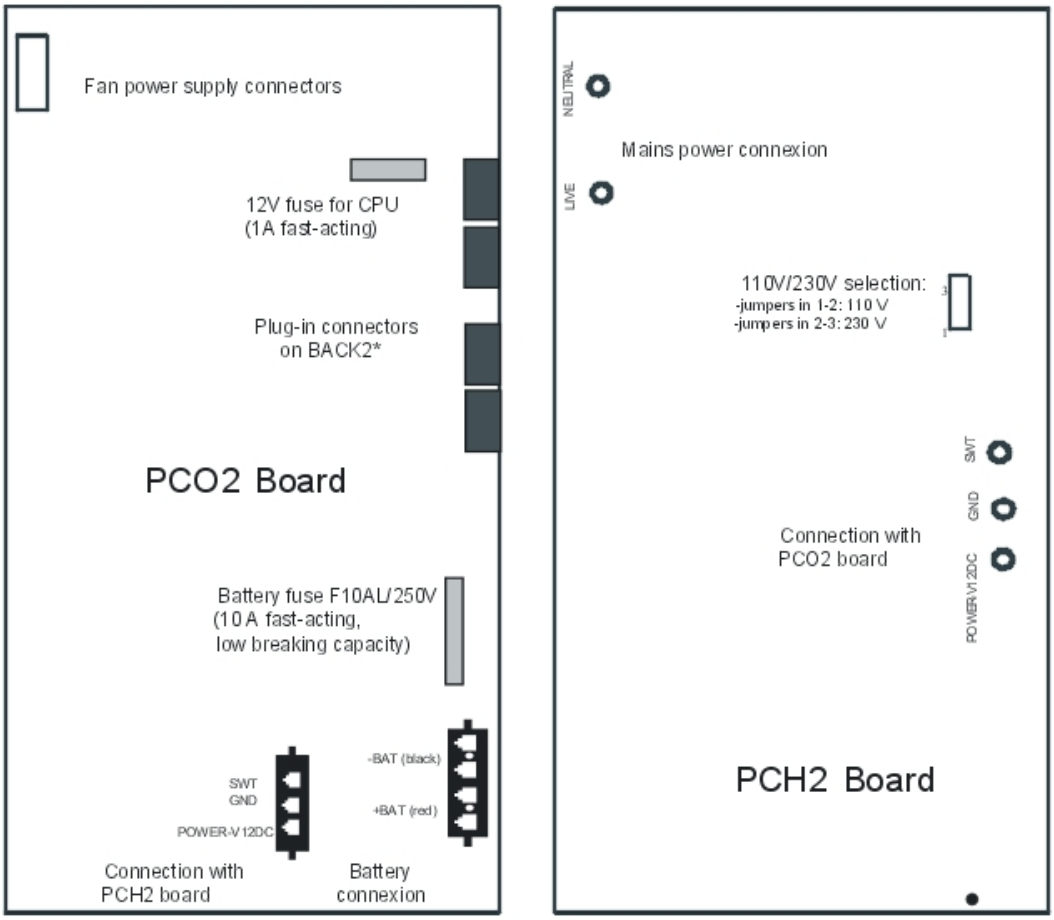
Power supply PS1/PS1N provides the different voltages required to operate a RACK S (former RACK 1) module and also acts as a backplane board (slots 1, 2 and CPU).



2.2.18.1.2 POWER SUPPLY PS2/PS2N

Power supply PS2/PS2N, which provides the different voltages required to operate a RACK M (former RACK 2) module, consists of 2 boards:

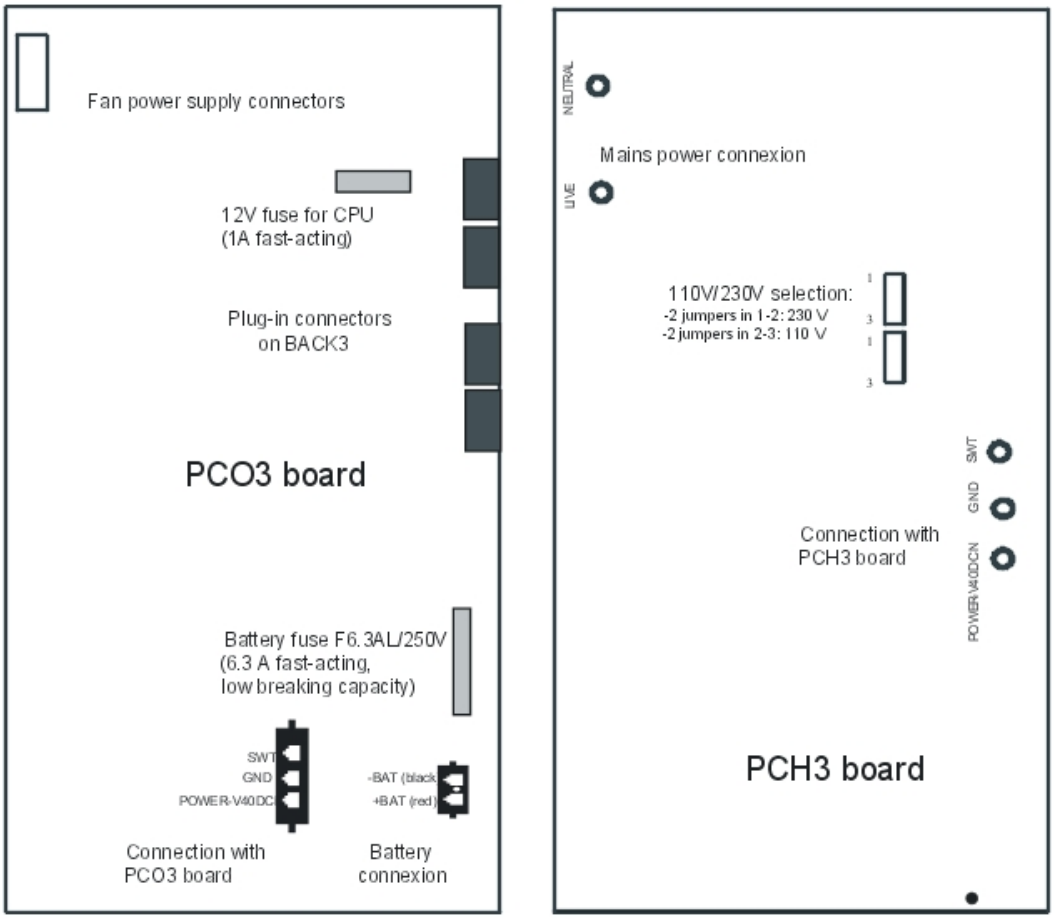
- PCH2: charger board
- PCO2: converter board



2.2.18.1.3 POWER SUPPLY PS3/PS3N

Power supply PS3/PS3N, which provides the different voltages required to operate a RACK L (former RACK 3) module, consists of 2 boards:

- PCH3: charger board
- PCO3: converter board



2.2.18.1.4 BATTERIES

Equipment:

- RACK S (former RACK 1): 1 battery
- RACK M (former RACK 2): 2 batteries mounted in parallel
- RACK L (former RACK 3): 3 batteries mounted in series

Battery characteristics:

- sealed lead battery
- 1.2 Ah / 12 V
- fire resistance better than or equal to UL94-V2

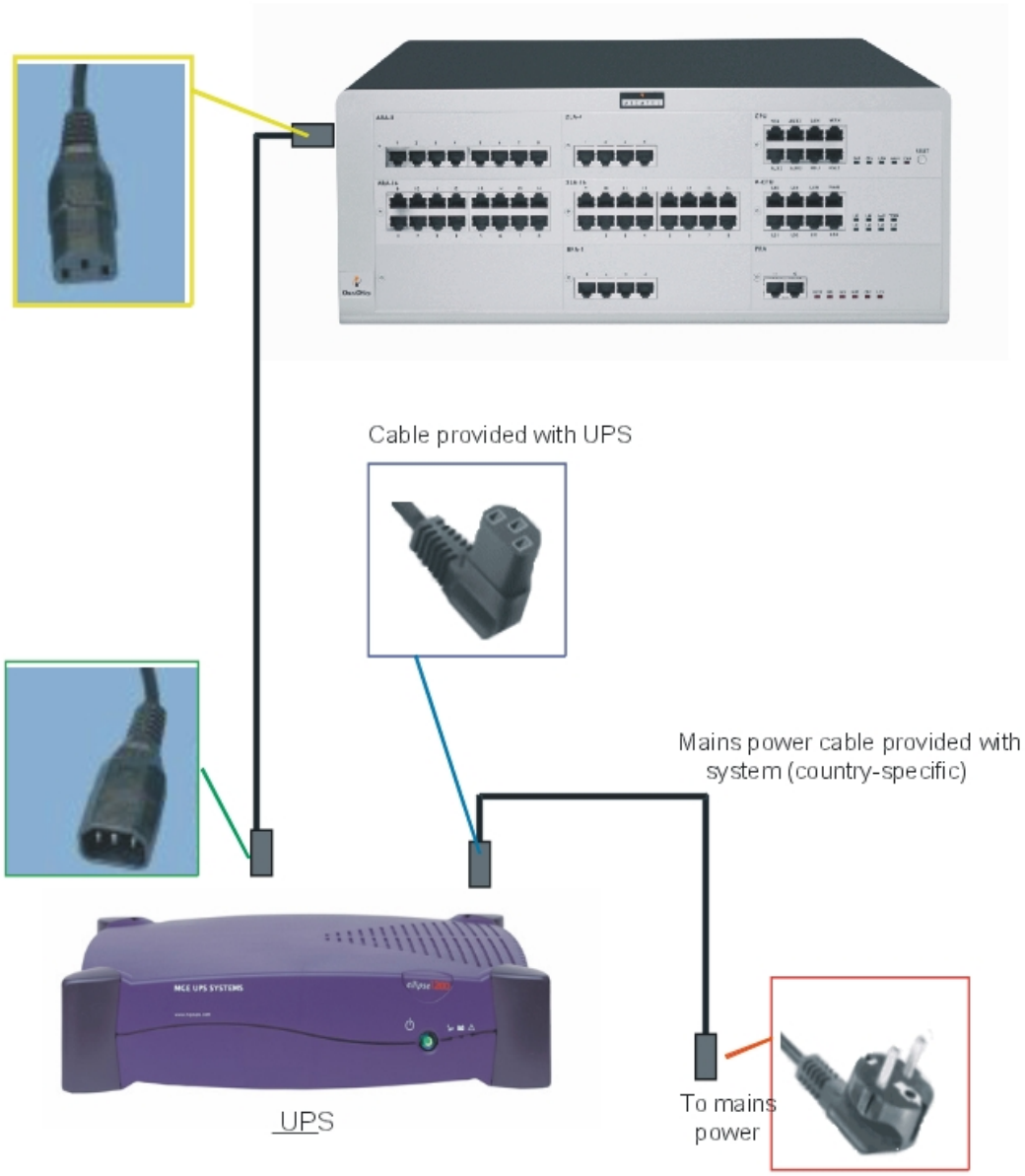
Maintenance:

To guarantee system shutdown without data loss in the event of a mains power failure, or if the mains plug is unplugged at the wall socket, replace the batteries every two years. This maintenance operation is vital to guarantee sufficient power autonomy to allow the files to be saved before the system shuts down.

In the case of only a voice module (without Hard Disk or CoCPU board), the standalone time is approximately 20 minutes.

2.2.18.1.5 UPS

A UPS (Uninterruptible Power Supply) is recommended because it increases the backup time provided by the system's batteries. A maximum of 2 Alcatel-Lucent OmniPCX Office Communication Server modules can be connected to a UPS.



Equipment:

The following table indicates compatible UPS models to use with each Alcatel-Lucent OmniPCX Office Communication Server system for a power autonomy of about 1 hour (40 minutes for the XL model used with a standard configuration):

System	UPS 220 V	UPS 110 V
Alcatel-Lucent OmniPCX Office Communication Server model S	Pulsar ellipse 300	Pulsar ellipse 300 USB

Alcatel-Lucent OmniPCX Office Communication Server model M	Pulsar ellipse 650S	Pulsar ellipse 650 RS232
Alcatel-Lucent OmniPCX Office Communication Server model L	Pulsar ellipse 1200S	Pulsar ellipse 1200 RS232
Alcatel-Lucent OmniPCX Office Communication Server model XL	Pulsar ellipse 1200S	Pulsar ellipse 1200 RS232

Choice of UPS:

The following table indicates for each Alcatel-Lucent OmniPCX Office Communication Server system (in extreme configurations) the consumption that is used to choose a UPS from the various models offered by UPS manufacturers:

System	Configuration	Primary consumption
Alcatel-Lucent OmniPCX Office Communication Server model S	24 terminals	50 W
	12 terminals + 1 CoCPU board	55 W
Alcatel-Lucent OmniPCX Office Communication Server model M	48 terminals	70 W
	48 terminals + 1 CoCPU board	85 W
Alcatel-Lucent OmniPCX Office Communication Server model L	96 terminals	105 W
	96 terminals + 1 CoCPU board	120 W
Alcatel-Lucent OmniPCX Office Communication Server model XL	192 terminals	210 W
	192 terminals + 2 CoCPU boards	230 W

2.2.18.1.6 EPS48 EXTERNAL POWER SUPPLY

The EPS48 external power supply (48V - 1A) is designed to power the new UAI16-1 boards, thus enabling the connection of power-hungry peripherals without a need for another module or a bigger module.

Plugged into the electrical power supply, a 2 m power cable with an 8-pin RJ45 connector powers the splitter used with the UAI16-1 board.

A green lamp indicates voltage.

The EPS48 external power supply's connection into the main power supply must be located as close as possible to the system and be easily accessible.

Output Points:

RJ45 pin	1	2	3	4	5	6	7	8
Outputs							0V	48 V

2.3 Dedicated Sets

2.3.1 IP Touch 4008/4018 Phone

2.3.1.1 Basic description

2.3.1.1.1 Overview

The Alcatel-Lucent OmniPCX Office Communication Server supports (among others) the following types of IP-Phones:

- In the Alcatel-Lucent 8 series product range: the Alcatel-Lucent IP Touch 4008 Phone
- In the Alcatel-Lucent IP Touch 8 series phone Extended Edition product range: the Alcatel-Lucent IP Touch 4008 phone Extended Edition
- In the Alcatel-Lucent 8 series product range: the Alcatel-Lucent IP Touch 4018 Phone
- In the Alcatel-Lucent IP Touch 8 series phone Extended Edition product range : the Alcatel-Lucent IP Touch 4018 phone Extended Edition

The features of the Alcatel-Lucent IP Touch 4018 phone Extended Edition set are roughly equivalent to the features of the Alcatel-Lucent IP Touch 4018 Phone set.

The main difference between the two sets is that the Alcatel-Lucent IP Touch 4018 phone Extended Edition set provides extended memory capacity.

As part of the **Proprietary** professional range, these IP phones are fully-featured with integrated IP connectivity and telephony, bringing you the converged power of data and voice over IP (VoIP). In addition to their optimized design, these terminals offer a grey display, wide band audio, superior quality ring tones and hands-free communication.

The Alcatel-Lucent IP Touch 4018 Phone and the Alcatel-Lucent IP Touch 4018 phone Extended Edition sets offer the following advantages:

- Instant Business Communications
- Optimized Ergonomics
- Superlative sound quality
- Unbeatable range of telephony features

Note:
In the rest of this documentation, any mention of Alcatel-Lucent IP Touch 4008 Phone sets also applies to Alcatel-Lucent IP Touch 4008 phone Extended Edition sets, and any mention of Alcatel-Lucent IP Touch 4018 Phone sets also applies to Alcatel-Lucent IP Touch 4018 phone Extended Edition sets, unless otherwise specified.

2.3.1.1.2 Instant Business Communications

The Alcatel-Lucent IP Touch 4018 Phone and the Alcatel-Lucent IP Touch 4018 phone Extended Edition sets are always ready to provide the best communication service whenever you need it, and to connect to other devices and applications in real-time. You'll find them fast and easy to use, with feature buttons and interactive soft keys.

2.3.1.1.3 Optimized Ergonomics

Attractive, innovative and intuitively designed, these terminals operate on the same simple, user-friendly ergonomics found in the best mobile phones and PDAs, so you won't waste any time accessing their powerful features and services. These phones come complete with:

- Display in different shades of grey
- Programmable feature buttons
- Up/down navigator
- Context-sensitive keys

2.3.1.1.4 Superlative sound quality

These phones provide the very best sound quality thanks to the following new enhancements:

- Compatibility with wide band audio, taking listening comfort to higher levels
- Full duplex hands-free speakerphone, including acoustic echo cancellation
- A comprehensive choice of standard ringtones and polyphonic melodies

2.3.1.1.5 Unbeatable range of telephony features

These sets offer the full range of telephony services found in the OmniPCX Office PBXs, unbeatable in terms of functionality, features, reliability and Quality of Service. These sets are available in all countries where the associated IP-enabled Alcatel-Lucent OmniPCX Office Communication Server system releases are launched.

2.3.1.2 Hardware description

2.3.1.2.1 Overview

The features of the Alcatel-Lucent IP Touch 4018 phone Extended Edition set are roughly equivalent to the features of the Alcatel-Lucent IP Touch 4018 Phone set.

The main difference between the two sets is that the Alcatel-Lucent IP Touch 4018 phone Extended Edition set provides extended memory capacity.

In the following paragraphs, descriptions and operations of the Alcatel-Lucent IP Touch 4018 Phone set also apply to the Alcatel-Lucent IP Touch 4018 phone Extended Edition set, unless specifically indicated.

2.3.1.2.2 Alcatel-Lucent IP Touch 4018 Phone set description

This section describes the:

- Set features
- Set keyboard
- Set display

The following figure illustrates the Alcatel-Lucent IP Touch 4018 Phone set.

Figure 2.99 : Alcatel-Lucent IP Touch 4018 Phone set

Set features

The features of the Alcatel-Lucent IP Touch 4018 Phone set are as follows:

- Corded comfort handset
- Full duplex hands-free
- Wide band audio
- Standard ring tones and polyphonic melodies
- Display in shades of grey
- Dialling keypad
- Fixed function keys
- Up/down navigator and OK key
- Programmable keys
- Ethernet LAN and PC connections
- Optical connectivity with external adapter
- Wall mounted kit [optional]

- 60° foot stand (“Big Foot”) [optional]

Set keyboard

The keyboard of the Alcatel-Lucent IP Touch 4018 Phone set includes:

- A dialling keypad
- Function keys
- Programmable keys
- A navigator

Dialling keypad

The dialling keypad comprises 12 keys.

Function keys

The fixed function keys are described in the table below.

table 2.31 : Fixed keys of the Alcatel-Lucent IP Touch 4018 Phone set

Key	Action
End	Can be used to: - terminate the current communication - stop ringing for an incoming call - end the current application (and return the display to its default)
Hands–free (with green LED)	Enables or disables the hands–free feature. Short press activates the hands-free feature. Long press on the hands-free key activates the Group Listening feature. The hands-free function is a full duplex function with echo cancellation and attenuation.
Volume + —	In OmniPCX Office, they adjust: - the handset/headset volume in communication mode - the built-in loudspeaker volume - the ringing level when the set rings
Redial	- **Short press:** Automatically redials the last number dialled. - **Long press:** Displays a list of recently dialled numbers. Use the up/down arrow keys to scroll between numbers, and press the **OK** key to redial the number currently displayed.
Message (with orange LED)	Provides access to: - voice-mail services - mini-message services

Key	Action
Mute (with green LED)	- When the set is in communication, this key switches the set to mute mode (disabling the set's microphone). - When the set is not in communication, this key allows an incoming internal call to be answered in hands-free mode.
Personal/Dial by name	- **Short press:** Provides access to the personal address book. - **Long press:** Provides access to the Dial by name feature.
Exit/Home	- **Short press:** Goes back one level in the application. - **Long press:** Exits the current application and returns to the default display.
Help/Menu	**Menu** - Press once to access the set's menu. This consists of 7 items - use the up/down arrow keys to move between menu items. - Press once followed by one of the keys 1 to 7 to access the corresponding menu item. - Press once followed by the **OK** key to access the first menu item (Who Am I?). **Help** Press once followed by another key to obtain information on that key's function. The options are: - **i** + programmable key - **i** + Message key - **i** + Redial key - **i** + End key - **i** + Personal/Dial by name key

Programmable keys

The programmable keys allow your preferred functions to be programmed (by an administrator), such as call forwarding or a specific call number. These keys then provide quick and easy access to these functions.

The programmable keys include:

- One personal key
- A set of 6 other programmable keys

Navigator

The navigator includes:

- A 2-direction navigation key
- A validation key (OK)
- An Exit/Home key (|<)

The Exit/Home key is used to exit the current application, or a long press will switch the display back to its default. In edit mode, it can be used to delete characters.

Set display

The table below lists the characteristics of the display of the Alcatel-Lucent IP Touch 4018 Phone set.

table 2.32 : Display of the Alcatel-Lucent IP Touch 4018 Phone set

Characteristics	Alcatel-Lucent IP Touch 4018 Phone
Display	Yes
Screen resolution	20 characters
Size of visible area	79 x 13 mm (3.11 x 0.51 inches)
Colour	Grey background

2.3.1.3 Commissioning

2.3.1.3.1 Overview

This module presents all the actions required for commissioning:

- The Alcatel-Lucent IP Touch 4018 Phone set
- The Alcatel-Lucent IP Touch 4018 phone Extended Edition set

The commissioning of Alcatel-Lucent IP Touch 4018 Phone and Alcatel-Lucent IP Touch 4018 phone Extended Edition sets is identical.

The following figure illustrates the connectors on the base of the Alcatel-Lucent IP Touch 4018 Phone and Alcatel-Lucent IP Touch 4018 phone Extended Edition sets.

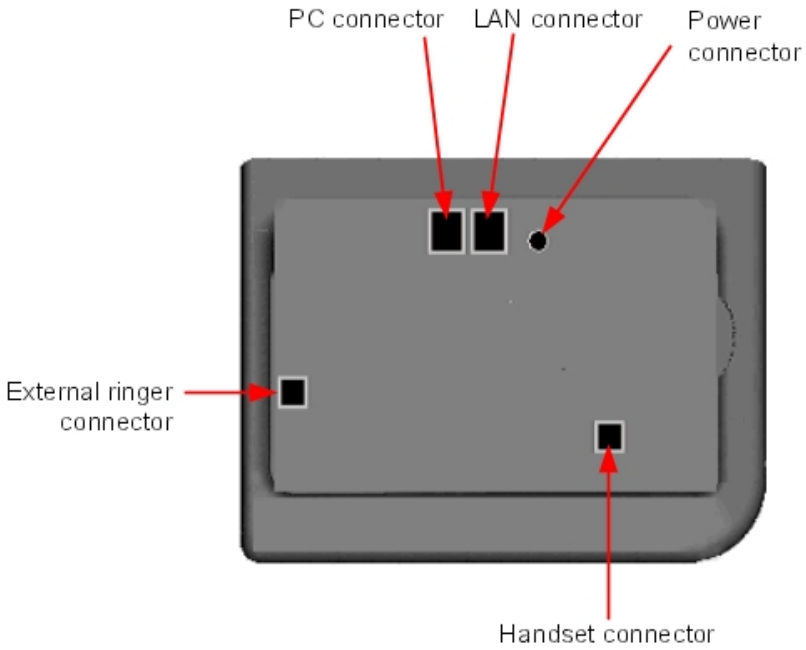


Figure 2.100 : Alcatel-Lucent IP Touch 4018 Phone and Alcatel-Lucent IP Touch 4018 phone Extended Edition connectors

2.3.1.3.2 Commissioning the set

This section describes how to:

- Connect the set
- Initialise the set
- Program keys

Prerequisites

None.

Connecting the sets

This section describes how to:

- Connect an IP Touch set to the LAN (Local Area Network)
- Connect the power supply

Prerequisites

None.

Connecting an IP Touch set to the LAN

To connect the set to the LAN:

1. Turn the set over so that you can see its base.
2. Plug the RJ45 cable into the set's LAN connector.
3. Connect the RJ45 cable to the LAN itself.

Connecting power supply

The set can be powered from two possible power sources:

- An AC/DC external adapter which is a 42V power supply
  A female jack is used to connect the power adapter. The AC/DC external adapter is the same for IP Touch and e-Reflex sets.
- Power over Ethernet (PoE)
  The supply via Ethernet can be implemented using a 802.3af standard-compatible switch.

To supply power via an AC/DC external adapter:

1. Plug the appropriate cable from the adapter into the set's power supply connector.

2. Connect the plug from the adapter to the mains power supply.
Initialisation starts.

Initialising the sets

This section describes how to:

- Choose the initialisation mode

- Initialise the IP Touch set

Prerequisites

The IP Touch set must be connected to the:

- LAN
- Power supply

Choosing the initialisation mode

The default mode is dynamic mode.

To choose the initialisation mode, refer to the table below.

table 2.33 : Initialisation modes

If	Then the required initialisation mode is	And
You have a DHCP server	Dynamic mode or **Proprietary** dynamic mode	Refer to table : Initialisation procedure In the case of **Proprietary** dynamic mode, the IP address of the set must be provided by the **Proprietary** router.
You do not have a DHCP server	Static mode	- Refer to table : Initialisation procedure - Obtain from your network administrator: • An IP address for the IP Touch set • The subnetwork mask • The router address • The TFTP server address (master VoIP board address)

Initialising the IP Touch set

To initialise the IP Touch set, refer to the table below.

Note 1:

*In each of the two cases below, you can view the IP Touch set's software version after Step 2 by selecting **Version** in the Main menu.*

table 2.34 : Initialisation procedure

For an initialisation that is	Procedure
Dynamic mode or **Proprietary** dynamic mode	**1.** Connect the power supply. **2.** After initialisationphase 2 is completed and before phase 5 starts, press **i**, then the # key. *The Main menu appears.* **3.** If the set was previously in static mode, choose **IP Parameters** from the **Main** menu. *The IP Parameters menu appears*. **4.** Choose **Dynamic** and press the **OK** key. **5.** Save by pressing the # key. **6.** Exit the **Main** menu by pressing the ***** key.
Static	**1.** Connect the power supply. **2.** Before initialisation phase 5 starts, press **i**, then the # key. *The Main menu appears.* **3.** From the **Main** menu, choose **IP Parameters**. *The IP Parameters menu appears*. **4.** Choose **Static** and press the **OK** key. **5.** Enter the following: **a.** IP address **b.** Subnetwork mask **c.** Router address **d.** TFTP server address **e.** TFTP port (69) **f.** CPU address **6.** Enter the required VLAN details, as follows: **a.** If required, select **Use VLAN** and then enter the VLAN ID number. **b.** Ensure that **Strict VLAN** is set as required. It is selected by default; de-selecting it allows you to use a DHCP server in another VLAN. **7.** Save the above parameter values by pressing the # key. **8.** Exit the **Main** menu by pressing the ***** key. *The set restarts from phase 1 with the new parameters.* *Note 2:* *If an error message appears during initialisation, disconnect the power adapter, then plug it in again, so that the system restarts initialisation.*

Restarting initialisation

If you want to change a parameter value, restart initialisation, as detailed below.

To restart initialisation:

1. Disconnect the IP Touch set from the power supply.

2. Reconnect the power supply.

3. Execute the initialization procedure as detailed in table : Initialisation procedure

Programming keys

This section describes how to program the programmable keys.

In fact, only the direct call key can be programmed (with a telephone number), which by

default is the sixth programmable key. However, the Personal/Dial by name key can be programmed in a similar way.

To program a key:

1. Press the **i** key followed by the required programmable key.
2. Press one key of the 2-way navigator (up or down).
3. Enter the telephone number to be associated with this programmable key.
4. Press **OK**. The set then goes back to its default display.

Relocating and retaining IP Touch sets

This section describes how to relocate and retain the same set.

In the procedure below, it is assumed that:

- there is one DHCP server
- no VLAN has to be configured.

Prerequisites

None.

Relocating and retaining the same set

To relocate and retain the same set:

1. Unplug the set.
2. Plug the set into a connector at its new location.

2.3.1.3.3 The Alcatel-Lucent IP Touch 4008 Phone set

The Alcatel-Lucent IP Touch 4008 Phone is a cost reduction of the Alcatel-Lucent IP Touch 4018 Phone with a new transceiver and a new LAN switch.

The Alcatel-Lucent IP Touch 4008 Phone configuration is the same as the Alcatel-Lucent IP Touch 4018 Phone configuration: both sets share the same profile.

The Alcatel-Lucent IP Touch 4008 phone Extended Edition configuration is the same as the Alcatel-Lucent IP Touch 4018 Phone configuration.

2.3.1.4 Maintenance

2.3.1.4.1 Overview

This module describes:

- The error and information messages that appear during the starting phase.
- The Ethernet link table.

2.3.1.4.2 Error and Information messages

The table below lists the error and information messages. It has the following format:

Short text = text displayed on the screen, in case of real error or for information.

Description = status/error description

table 2.35 : Starting phase error messages

Short text	Description
END	Starting phase is terminated (successful or unsuccessful)
STARTED	Step started
SUCCESS	Step successful
FAIL	Step failed
RETRYING	Retrying step
NO MAC ADDRESS	No Ethernet MAC address stored in flash
DHCP NOT RESPONDING DHCP	Server is not responding
BAD IP ADDRESS	IP address is incorrect
BAD ROUTER ADDRESS	Router address is incorrect
ROUTER PING FAILED	Router not responding to ping
BAD TFTP ADDRESS	TFTP server address is incorrect
ADDRESSES MISMATCH	Address, mask and router do not match
TFTP NOT RESPONDING	TFTP server is not responding
TFTP SERVER ERROR	TFTP server error
BAD FILE CONTENT	Error found in downloaded file
FILE TOO LARGE	File is too large (cannot be downloaded)
SAME VERSION FOUND	The version retrieved is the same as the version running
NEW VERSION FOUND	New IP Touch software version found (download)
FLASHING	Flashing in progress
FLASHING FAILED	Failed to flash downloaded binary
TRYING ANOTHER CPU	Trying next address from configuration file
NO ETHERNET LINK	Ethernet link not connected (LAN port only)
initializing	First text message after hardware reset and copyright information
1/5 network start	Phase 1 is running: the set is starting its network interface
2/5 network setup	Phase 2 is running: the set is looking for IP addresses
3/5 config download	Phase 3 is running: the set is trying to get a lanpbx file
4/5 binary download	Phase 4 is running: the set is downloading a new binary
5/5 connecting	Phase 5 is running: the set is trying to talk to the system

2.3.1.4.3 Ethernet Link

By default, IP Touch sets are configured to perform auto-negotiation on both ports (LAN and PC). Provided that the PC and the LAN switch are also configured to perform auto-negotiation,

this is the best configuration for QoS improvement.

However, depending on the network configuration, it may not always be possible to leave the terminal in auto-negotiation: link speed and duplex of both ports can be forced to determined values using the supervisor menu:

- Plug in the set, as described: module IP Touch 4008/4018 Phone - Commissioning § Commissioning the set .
- Once the set displays **initialization**, press **i**, then #.
- Use the navigation key to select **Ethernet Links**
- Modify data as requested

A configuration mismatch between the terminal and PC/LAN switch can lead to negative effects on the voice quality:

- No link (or speed mismatch): 8, 9, 11 and 12
- Packet loss (or duplex mismatch): 2, 4, 7 and 14

Note 1:
Collisions are not detected by the device operating in full-duplex mode: packets from this device are never re-transmitted if a collision occurs on them.

The following table lists all possible Ethernet port configuration combinations when connecting an IP Touch set to an external device (switch on LAN side, PC on PC side). For each combination, the table shows the link status: valid or invalid (duplex or speed mismatch), as described above.

table 2.36 : Ethernet Link Combinations

	Terminal Port	**External Device Port**	**Link Status**
1	auto-negotiation	auto-negotiation	Valid
2	auto-negotiation	100-FULL	Invalid (packet loss)
3	auto-negotiation	100-HALF	Valid
4	auto-negotiation	10-FULL	Invalid (packet loss)
5	auto-negotiation	10-HALF	Valid
6	100-FULL	100-FULL	Valid
7	100-FULL	100-HALF	Invalid (packet loss)
8	100-FULL	10-FULL	Invalid (no link)
9	100-FULL	10-HALF	Invalid (no link)
10	100-HALF	100-HALF	Valid
11	100-HALF	10-FULL	Invalid (no link)
12	100-HALF	10-HALF	Invalid (no link)
13	10-FULL	10-FULL	Valid
14	10-FULL	10-HALF	Invalid (packet loss)
15	10-HALF	10-HALF	Valid

Note 2:
When the two ports of an Alcatel-Lucent IP Touch 4018 Phone or Alcatel-Lucent IP Touch 4018 phone Extended Edition set are configured in auto-negotiation mode, if the negotiation has led to a 10 Mbps rate

on the PC port and a 100 Mbps rate on the LAN port, the IP Touch set automatically tries to renegotiate a 10 Mbps rate on the LAN port. This prevents congestion problems on the PC.

2.3.2 IP Touch 4028/4038/4068 Phone

2.3.2.1 Basic description

2.3.2.1.1 Overview

The Alcatel-Lucent OmniPCX Office Communication Server supports(among others)the following types of IP-Phones:

- In the Alcatel-Lucent IP Touch 8 series phone product range:
  - Alcatel-Lucent IP Touch 4068 Phone
  - Alcatel-Lucent IP Touch 4038 Phone
  - Alcatel-Lucent IP Touch 4028 Phone
- In the Alcatel-Lucent IP Touch 8 series phone extended edition product range:
  - Alcatel-Lucent IP Touch 4068 phone Extended Edition
  - Alcatel-Lucent IP Touch 4038 phone Extended Edition
  - Alcatel-Lucent IP Touch 4028 phone Extended Edition

Note:

The features of the Alcatel-Lucent IP Touch 4028/4038/4068 phone extended edition sets are roughly equivalent to the features of the Alcatel-Lucent IP Touch 4028/4038/4068 phone sets. Any difference is expressly indicated in this document.

The main difference between the two types of sets is that the Alcatel-Lucent IP Touch 4028/4038/4068 phone extended edition sets provide a "Gigabit" Ethernet interface.

As part of the Alcatel-Lucent professional range, these state-of-the-art IP phones are fully-featured with integrated IP connectivity and telephony, bringing you the converged power of data and voice over IP (VoIP). In addition to their optimized design, these terminals offer high-resolution, adjustable colour or grey screens, wide band audio, superior quality ring tones, hands-free communication, wireless freedom (Alcatel-Lucent IP Touch 4068 Phone and Alcatel-Lucent IP Touch 4068 phone Extended Edition only), as well as the capability to support any web-based business application.

The Alcatel-Lucent IP Touch 4028/4038/4068 phone setsand the Alcatel-Lucent IP Touch 4028/4038/4068 phone extended edition setsoffer the following advantages:

- Instant Business Communications
- Optimized Ergonomics
- Superlative sound quality
- Expandable key programming
- Open to a whole new world of applications and services
- Unbeatable range of telephony features
- As of R7.0, the use of Unicode - Chinese and Cyrillic - characters to dial by name, as well as in phone book entries and softkey label customization is possible. For more information, refer to module Input Method Editor - Operation .

2.3.2.1.2 Instant Business Communications

These sets are always ready to provide the best communication service whenever you need it, and to connect to other devices and applications in real-time. You'll find them fast and easy to use, with feature buttons and interactive soft keys, making them the ideal focal point for all your business communications.

2.3.2.1.3 Optimized Ergonomics

Attractive, innovative and intuitively designed, these terminals operate on the same simple, user-friendly ergonomics found in the best mobile phones and PDAs, so you won't waste any time accessing their powerful features and services. Each phone comes complete with:

- Colour or grey adjustable screen
- Programmable feature buttons
- Four-way navigator
- Context-sensitive keys
- Integrated alphabetic keyboard for functions such as text messaging and dial by name

2.3.2.1.4 Superlative sound quality

These phones provide the very best sound quality thanks to a wide range of new enhancements:

- Compatibility with wide band audio, taking listening comfort to higher levels
- Full duplex hands-free speakerphone, including acoustic echo cancellation
- A comprehensive choice of standard ringtones and polyphonic melodies

Each set includes a built-in socket for the use of headsets, additional speakers or teleconferencing systems.

2.3.2.1.5 Expandable key programming

Each set features a number of programmable keys allowing quick access to frequently used telephone numbers and telephony functions. The number of programmable keys can be expanded using one or more add-on modules containing additional keys. Add-on modules are available with 10 or 40 keys, as well as a 14-key module with programmable LCD key labels.

2.3.2.1.6 Open to a whole new world of applications and services

All three sets are fully equipped to welcome outside applications via an XML interface, enabling you to customise your communications infrastructure to the unique demands of your business. Users can receive tailor-made applications – such as hosted or web-based - from customers or developers at the turn of a software key. At the same time, they can keep pace with new communication features from Alcatel-Lucent, such as OmniTouch Unified Communications.

2.3.2.1.7 Unbeatable range of telephony features

These sets offer the full range of telephony services found in the OmniPCX Office PBXs from Alcatel-Lucent, unbeatable in terms of functionality, features, reliability and Quality of Service. The sets are available in all countries where the associated IP-enabled Alcatel-Lucent OmniPCX Office Communication Server system releases are launched.

2.3.2.2 Hardware description

2.3.2.2.1 Overview

The Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone and Alcatel-Lucent IP Touch 4068 Phone sets offer similar features. The main differences between the sets concern:

- Type of display (resolution, grey/colour, back light)
- Number of soft keys
- Support of a Bluetooth headset

For more information, refer to table : Features of the Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone and Alcatel-Lucent IP Touch 4068 Phone sets .

The features of Alcatel-Lucent IP Touch 4028 phone Extended Edition, Alcatel-Lucent IP Touch 4038 phone Extended Edition and Alcatel-Lucent IP Touch 4068 phone Extended Edition sets are roughly identical to the features of Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone and Alcatel-Lucent IP Touch 4068 Phone sets.

The main difference between extended edition sets and other 8 series sets is that top-of-the-range Alcatel-Lucent 8 series phone extended edition sets provide a "Gigabit" Ethernet interface.

In the following paragraphs, only Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone and Alcatel-Lucent IP Touch 4068 Phone sets are mentioned. However, descriptions and operations of these sets also apply to the Alcatel-Lucent IP Touch 4028 phone Extended Edition set, Alcatel-Lucent IP Touch 4038 phone Extended Edition set and Alcatel-Lucent IP Touch 4068 phone Extended Edition set, unless specifically indicated:

2.3.2.2.2 Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone and Alcatel-Lucent IP Touch 4068 Phone descriptions

This section describes the:

- Set features
- Set keyboard
- Set display

The following figure illustrates the Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone and Alcatel-Lucent IP Touch 4068 Phone sets. In fact, the figure shows the Alcatel-Lucent IP Touch 4068 Phone set, but the other sets are similar.

Figure 2.101 : Alcatel-Lucent IP Touch 4068 Phone set

Set features

The following table details the features of the Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone and Alcatel-Lucent IP Touch 4068 Phone sets.

table 2.37 : Features of the Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone and Alcatel-Lucent IP Touch 4068 Phone sets

Features	Alcatel-Lucent IP Touch 4028 Phone	Alcatel-Lucent IP Touch 4038 Phone	Alcatel-Lucent IP Touch 4068 Phone
Corded comfort handset	Yes	Yes	Yes
Full duplex hands-free	Yes	Yes	Yes
Wide band audio	Yes	Yes	Yes
G711 ring tones	Yes	Yes	Yes
Display	Yes (grey)	Yes (grey)	Yes (colour)
Display back light	No	No	Yes
Dialling keypad	Yes	Yes	Yes

Features	Alcatel-Lucent IP Touch 4028 Phone	Alcatel-Lucent IP Touch 4038 Phone	Alcatel-Lucent IP Touch 4068 Phone
Alphabetic keyboard	Yes	Yes	Yes
Fixed function keys	Yes (8)	Yes (8)	Yes (8)
4-way navigator and OK key	Yes	Yes	Yes
Programmable keys (F1/F2)	Yes (2)	Yes (2)	Yes (2)
Virtual add-on keys	Yes (40)	Yes (40)	Yes (40)
Display soft keys	Yes (6)	Yes (10)	Yes (10)
Alarm (two-colour screen LED)	Yes	Yes	Yes
Ethernet LAN and PC connections	Yes	Yes	Yes
Headset connection socket	Yes	Yes	Yes
Bluetooth (wireless) headset	No	No	Yes
Add-on modules	Yes (optional)	Yes (optional)	Yes (optional)
Wall mounted kit	Yes (optional)	Yes (optional)	Yes (optional)
60° foot stand (“Big Foot”)	Yes (optional)	Yes (optional)	Yes (optional)

Set keyboard

The keyboards of the Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone and Alcatel-Lucent IP Touch 4068 Phone sets include:

- A dialling keypad
- An alphabetic keyboard
- Function keys
- Programmable keys
- A navigator

Dialling keypad

The dialling keypad includes 12 keys.

Alphabetic keyboard

The alphabetic keyboard includes 34 keys.

The alphabetic keyboard exists in five versions: French, German, International, Scandinavian and American.

Function keys

The fixed function keys are described in the table below.

table 2.38 : Fixed keys of the Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone and Alcatel-Lucent IP Touch 4068 Phone sets

Key	Action
End	Can be used to: - terminate the current communication - stop ringing for an incoming call - end the current application (and return the display to the home page)
Hands–free (with green LED)	Enables or disables the hands–free feature. Short press activates the hands-free feature. Switches from handset to headset. Long press on the hands-free key activates the Group Listening feature. The hands-free function is a full duplex function with echo cancellation and attenuation.
Volume - + - —	In OmniPCX Office, they adjust: - the handset/headset volume in communication mode - the built-in loudspeaker volume - the ringing level when the set rings
Redial	- **Short press:** Automatically redials the last number dialled. - **Long press:** Displays a list of recently dialled numbers. Use the up/down arrow keys to scroll between numbers, and press the **OK** key to redial the number currently displayed.
Message (with orange LED)	Provides access to: - voice-mail services - mini-message services
Exit/Home	- **Short press:** Goes back one level in the application. - **Long press:** Exits the current application and returns the display to the Home page.
Mute (with green LED)	When the set is in communication, this key switches the set to mute mode (disabling the set's microphone).

Programmable keys

The programmable keys allow you to programme your preferred functions, such as call forwarding, enable headset and specific call numbers. These keys then provide quick and easy access to these functions.

The programmable keys include:

- Two personal keys (F1 and F2)
- 40 virtual add-on keys

All the virtual add-on keys are programmed from the **PERSO** tab (on the display), using the soft keys next to the display. For more information on the graphical display tabs, refer to **Tabs** below.

Navigator

The navigator includes:

- One 4–direction navigation device
- One central validation key (OK)

Set display

The table below lists the characteristics of the displays of the Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone and Alcatel-Lucent IP Touch 4068 Phone sets.

table 2.39 : Displays of the Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone and Alcatel-Lucent IP Touch 4068 Phone sets

Characteristics	Alcatel-Lucent IP Touch 4028 Phone	Alcatel-Lucent IP Touch 4038 Phone	Alcatel-Lucent IP Touch 4068 Phone
Graphical display	Yes	Yes	Yes
Screen resolution	64 x 128 pixels	100 x 160 pixels	240 x 320 pixels
Size of visible area	70 x 38 mm (2.76 x 1.50 inches)	78 x 51 mm (3.07 x 2.01 inches)	73.52 x 55.64 mm (2.89 x 2.19 inches)
Colour	4 grey scales	4 grey scales	4096 colours
Back light	No	No	Yes
Tilting	Yes	Yes	Yes

Tabs

The graphical display home page includes three tabs:

- The **MENU** tab which gives access to all the functions and applications accessible by users.
- The **PERSO** tab which includes up to 40 virtual programmable keys.
- The **INFO** tab which provides information about phone status.

Note:

Further tabs can be created by applications such as .

2.3.2.3 Commissioning

2.3.2.3.1 Overview

This module presents all the actions required for commissioning: .

- The Alcatel-Lucent 8 series:
  - Alcatel-Lucent IP Touch 4028 Phone
  - Alcatel-Lucent IP Touch 4038 Phone
  - Alcatel-Lucent IP Touch 4068 Phone
- The Alcatel-Lucent IP Touch 8 series phone Extended Edition:
  - Alcatel-Lucent IP Touch 4028 phone Extended Edition
  - Alcatel-Lucent IP Touch 4038 phone Extended Edition
  - Alcatel-Lucent IP Touch 4068 phone Extended Edition

The commissioning of Alcatel-Lucent 8 series and Alcatel-Lucent IP Touch 8 series phone Extended Edition is the same.

In the following paragrahs, when Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone and Alcatel-Lucent IP Touch 4068 Phone are mentioned, they also refer to their extended edition counterpart, unless specifically indicated.

The following figure illustrates the connectors on the base of each set.

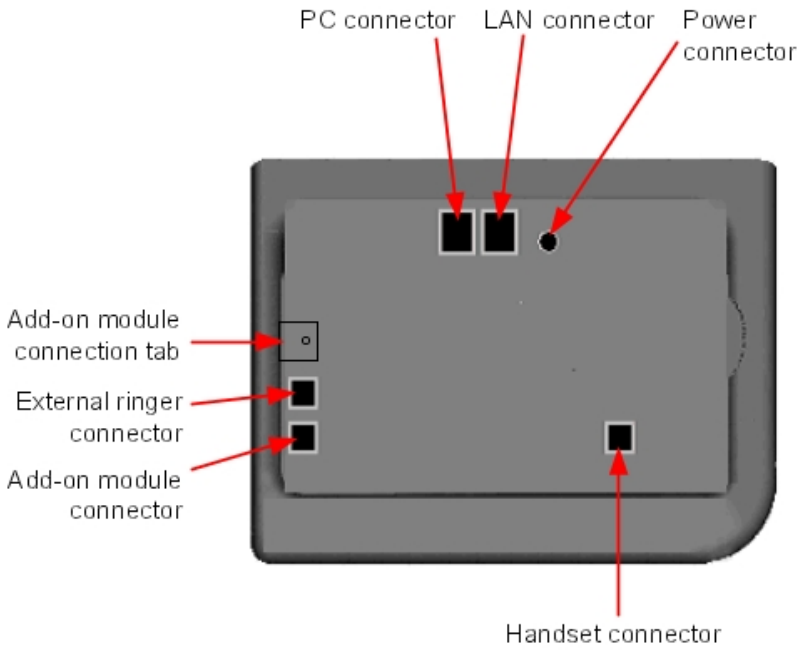


Figure 2.102 : Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone and Alcatel-Lucent IP Touch 4068 Phone connectors

2.3.2.3.2 Commissioning the sets

This section describes how to:

- Connect the sets
- Initialise the sets
- Connect optional equipment
- Program keys

Prerequisites

None.

Connecting the sets

This section describes how to:

- Connect an IP Touch set to the LAN (Local Area Network)

- Connect the power supply

Prerequisites

None.

Connecting an IP Touch set to the LAN

To connect the set to the LAN:

1. Turn the set over so that you can see its base.
2. Plug the RJ45 cable into the set's LAN connector.
3. Connect the RJ45 cable to the LAN itself.

Connecting power supply

The set can be powered from two possible power sources:

- An AC/DC external adapter which is a 42V power supply
  A female jack is used to connect the power adapter. The AC/DC external adapter is the same for IP Touch and e-Reflex sets.
- Power over Ethernet (PoE)
  The supply via Ethernet can be implemented using a 802.3af standard-compatible switch.

To supply power via an AC/DC external adapter:

1. Plug the appropriate cable from the adapter into the set's power supply connector.

2. Connect the plug from the adapter to the mains power supply.
Initialisation starts.

Initialising the sets

This section describes how to:

- Choose the initialisation mode
- Initialise the IP Touch set

Prerequisites

The IP Touch set must be connected to the:

- LAN
- Power supply

Choosing the initialisation mode

The default mode is dynamic mode.

To choose the initialisation mode, refer to the table below.

table 2.40 : Initialisation modes

If	Then the required initialisation mode is	And
You have a DHCP server	Dynamic mode or **Proprietary** dynamic mode	Refer to table : Initialisation procedure In the case of **Proprietary** dynamic mode, the IP address of the set must be provided by the **Proprietary** router.
You do not have a DHCP server	Static mode	- Refer to table : Initialisation procedure - Obtain from your network administrator: • An IP address for the IP Touch set • The subnetwork mask • The router address • The TFTP server address (master VoIP board address) *Note:* *You need to know your set's directory number.*

Initialising the IP Touch set

To initialise the IP Touch set, refer to the table below.

table 2.41 : Initialisation procedure

For an initialisation that is	Procedure
Dynamic mode or **Proprietary** dynamic mode	**1.** Connect the power supply. **2.** Before initialisation phase 5 starts, press **i**, then the # key. *The Main menu appears.* **3.** If the set was previously in static mode, choose **IP Parameters** from the **Main** menu. *The IP Parameters menu appears*. **4.** Choose **Dynamic**. **5.** Save by pressing the soft key in the upper left part of the display. **6.** Exit the **Main** menu by pressing the soft key in the upper right part of the display.

Static	**1.** Connect the power supply. **2.** Before initialisation phase 5 starts, press **i**, then the # key. *The Main menu appears.* **3.** From the **Main** menu, choose **IP Parameters**. *The IP Parameters menu appears*. **4.** Choose **Static**. **5.** Enter the following: **a.** IP address **b.** Subnetwork mask **c.** Router address **d.** TFTP server address **e.** TFTP port (69) **f.** CPU address **6.** Enter the required VLAN details, as follows: **a.** If required, select **Use VLAN** and then enter the VLAN ID number. **b.** Ensure that **Strict VLAN** is set as required. It is selected by default; de-selecting it allows you to use a DHCP server in another VLAN. **7.** Save by pressing the soft key in the upper left part of the display. **8.** Exit the **Main** menu by pressing the soft key in the upper right part of the display. *The set restarts from phase 1 with the new parameters.* *Note:* *If an error message appears during initialisation, disconnect the power adapter, then plug it in again, so that the system restarts initialisation.*

Restarting initialisation

If you want to change a parameter value, restart initialisation, as detailed below.

To restart initialisation:

1. Disconnect the IP Touch set from the power supply.

2. Reconnect the power supply.

3. Execute the initialisation procedure as detailed in table : Initialisation procedure

Connecting optional equipment

This section describes how to:

- Connect an Add-On module (AOM) to the sets
- Connect a headset
- Connect an external station speaker

Connecting an Add-On module to the sets

Add-On Modules (AOMs) can be connected to the Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone and Alcatel-Lucent IP Touch 4068 Phone sets. They are added to the right side of the set.

Three types of Add-On Module exist and provide keys associated with icons:

- AOM10 provides 10 keys
- AOM40 provides 40 keys

- AOM Alcatel-Lucent 8 series and Alcatel-Lucent 9 series Smart Display Module provides 14 keys with programmable LCD labels

Prerequisites

None.

Rules and restrictions

The following rules apply to the use of Add-On Modules with the Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone and Alcatel-Lucent IP Touch 4068 Phone sets:

- A maximum of three Add-On Modules of the types AOM10 and AOM40 can be connected to each set, providing up to 120 additional keys.
- A maximum of three Smart Display Modules can be connected to each set, providing up to 42 additional keys.
- Add-On Modules of types AOM10 and AOM40 can be used on the same set, but a Smart Display Module cannot be used in conjunction with an AOM10 or AOM40.
- If an AOM10 is used with other Add-On Modules, it must be connected as the last module on the far right of the set.

Connecting Add-On Modules

To connect an Add-On Module:

1. Remove the tab located on the right side of the IP Touch set.
2. Plug the Add-On Module's RJ45 connector into the set's RJ45 connector.
3. Insert the Add-On Module attachments into the appropriate holes located on the right side of the IP Touch set.
4. Screw the Add-On Module to the IP Touch set.

Note:
If the IP Touch set is on when you plug in an Add-On Module, you must restart the set after connection.

Connecting headsets

The headset jack is located on the left side of the set.

The 3.5 mm female jack can receive a headset jack.

The hands-free key allows you to switch from handset to headset.

Prerequisites

None.

Connecting a headset

To connect a headset, simply plug the headset jack into the associated connector on the side of the set.

Connecting external station speakers

The external station speaker jack is located on the left side of the IP Touch set.

The 3.5 mm female jack can receive an external station speaker jack.

In order to take the external station speaker into account, the set customisation for the jack has to be set to “Loudspeaker”.

Prerequisites

None.

Connecting an external station speaker

To connect an external station speaker, plug the external station speaker jack into the associated connector on the side of the set.

Programming keys

This section describes how to program a programmable key from the:

- F1/F2 keys
- Add-On Module keys (if any)
- virtual add-on keys

Two methods are presented.

Programming a key

To program a key:

1. From the **MENU** tab, select **Settings**.
   The Settings menu appears.
2. From the **Settings** menu, select **Keys**.
   The virtual add-on keys appear.
3. Select the key to be programmed, as follows:
   - To program a virtual add-on key, scroll using the up/down navigator keys until you reach the required virtual key and then press the corresponding soft key.
   - To program the F1 or F2 key, or a key on a connected Add-On Module, simply press this key.
4. Select **Name** and enter the name to be associated with the selected key, then press **OK**.
   The desired name is associated with the key.
5. Select **Number** and enter the telephone number to be associated with the key, then press **OK**.
   The desired number is associated with the key.
6. Press **Exit** to go back to home page.

Programming a key (fast customisation)

You can also program a key using the following method:

1. Select the key to be programmed, as follows:
   - To program a virtual add-on key, from the **PERSO** tab press **i** followed by the required key.
   - To program the F1 or F2 key, or a key on a connected Add-On Module, from any tab press **i** followed by the required key.

2. Select **Name** and enter the name to be associated with the selected key, then press **OK**.
   The desired name is associated with the key.
3. Select **Number** and enter the telephone number to be associated with the key, then press **OK**.
   The desired number is associated with the key.
4. Press **Exit** to go back to the home page.

Relocating and retaining IP Touch sets

This section describes how to relocate and retain the same set.

In the procedure below, it is assumed that:

- there is one DHCP server
- no VLAN has to be configured.

Prerequisites

None.

Relocating and retaining the same set

To relocate and retain the same set:

1. Unplug the set.
2. Plug the set into a connector at its new location.

2.3.2.4 Bluetooth - Basic description

2.3.2.4.1 Overview

The Alcatel-Lucent IP Touch 4068 Phone set features Bluetooth® class 3 (1mW) wireless technology. This technology uses the ISM 2.4 GHz radio frequency band.

Wireless audio accessory Bluetooth® 1.1, 1.2and 2.0with headset profile operates with Alcatel-Lucent IP Touch 4068 Phone.

Optimum audio quality is obtained at up to 3 meters line of sight from the Alcatel-Lucent IP Touch 4068 Phone terminal. The range of a Bluetooth® device class 3 is around 10 meters.

The ISM 2.4 GHz radio frequency spectrum may be shared with other applications. Bluetooth® 1.2 version is more robust to the interference caused by Wifi 802.11b and 802.11g devices.

Alcatel-Lucent IP Touch Bluetooth® wireless handsetreference 3GV27007xxis 1.2 enabled and operates with Alcatel-Lucent IP Touch 4068 Phone reference 3GV27043xx from Alcatel-Lucent OmniPCX Office Communication Server R4.1.

Alcatel-Lucent IP Touch Bluetooth® wireless handset reference 3GV27059xx is 1.2 enabled and operates with Alcatel-Lucent IP Touch 4068 phone Extended Edition reference (3GV27062xx) from Alcatel-Lucent OmniPCX Office Communication Server R7.0.

Caution:

- ***The Bluetooth wireless handset 3GV27059xx does not operate with the Alcatel-Lucent IP Touch 4068 Phone (3GV27043xx) set***
- ***The Bluetooth wireless handset 3GV27007xx does not operate with the Alcatel-Lucent IP Touch 4068 phone Extended Edition (3GV27062xx) set***

Bluetooth® 1.2 headset accessories operate in 1.2 with Alcatel-Lucent IP Touch 4068 Phone reference 3GV27043xx from Alcatel-Lucent OmniPCX Office Communication Server R4.1.

The Alcatel-Lucent IP Touch 4068 Phone is compliant with the essential requirements of directive 1999/5/EC of the European Parliament and Council (EC member states), and with section 15 of the Federal Communications Commission (United States) regulations. The set is designed and manufactured to remain within the SAR (Specific Absorption Rate) radio transmission limits established by the different countries concerned (FCC for the USA). The set must not be used with Bluetooth® wireless accessories in countries in which this technology is not authorized.

2.3.2.4.2 Characteristics of the Bluetooth® wireless technology accessory

The audio quality obtained by accessory users depends on the technical characteristics of the accessory, notably acoustic coupling.

Alcatel-Lucent recommends the use of Bluetooth® 1.2 headsets complying with recommendation TIA/EIA-810-A - that specifies a minimum TCLw attenuation of 52 dB.

A headset that does not comply with the recommendation generates an unpleasant echo for the remote party. To obtain technical information on your accessory, please contact your supplier.

2.3.2.4.3 Safety rules

Using a Bluetooth® wireless accessory may result in perceptible noise for persons with a hearing aid. Accessories must not be used in areas with warning signs indicating that electrical devices or products using radio frequencies must be switched off. Such areas commonly include hospitals, areas where explosive products are stored or handled, and areas where flammable gases or vapours may be present.

To limit any risk of interference, Alcatel-Lucent recommends that persons with a pacemaker do not remain in the proximity of the Alcatel-Lucent IP Touch 4068 Phone set when it is connected to a wireless accessory.

2.3.2.5 Bluetooth - Installation

2.3.2.5.1 Commissioning a Bluetooth® Handset

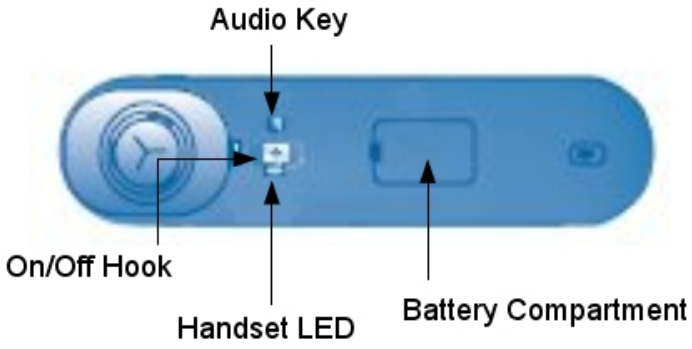


Figure 2.103 : Alcatel-Lucent IP Touch 4068 Phone Bluetooth® Handset

Connecting the Battery

The battery pack is housed in the battery compartment located in the handset.

The battery pack is recharged when the handset is placed on its socket. A complete battery charge takes 16 hours.

The autonomy of the battery is 10 hours in conversation and 33 hours in standby.

Note:
On the Alcatel-Lucent IP Touch 4068 phone Extended Edition Bluetooth® Handset, the autonomy of the battery is 100 hours in standby.

The handset Led indicates the battery charge state (when the handset is on its socket):

- Led off: the battery is charged
- Led green steady: the battery is charging

Pairing the Handset

Before a Bluetooth® handset can be used, it must be paired correctly to the Alcatel-Lucent IP Touch 4068 Phone set:

1. On the Alcatel-Lucent IP Touch 4068 Phone set, select the Menu page and navigate to: **Settings -> My phone -> Bluetooth -> Add device**
2. On the Bluetooth® handset do a simultaneous long press on the On/Off Hook key and the Audio key 

   A sound made of three different tones is audible and the led flashes alternatively green and orange.The Bluetooth® handset enters in pairing mode for about one minute and then goes off.The Alcatel-Lucent IP Touch 4068 Phone searches for Bluetooth® equipment, waits until the type of equipment is detected and displays its address.
3. On the Alcatel-Lucent IP Touch 4068 Phone set, select the relevant equipment and press the Add key.
   A sound made of three different tones confirms the correct installation of the handset. The handset led flashes green or orange depending on the battery charge.

Adjusting Audio Level

There are two ways to adjust the audio level:

- On the Alcatel-Lucent IP Touch 4068 Phone set with the keys 
- On the Bluetooth® handset with the key 

Consecutive presses adjust the handset volume (3 levels).

Activating Mute Feature

When the mute feature is enabled your correspondent can no longer hear you.

There are two ways to activate the mute feature:

- On the Alcatel-Lucent IP Touch 4068 Phone set with the mute key 
- On the Bluetooth® handset with a long press on the key 

2.3.2.5.2 Commissioning a Bluetooth® Headset

Pairing the Headset

Before a Bluetooth® handset can be used, it must be paried correctly to the Alcatel-Lucent IP Touch 4068 Phone set:

Prerequiste: the headset must be in detectable mode (Refer to the user documentation supplied with the headset).

1. On the Alcatel-Lucent IP Touch 4068 Phone set, select the **Menu** page and navigate to: **Settings** -> **My phone** -> **Bluetooth** -> **Add device**
   The Alcatel-Lucent IP Touch 4068 Phone set searches for Bluetooth® equipment. When the type of equipment is detected, its address is displayed.
2. Select the relevant equipment and press the **Add** key. Press the **OK** key to validate.
3. Enter the headset PIN code by dialling the code on the numeric keypad of the Alcatel-Lucent IP Touch 4068 Phone. Press the **OK** key to validate.
   An acknowledgement message and the headset icon are displayed on the Alcatel-Lucent IP Touch 4068 Phone set screen.

Adjusting Audio Level

There are two ways to adjust the audio level:

- On the Alcatel-Lucent IP Touch 4068 Phone set with the keys
- On the Bluetooth® headset (Refer to the user documentation supplied with the headset)

2.3.2.5.3 Removing of a Bluetooth® Equipment (Headset or Handset)

1. On the Alcatel-Lucent IP Touch 4068 Phone set select the **Menu** page and navigate to **Settings** -> **My phone** -> **Bluetooth** -> **My devices**
   The Alcatel-Lucent IP Touch 4068 Phone set displays the bound Bluetooth® equipment.
2. Select the equipment to be removed and press the **Remove dvc** key. Press the **OK** key to validate.
   The equipment is removed and a acknowledgement message is displayed.

2.3.2.6 Maintenance

2.3.2.6.1 Overview

This module describes:

- The error and information messages that appear during the starting phase.
- The Ethernet link table.

2.3.2.6.2 Error and Information messages

The table below lists the error and information messages. It has the following format:

Short text = text displayed on the screen, in case of real error or for information.

Description = status/error description

table 2.42 : Starting phase error messages

Short text	Description
END	Starting phase is terminated (successful or unsuccessful)
STARTED	Step started
SUCCESS	Step successful
FAIL	Step failed
RETRYING	Retrying step
NO MAC ADDRESS	No Ethernet MAC address stored in flash
DHCP NOT RESPONDING DHCP	Server is not responding
BAD IP ADDRESS	IP address is incorrect
BAD ROUTER ADDRESS	Router address is incorrect
ROUTER PING FAILED	Router not responding to ping
BAD TFTP ADDRESS	TFTP server address is incorrect
ADDRESSES MISMATCH	Address, mask and router do not match
TFTP NOT RESPONDING	TFTP server is not responding
TFTP SERVER ERROR	TFTP server error
BAD FILE CONTENT	Error found in downloaded file
FILE TOO LARGE	File is too large (cannot be downloaded)
SAME VERSION FOUND	The version retrieved is the same as the version running
NEW VERSION FOUND	New IP Touch software version found (download)
FLASHING	Flashing in progress
FLASHING FAILED	Failed to flash downloaded binary
TRYING ANOTHER CPU	Trying next address from configuration file
NO ETHERNET LINK	Ethernet link not connected (LAN port only)
initializing	First text message after hardware reset and copyright information
1/5 network start	Phase 1 is running: the set is starting its network interface
2/5 network setup	Phase 2 is running: the set is looking for IP addresses
3/5 config download	Phase 3 is running: the set is trying to get a lanpbx file
4/5 binary download	Phase 4 is running: the set is downloading a new binary
5/5 connecting	Phase 5 is running: the set is trying to talk to the system

2.3.2.6.3 Ethernet link

By default, IP Touch sets are configured to perform auto-negotiation on both ports (LAN and PC). Provided that the PC and the LAN switch are also configured to perform auto-negotiation,

this is the best configuration for QoS improvement.

However, depending on the network configuration, it may not always be possible to leave the terminal in auto-negotiation: link speed and duplex of both ports can be forced to determined values using the supervisor menu:

- Plug in the set
- Once the set displays **initialization**, press **i**, then **#**
- Select **Ethernet Links**
- Modify data as requested

The 1000 Mbit/s rate is available on Alcatel-Lucent IP Touch 4028/4038/4068 phone Extended Edition sets configured in auto-negotiation mode and cannot be forced through the MMI.

A configuration mismatch between the terminal and PC/LAN switch can lead to negative effects on the voice quality:

- No link (or speed mismatch): 8, 9, 11 and 12
- Packet loss (or duplex mismatch): 2, 4, 7 and 14

Note 1:
Collisions are not detected by the device operating in full-duplex mode: packets from this device are never re-transmitted if a collision occurs on them.

The following table lists all possible Ethernet port configuration combinations when connecting an IP Touch set to an external device (switch on LAN side, PC on PC side). For each combination, the table shows the link status: valid or invalid (duplex or speed mismatch), as described above.

table 2.43 : Ethernet Link Combinations

	Terminal Port	**External Device Port**	**Link Status**
1	auto-negotiation	auto-negotiation	Valid
2	auto-negotiation	100-FULL	Invalid (packet loss)
3	auto-negotiation	100-HALF	Valid
4	auto-negotiation	10-FULL	Invalid (packet loss)
5	auto-negotiation	10-HALF	Valid
6	100-FULL	100-FULL	Valid
7	100-FULL	100-HALF	Invalid (packet loss)
8	100-FULL	10-FULL	Invalid (no link)
9	100-FULL	10-HALF	Invalid (no link)
10	100-HALF	100-HALF	Valid
11	100-HALF	10-FULL	Invalid (no link)
12	100-HALF	10-HALF	Invalid (no link)
13	10-FULL	10-FULL	Valid
14	10-FULL	10-HALF	Invalid (packet loss)
15	10-HALF	10-HALF	Valid

It is not necessary to reset the terminal after changing the configuration.

Note 2:

When the two ports of an Alcatel-Lucent IP Touch 4028/4038/4068 set are configured in auto-negotiation mode, if the negotiation has led to a 10 Mbps rate on the PC port and a 100 Mbps rate on the LAN port, the IP Touch set automatically tries to renegotiate a 10 Mbps rate on the LAN port. This prevents congestion problems on the PC.

This does not apply to Alcatel-Lucent IP Touch 4028/4038/4068 phone Extended Edition sets.

2.3.3 4019 Digital Phone

2.3.3.1 Basic description

2.3.3.1.1 Overview

This phone is part of the Alcatel-Lucent professional range. In addition to its optimized design, this terminal offers a grey display, wide band audio, a choice of ring tones, and group listening.

The Alcatel-Lucent 4019 Digital Phone set offers the following advantages:

- Instant Business Communications
- Optimized Ergonomics
- Superlative sound quality
- Wide range of telephony features

2.3.3.1.2 Instant Business Communications

The Alcatel-Lucent 4019 Digital Phone is always ready to provide the best communication service whenever you need it, and to connect to other devices and applications in real-time. You'll find it fast and easy to use, with feature buttons and interactive soft keys.

2.3.3.1.3 Optimized Ergonomics

Attractive, innovative and intuitively designed, this terminal operates on the same simple, user-friendly ergonomics found in the best mobile phones and PDAs, so that you won't waste any time accessing its features and services. The phone comes complete with:

- Grey display
- Programmable feature buttons
- Up/down navigator
- Context-sensitive keys

2.3.3.1.4 Superlative sound quality

This phone provides the very best sound quality thanks to the following new enhancements:

- A group listening capability from its built-in speaker
- A comprehensive choice of standard ringtones and polyphonic melodies

2.3.3.1.5 Unbeatable range of telephony features

This set offers the full range of telephony services found in the OmniPCX Office PBXs from Alcatel-Lucent, unbeatable in terms of functionality, features, reliability and Quality of Service. The set is available in all countries where the associated Alcatel-Lucent OmniPCX Office Communication Server system releases are launched. It is compatible with OmniPCX Office

release 4.0.

2.3.3.2 Hardware description

2.3.3.2.1 Alcatel-Lucent 4019 Digital Phone set description

This section describes the:

- Set features
- Set keyboard
- Set display

The following figure illustrates the Alcatel-Lucent 4019 Digital Phone set.

Figure 2.104 : Alcatel-Lucent 4019 Digital Phone set

Set features

The features of the Alcatel-Lucent 4019 Digital Phone set are as follows.

- Corded comfort handset
- Group listening through built-in loudspeaker
- Standard ring tones and polyphonic melodies

- Grey display
- Dialling keypad
- Fixed function keys
- Up/down navigator and OK key
- Programmable keys
- Wall mounted kit [optional]
- 60° foot stand (“Big Foot”) [optional]

Set keyboard

The keyboard of the Alcatel-Lucent 4019 Digital Phone set includes:

- A dialling keypad
- Function keys
- Programmable keys
- A navigator

Dialling keypad

The dialling keypad comprises 12 keys.

Function keys

The fixed function keys are described in the table below.

table 2.44 : Fixed keys of the Alcatel-Lucent 4019 Digital Phone set

Key	Action
End	Can be used to: - terminate the current communication - stop ringing for an incoming call - end the current application (and return the display to its default)
Loudspeaker (with green LED)	Enables or disables the built-in loudspeaker. This key activates the group listening feature.
Volume - + - —	In OmniPCX Office, they adjust: - the handset/headset volume in communication mode - the built-in loudspeaker volume - the ringing level when the set rings
Redial	- **Short press:** Automatically redials the last number dialled. - **Long press:** Displays a list of recently dialled numbers. Use the up/down arrow keys to scroll between numbers, and press the **OK** key to redial the number currently displayed.
Message (with orange LED)	Provides access to: - voice-mail services - mini-message services

Key	Action
Mute (with green LED)	When the set is in communication, this key switches the set to mute mode (disabling the set's microphone).
Personal/Dial by name	- **Short press:** Provides access to the personal address book. - **Long press:** Provides access to the Dial by name feature.
Exit/Home	- **Short press:** Goes back one level in the application. - **Long press:** Exits the current application and returns to the default display.
Help/Menu	**Menu** - Press once to access the set's menu. This consists of 7 items - use the up/down arrow keys to move between menu items. - Press once followed by one of the keys 1 to 7 to access the corresponding menu item. - Press once followed by the **OK** key to access the first menu item (Who Am I?). **Help** Press once followed by another key to obtain information on that key's function. The options are: - **i** + programmable key - **i** + Message key - **i** + Redial key - **i** + End key - **i** + Personal/Dial by name key

Programmable keys

The programmable keys allow your preferred functions to be programmed (by an administrator), such as call forwarding or a specific call number. These keys then provide quick and easy access to these functions.

The programmable keys include:

- One personal key
- A set of 6 other programmable keys

Navigator

The navigator includes:

- A 2-direction navigation key
- A validation key (OK)
- An Exit/Home key (|<)

The Exit/Home key is used to exit the current application, or a long press will switch the display back to its default. In edit mode, it can be used to delete characters.

Set display

The table below lists the characteristics of the display of the Alcatel-Lucent 4019 Digital Phone set.

table 2.45 : Display of the Alcatel-Lucent 4019 Digital Phone set

Characteristics	Alcatel-Lucent 4019 Digital Phone
Display	Yes
Screen resolution	20 characters
Size of visible area	79 x 13 mm (3.11 x 0.51 inches)
Colour	Grey background

2.3.3.3 Commissioning

2.3.3.3.1 Overview

This module presents all the actions required for commissioning the Alcatel-Lucent 4019 Digital Phone set.

The following figure illustrates the connectors on the base of the set.

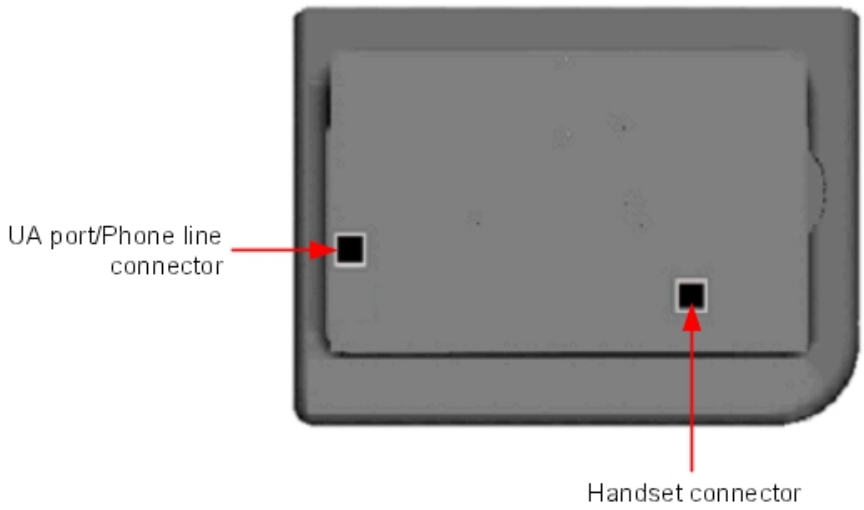


Figure 2.105 : Alcatel-Lucent 4019 Digital Phone connectors

2.3.3.3.2 Commissioning the set

This section describes how to:

- Connect the set
- Program keys

Prerequisites

None.

Connecting the set

This section describes how to connect the set to the telephone system.

Prerequisites

None.

Connecting the set to the telephone system

To connect the set to the telephone system:

1. Turn the set over so that you can see its base.
2. Plug the RJ11 cable into the set's UA port/phone line connector.
3. Connect the RJ11 cable to a UA port in the telephone system.

Programming keys

This section describes how to program the programmable keys.

In fact, only the direct call key can be programmed (with a telephone number), which by default is the sixth programmable key. However, the Personal/Dial by name key can be programmed in a similar way.

To program a key:

1. Press the **i** key followed by the required programmable key.
2. Press one key of the 2-way navigator (up or down).
3. Enter the telephone number to be associated with this programmable key.
4. Press **OK**. The set then goes back to its default display.

2.3.4 4029/4039 Digital Phone

2.3.4.1 Basic description

2.3.4.1.1 Overview

These state-of-the-art phones are part of the Alcatel-Lucent professional range. In addition to their optimized design, these terminals offer high-resolution, adjustable grey screens, wide band audio, superior quality ring tones and hands-free communication.

The Alcatel-Lucent Alcatel-Lucent 4029 Digital Phone and Alcatel-Lucent 4039 Digital Phone sets offer the following advantages:

- Instant Business Communications
- Optimized Ergonomics
- Superlative sound quality
- Expandable key programming
- Unbeatable range of telephony features

- As of Release 6.0 of Alcatel-Lucent OmniPCX Office Communication Server, the use of Unicode - Chinese and Cyrillic - characters for dial by name, phone book entry and softkey label customization is possible. For more information, refer to module Input Method Editor - Operation .

2.3.4.1.2 Instant Business Communications

These sets are always ready to provide the best communication service whenever you need it, and to connect to other devices and applications in real-time. You'll find them fast and easy to use, with feature buttons and interactive soft keys, making them the ideal focal point for all your business communications.

2.3.4.1.3 Optimized Ergonomics

Attractive, innovative and intuitively designed, these terminals operate on the same simple, user-friendly ergonomics found in the best mobile phones and PDAs, so that you won't waste any time accessing their powerful features and services. Each phone comes complete with:

- Grey adjustable screen
- Programmable feature buttons
- Four-way navigator
- Context-sensitive keys
- Integrated alphabetic keyboard for functions such as text messaging and dial by name

2.3.4.1.4 Superlative sound quality

These phones provide the very best sound quality thanks to a wide range of new enhancements:

- Hands-free speakerphone, including acoustic echo cancellation
- A comprehensive choice of standard ringtones and polyphonic melodies

Each set includes a built-in socket for the use of headsets and external hands-free devices.

2.3.4.1.5 Expandable key programming

Each set features a number of programmable keys allowing quick access to frequently used telephone numbers and telephony functions. The number of programmable keys can be expanded using one or more add-on modules containing additional keys. Add-on modules are available with 10 or 40 keys, as well as a 14-key module with programmable LCD key labels.

2.3.4.1.6 Unbeatable range of telephony features

These sets offer the full range of telephony services found in OmniPCX Office PBXs from Alcatel-Lucent, unbeatable in terms of functionality, features, reliability and quality of service. The sets are available in all countries where the associated Alcatel-Lucent OmniPCX Office Communication Server system releases are launched. They are compatible with OmniPCX Office release 4.0.

2.3.4.2 Hardware description

2.3.4.2.1 Overview

The Alcatel-Lucent 4029 Digital Phone and Alcatel-Lucent 4039 Digital Phone sets offer similar features. The main differences between the sets are:

- Type of display (resolution)
- Number of soft keys

For more information, refer to table : Features of the Alcatel-Lucent 4029 Digital Phone and Alcatel-Lucent 4039 Digital Phone sets .

2.3.4.2.2 Alcatel-Lucent Alcatel-Lucent 4029 Digital Phone and Alcatel-Lucent 4039 Digital Phone descriptions

This section describes the:

- Set features
- Set keyboard
- Set display

The following figure illustrates the Alcatel-Lucent 4029 Digital Phone and Alcatel-Lucent 4039 Digital Phone sets. In fact, the figure shows the Alcatel-Lucent 4039 Digital Phone set, but the Alcatel-Lucent 4029 Digital Phone set is similar.

Figure 2.106 : Alcatel-Lucent Alcatel-Lucent 4039 Digital Phone set

Set features

The following table details the features of the Alcatel-Lucent 4029 Digital Phone and Alcatel-Lucent 4039 Digital Phone sets.

table 2.46 : Features of the Alcatel-Lucent 4029 Digital Phone and Alcatel-Lucent 4039 Digital Phone sets

Features	Alcatel-Lucent 4029 Digital Phone	Alcatel-Lucent 4039 Digital Phone
Corded comfort handset	Yes	Yes
Full duplex hands-free	Yes	Yes
Wide band audio	Yes	Yes
Standard ring tones and polyphonic melodies	Yes	Yes
Display	Yes (64 x 128 pixels)	Yes (100 x 160 pixels)
Dialling keypad	Yes	Yes
Alphabetic keyboard	Yes	Yes
Fixed function keys	Yes (8)	Yes (8)
4-way navigator and OK key	Yes	Yes
Programmable keys (F1/F2)	Yes (2)	Yes (2)
Virtual add-on keys	Yes (40)	Yes (40)
Display soft keys	Yes (6)	Yes (10)
Alarm (two-colour screen LED)	Yes	Yes
Headset connection socket	Yes	Yes
Add-on modules	Yes (optional)	Yes (optional)
Wall mounted kit	Yes (optional)	Yes (optional)
60° foot stand (“Big Foot”)	Yes (optional)	Yes (optional)

Set keyboard

The keyboards of the Alcatel-Lucent 4029 Digital Phone and Alcatel-Lucent 4039 Digital Phone sets include:

- A dialling keypad
- An alphabetic keyboard
- Function keys
- Programmable keys
- A navigator

Dialling keypad

The dialling keypad comprises 12 keys.

Alphabetic keyboard

The alphabetic keyboard comprises 34 keys.

The alphabetic keyboard exists in five versions: French, German, International, Scandinavian

and American.

Function keys

The fixed function keys are described in the table below.

table 2.47 : Fixed keys of the Alcatel-Lucent 4029 Digital Phone and Alcatel-Lucent 4039 Digital Phone sets

Key	Action
End	Terminates current communication
Hands–free (with green LED)	Enables or disables the hands–free feature. Short press activates the hands-free feature. Switches from handset to headset. Long press on the hands-free key activates the Group Listening feature. The hands-free function is a full duplex function with echo cancellation and attenuation.
Volume - + - —	In OmniPCX Office, they adjust: - the handset/headset volume in communication mode - the built-in loudspeaker volume - the ringing level when the set rings
Redial	- **Short press:** Automatically redials the last number dialled. - **Long press:** Displays a list of recently dialled numbers. Use the up/down arrow keys to scroll between numbers, and press the **OK** key to redial the number currently displayed.
Message (with orange LED)	Provides access to: - voice-mail services - mini-message services
Exit/Home	- **Short press:** Goes back one level in the application. - **Long press:** Exits the current application and returns the display to the Home page.
Mute (with green LED)	When the set is in communication, this key switches the set to mute mode (disabling the set's microphone).

Programmable keys

The programmable keys allow you to programme your preferred functions, such as call forwarding, enable headset and specific call numbers. These keys then provide quick and easy access to these functions.

The programmable keys include:

- Two personal keys (F1 and F2)
- 40 virtual add-on keys

All the virtual add-on keys are programmed from the **PERSO** tab (on the display), using the

soft keys next to the display. For more information on the graphical display tabs, refer to **Tabs** below.

Navigator

The navigator includes:

- One 4-direction navigation device
- One central validation key (OK)

Set display

The table below lists the characteristics of the displays of the Alcatel-Lucent 4029 Digital Phone and Alcatel-Lucent 4039 Digital Phone sets.

table 2.48 : Displays of the Alcatel-Lucent 4029 Digital Phone and Alcatel-Lucent 4039 Digital Phone sets

Characteristics	**Alcatel-Lucent 4029 Digital Phone**	**Alcatel-Lucent 4039 Digital Phone**
Graphical display	Yes	Yes
Screen resolution	64 x 128 pixels	100 x 160 pixels
Size of visible area	70 x 38 mm (2.76 x 1.50 inches)	78 x 51 mm (3.07 x 2.01 inches)
Colour	4 grey scales	4 grey scales
Tilting	Yes	Yes

Tabs

The graphical display home page includes three tabs:

- The **MENU** tab which gives access to all the functions and applications accessible by users.
- The **PERSO** tab which includes up to 40 virtual programmable keys.
- The **INFO** tab which provides information about phone status.

Note:

Further tabs can be created by applications such as (ACD).

2.3.4.3 Commissioning

2.3.4.3.1 Overview

This module presents all the actions required for commissioning the Alcatel-Lucent 4029 Digital Phone and Alcatel-Lucent 4039 Digital Phone sets.

The following figure illustrates the connectors on the base of each set.

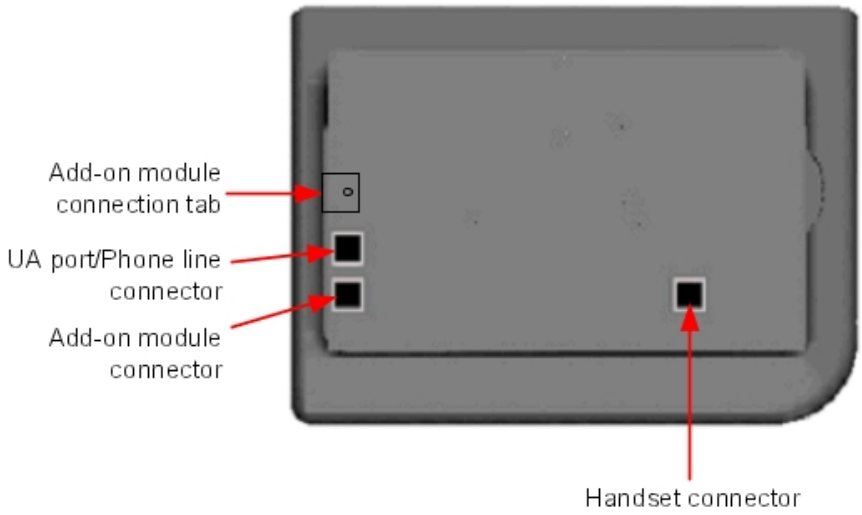


Figure 2.107 : Alcatel-Lucent 4029 Digital Phone and Alcatel-Lucent 4039 Digital Phone connectors

2.3.4.3.2 Commissioning the sets

This section describes how to:

- Connect the sets
- Connect optional equipment
- Program keys

Prerequisites

None.

Connecting the sets

This section describes how to connect a set to the telephone system.

Prerequisites

None.

Connecting to the telephone system

To connect a set to the telephone system:

1. Turn the set over so that you can see its base.
2. Plug the RJ11 cable into the set's UA port/phone line connector.
3. Connect the RJ11 cable to a UA port in the telephone system.

Connecting optional equipment

This section describes how to:

- Connect an Add-On module (AOM) to the sets
- Connect a headset
- Connect an external hands-free device

Connecting an Add-On module to the sets

Add-On Modules (AOMs) can be connected to the Alcatel-Lucent 4029 Digital Phone and Alcatel-Lucent 4039 Digital Phone sets. They are added to the right side of the set.

Three types of Add-On Module exist and provide keys associated with icons:

- AOM10 provides 10 keys
- AOM40 provides 40 keys
- AOM Alcatel-Lucent 8 series and Alcatel-Lucent 9 series Smart Display Module provides 14 keys with programmable LCD labels

Prerequisites

None.

Rules and restrictions

The following rules apply to the use of Add-On Modules with the Alcatel-Lucent 4029 Digital Phone and Alcatel-Lucent 4039 Digital Phone sets:

- A maximum of three Add-On Modules of the types AOM10 and AOM40 can be connected to each set, providing up to 120 additional keys.
- A maximum of three Smart Display Modules can be connected to each set, providing up to 42 additional keys.
- Add-On Modules of types AOM10 and AOM40 can be used on the same set, but a Smart Display Module cannot be used in conjunction with an AOM10 or AOM40.
- If an AOM10 is used with other Add-On Modules, it must be connected as the last module on the far right of the set.

Connecting Add-On Modules

To connect an Add-On Module:

1. Remove the tab located on the right side of the set.
2. Plug the Add-On Module's RJ45 connector into the set's RJ45 connector.
3. Insert the Add-On Module attachments into the appropriate holes located on the right side of the set.
4. Screw the Add-On Module to the set.

Note:
If the set is on when you plug in an Add-On Module, you must restart the set after connection.

Connecting headsets

The headset jack is located on the left side of the set.

The 3.5 mm female jack can receive a headset jack.

The hands-free key allows you to switch from handset to headset.

Prerequisites

None.

Connecting a headset

To connect a headset, simply plug the headset jack into the associated connector on the side of the set.

Connecting an external hands-free device

The external device jack is located on the left side of the set.

The 3.5 mm female jack can receive the jack of an external hands-free device.

In order to take the external hands-free device into account, the set's customisation for the jack must be set to "Handsfree".

Prerequisites

None.

Connecting an external hands-free device

To connect an external hands-free device, plug the external device's jack into the associated connector on the side of the set.

Programming keys

This section describes how to program a programmable key from the:

- F1/F2 keys
- Add-On Module keys (if any)
- virtual add-on keys

Two methods are presented.

Programming a key

To program a key:

1. From the **MENU** tab, select **Settings**.
   The Settings menu appears.
2. From the **Settings** menu, select **Keys**.
   The virtual add-on keys appear.
3. Select the key to be programmed, as follows:
   - To program a virtual add-on key, scroll using the up/down navigator keys until you reach the required virtual key and then press the corresponding soft key.
   - To program the F1 or F2 key, or a key on a connected Add-On Module, simply press this key.
4. Select **Name** and enter the name to be associated with the selected key, then press **OK**.
   The desired name is associated with the key.

Note:
As of release 6.0 of Alcatel-Lucent OmniPCX Office Communication Server, it is possible to use Unicode - Chinese and Cyrillic - characters. It is at this step that it becomes active, if used. For more information about IME, refer to the section Operation - Input Method Editor in this chapter.

5. Select **Number** and enter the telephone number to be associated with the key, then press **OK**.
   The desired number is associated with the key.
6. Press **Exit** to go back to home page.

Programming a key (fast customisation)

You can also program a key using the following method:

1. Select the key to be programmed, as follows:
   - To program a virtual add-on key, from the **PERSO** tab press **i** followed by the required key.
   - To program the F1 or F2 key, or a key on a connected Add-On Module, from any tab press **i** followed by the required key.
2. Select **Name** and enter the name to be associated with the selected key, then press **OK**.
   The desired name is associated with the key.
3. Select **Number** and enter the telephone number to be associated with the key, then press **OK**.
   The desired number is associated with the key.
4. Press **Exit** to go back to the home page.

2.3.5 Input Method Editor

2.3.5.1 Operation

The Input Method Editor (IME) allows a user to input non-Latin characters on sets with a standard Latin keyboard (with or without special markings on the keyboard).

Note 1:
The IME is available on Alcatel-Lucent 4029/4039 Digital Phone sets as of R6.0 and Alcatel-Lucent IP Touch 4028/4038/4068 sets as of R7.0 .

This input method is used for dial by name, customizing programmed key names and editing text messages and configuring the phone names on the Operatorset.

The IME supports Latin, Cyrillic, and Chinese characters. For input of Chinese characters, the IME opens an input session. The type of character is associated with an input method:

Characters	**Input Method**
Chinese - mainland China	Pinyin, Latin
Chinese - Hong Kong	Stroke, Latin
Chinese - Taiwan	Zhuyin, Latin
Russian	Cyrillic, Latin

Note 2:

For the input methods of Pinyin, Stroke and Zhuyin, when the target country is Chinese, or Cantonese, or Taiwanese, these 3 input methods should be used. If not, these 3 input methods are not used.

For the input method of Cyrillic, there are no restrictions. When the current language is Russian, it can be used.

Opening an IME input session:

When one of the Chinese input methods is used, an input session starts when the user presses an alpha key.

The following figure shows the schema of the IME input session. It appears on the bottom softkey line of the set's screen display.

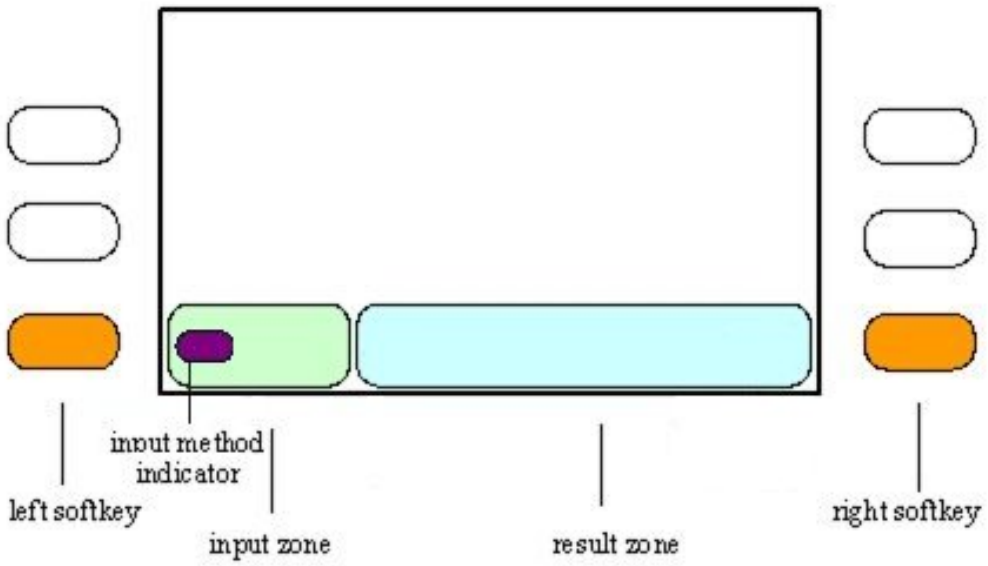


Figure 2.108 : Open the IME input session

The softkeys and areas operate in IME as follows:

- The input area displays characters as the user enters them.

  Note 3:
  For Pinyin input method, Latin characters are displayed in the input area.

- The result area displays the list of candidate characters in the same character type as the input method.
- The input method indicator shows the input method in use.
- The left softkey is used to toggle between input methods.
- The right softkey is not used.

The following screens show an example of the basic operation of an IME input session. In the example the input method is Pinyin.

The following figure shows the IME after the user has entered the letters "yu".

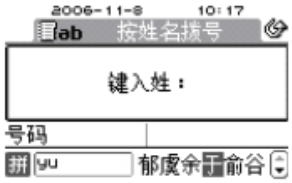


Figure 2.109 : Opened IME session with entered letters

The letters “yu” is displayed in Latin character type in the input area of the IME. The input method indicator shows the current input method is Pinyin. The result area lists candidate Chinese characters for the input letters “yu”.

The way input characters are processed, the resulting candidate characters displayed, and the function of special keys varies according to input method.

Closing an IME input session:

The IME input session closes automatically when no activity is detected from the user. Two timers control this function. When the first timer, T1, expires, it closes the input session without clearing the input and result areas. The second timer, T2, should be greater than T1. When T2 expires, it closes the input session and clears the input and result areas. Both timers are reloaded every time the user presses an alpha key. If the user presses an alpha key after T1 has expired, but T2 has not yet expired, the input session is re-opened with the previous contents of the input and result areas.

The input session also closes when the user presses:

- OK (confirms character choice)
- RELEASE
- Back/Exit

Changing input methods:

The user can change the current input method to any which is configured on the set by pressing + ([alt] + [space]). An input method selector dialogue box pops up, displaying the possible input methods, as shown in the following figure.

Figure 2.110 : Change input method

In the pop-up dialogue box, the user scrolls with [space] (while keeping [alt] pressed), and selects by releasing [alt]. If the Latin or Cyrillic input method is selected, the IME input session closes because it is not used by these input methods.

Note 4:

If the language is Russian, there are no input sessions for Cyrillic, after changing the input method to Cyrillic, it can input Russian character directly on the alphabetic keyboard.

Alternately, when the current Input Method is Pinyin, the user can use the left softkey to toggle between two input methods. In this example, if the user presses the left softkey, the current input method toggles from Pinyin to Latin and the IME input session remains open, as shown in the following figure.

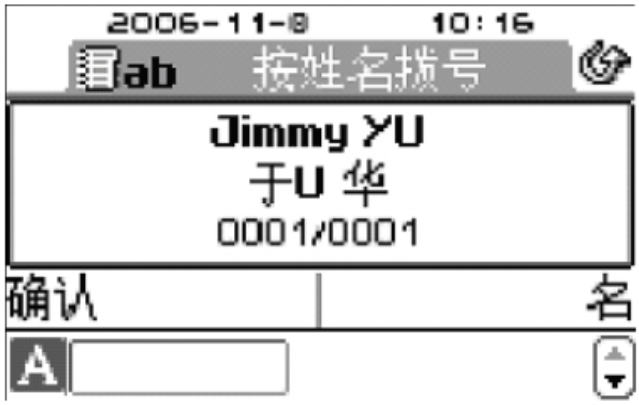


Figure 2.111 : Toggle input method; example screen 1

Now the user can input Latin characters directly without closing the input session. The input method indicator shows that the current input method is Latin. After one Latin character is entered ("U"), the input session closes, although Pinyin is still available as the default input method.

To toggle back to Pinyin, the user presses the left softkey and the input session re-opens, as shown in the following figure.

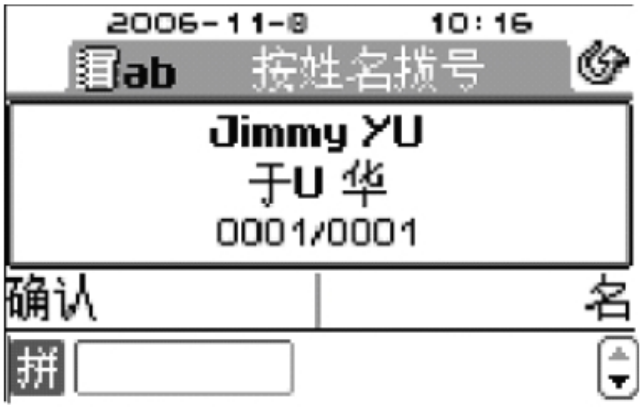


Figure 2.112 : Toggle input method; example screen 2

Input Method for programming a key name:

Each user can program the key name on the phone. In this case, the input session does not, however, close automatically after the user presses OK to confirm a Unicode character. It is kept until the user presses the Back/Exit key, followed by OK to save the key name.

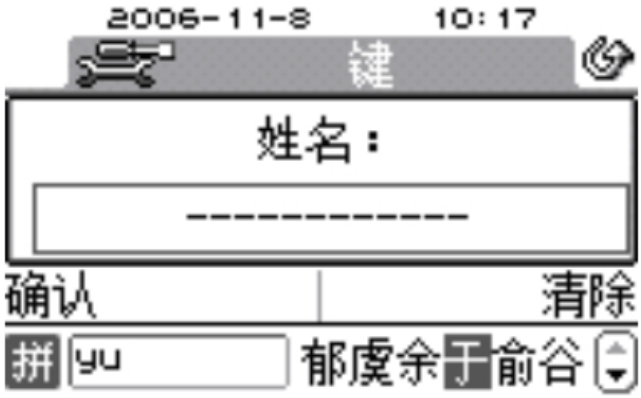


Figure 2.113 : Program a key name

Input Method for programming names on the Operator set:

Note 5:

As of release 6.0 of Alcatel-Lucent OmniPCX Office Communication Server, it is possible to use Unicode - Chinese and Cyrillic -characters.

The administrator of Alcatel-Lucent OmniPCX Office Communication Server can modify all the phone names via the operator set. This case is the same as the one presented above - "Programming a key name". The input session will not close automatically after OK pressed to confirm a Unicode character. It is kept until the user presses the Back/Exit key followed by OK to save the phone name.

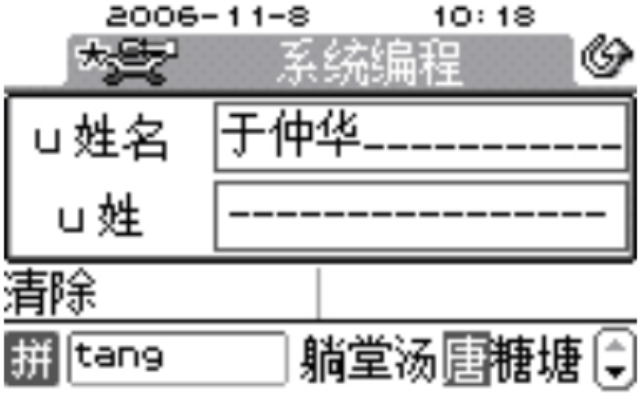


Figure 2.114 : Configure a phone name

2.3.6 Terminal downloading

2.3.6.1 Operation

2.3.6.1.1 Overview

The Alcatel-Lucent 4019 Digital Phone, Alcatel-Lucent 4029 Digital Phone and Alcatel-Lucent 4039 Digital Phone telephone sets contain certain files that are pre-installed in the factory:

- The Alcatel-Lucent 4019 Digital Phone set contains software files.
- The Alcatel-Lucent 4029 Digital Phone and Alcatel-Lucent 4039 Digital Phone sets contain software and data files.

In the latter case, the data files include components such as fonts and ring tones, which may be country-specific.

Alcatel-Lucent OmniPCX Office Communication Server provides the facility for the software and/or data files embedded in the terminals to be updated by the call server if the versions of the embedded files are different from the versions of the equivalent files available in the Alcatel-Lucent OmniPCX Office Communication Server system. In this case, the relevant files are normally downloaded from the system to the terminal when the terminal is restarted.

Note:

New terminal software versions may become available in the system when the system is updated with new Alcatel-Lucent OmniPCX Office Communication Server software. Updates of the files embedded in the terminals may then be required.

2.3.6.1.2 Timing

The terminal download mechanism is activated when a terminal is restarted. During the restart phase, the versions of the files embedded in the terminal are compared with the versions of the same files available for download from the system. If the two versions of the same file are different, a download request is sent to the call server. When the call server detects a download request from a terminal, the terminal is entered into a queue of terminals waiting for downloads.

Note:

A terminal may also request a download during the restart phase if the files inside the terminal have been corrupted, or if the previous download failed or was interrupted.

The user can delay a terminal download so that it is performed at a specified time (date and hour). This allows terminal downloading to be performed at a convenient time, such as during business closing hours or at weekends.

Other deviations from the normal download procedure are also possible:

- The user can specify that the next terminal download will be performed following the next software swap (when the system switches to running the new software).
- The user can force a download, even if the versions of the embedded files are the same as the versions of the equivalent files in the system.
- The user can choose to forbid downloads, even if the versions of the embedded files are different from the versions of the equivalent files in the system.

The timing of terminal updates is configured in the OMC tool, which presents the following options:

- **No Downloading:** There will be no updates to the files embedded in the terminals.
- **Download after swap:** New files will be downloaded to the terminals following the next software swap.
- **Delay Downloading at:** New files will be downloaded to the terminals at the specified date and time.
- **Download immediately:** New files will be downloaded to the terminals immediately (a forced download).

2.3.6.1.3 Operation

During a terminal download, the following conditions apply:

- The terminal cannot be used (the call server puts the terminal out of service).
- The terminal must not be re-configured (with the configuration tools).
- If a problem occurs during a download, the download is attempted a second time. If the problem persists, the terminal is put out of service.
- If a terminal download is not performed within a certain timeout period from the time of the download request, the terminal is reset. See the note below.
- If two terminals share the same telephone resources, they cannot be updated simultaneously - the downloads to the two terminals are performed sequentially.

Note:

If a timeout occurs during a download, you are advised to disconnect and then reconnect the terminal to the system, so that the download procedure restarts.

2.3.6.1.4 Duration

The time taken to complete a terminal download depends on the number of terminals that are being updated at the same time, as well as how and where the terminal is connected to the system, as follows:

- The more terminals there are to be updated, the longer the expected wait for an individual

terminal to be updated.

- Downloads to terminals connected to extension cabinets take longer than to terminals connected to the main cabinet.
- Downloads to terminals with shared system connections take longer than to terminals with dedicated system connections.

2.3.7 V24/CTI Interface Module

2.3.7.1 Hardware description

2.3.7.1.1 Overview

The V24/CTI Interface Module allows a Data Terminal Equipment (DTE) to be connected to the OmniPCX Office, via a UA link, by means of an RS232 serial link (CTI port) or a V24 link.

The V24/CTI Interface Module can be used alone or combined with an Alcatel-Lucent 9 series set.

The V24/CTI Interface Module replaces the 4093 PLUGWARE V24/CTI. The two interface modules can operate together: a data link can be set between an V24/CTI Interface Module Interface Module and a 4093 PLUGWARE V24/CTI.

Note:

The V24/CTI Interface Module is also compatible with UA 3G sets.

CTI port

The RS232 serial link carries signalling (up to 9600 bit/s) and allows telephone operations such as call management and call monitoring. The audio part is carried out by the associated dedicated set.

V24 port

The V24 port is considered as a DCE and provides a capacity of 19200 bit/s (ECMA 102) for an asynchronous V24 transmission. The electrical interface complies with the V28 recommendation of the CCITT.

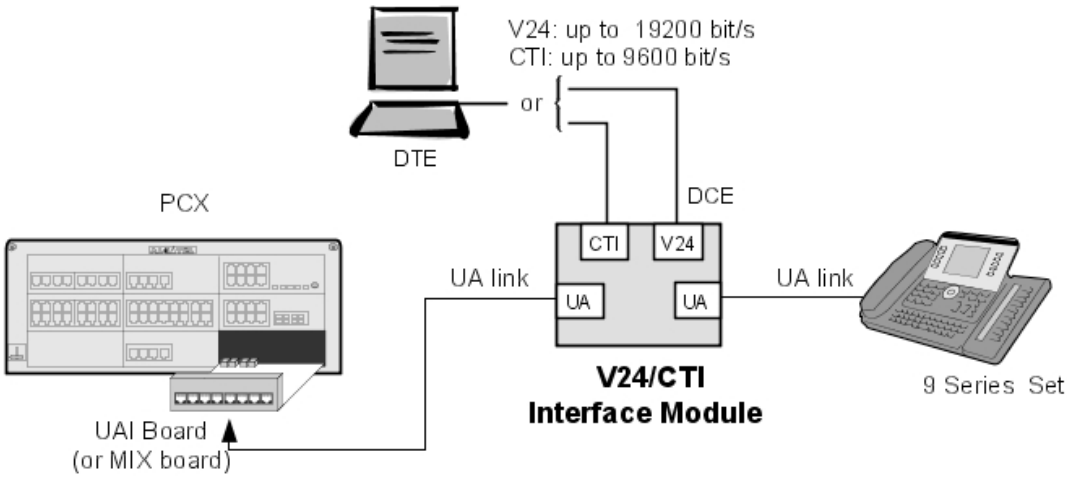


Figure 2.115 : V24/CTI Interface Module Configuration Example

2.3.7.1.2 Compliant Standards

Safety Requirements

- EN60950: European requirements
- UL 1950: US requirements
- CAN/CSA-C22.2 No 950-95: Canada

ECM

- EN55022: Limits and methods of measurement of radio interference characteristics of information technology equipment
- EN55024: Limits and methods of measurement of immunity characteristics of information technology equipment
- FCC part15: US requirements

V24 & CTI

- CCITT Rec.: V24,V28, V25bis, V54, V110
- Hayes protocols
- ECMA 102: Attachment requirements for pan-European approval for connection to PSTN of TE (excluding TE supporting the voice telephony service) in which network addressing, if provided, is by means of DTMF signalling

Environment Classes

- ETS 300 019: Environmental conditions and tests for telecommunication equipment:
  - Part 1-1: Storage
  - Part 1-2: Transportation
  - Part 1-3: Environmental conditions

Eco Design

- ISO 14040: Environmental management – Life cycle assessment – Principles and framework (1997)
- RoHS

2.3.8 AP Interface Module

2.3.8.1 Hardware description

2.3.8.1.1 Overview

The AP Interface Module (Analog Peripheral) allows an analog device such as fax, modem, minitel, answering machine to be connected to the Alcatel-Lucent OmniPCX Office Communication Server via a UA link.

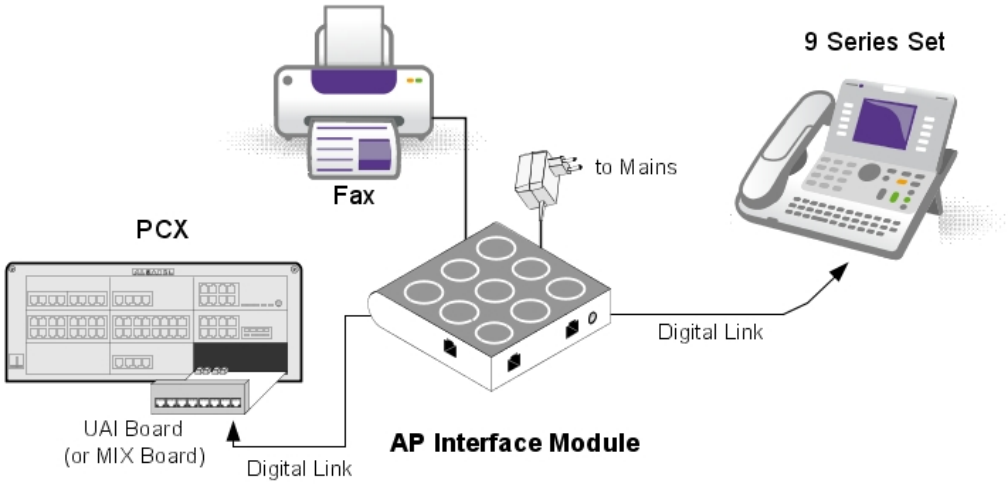


Figure 2.116 : Example of Configuration with an AP Interface Module

AP Interface Module can be used alone or combined with an Alcatel-Lucent 9 series set.

Note:

The AP Interface Module is also compatible with Alcatel Reflexes sets.

AP Interface Module powers the analog device (DTMF signalling, ringer) and, to do this, requires an external power supply (230V AC/30V AC adapter). In this document, this set is called Z set.

2.3.8.1.2 Compliant Standards

Safety Requirements

- EN60950: European requirements
- UL 1950: US requirements
- CAN/CSA-C22.2 No 950-95: Canada

ECM

- EN55022: Limits and methods of measurement of radio interference characteristics of information technology equipment
- EN55024: Limits and methods of measurement of immunity characteristics of information technology equipment
- FCC part15: US requirements

Analog Transmission

- ETS 300 439: Business TeleCommunications (BTC); Transmission characteristics of digital Private Branch eXchanges (PBXs)
- TBR21: Attachment requirements for pan-European approval for connection to PSTN of TE (excluding TE supporting the voice telephony service) in which network addressing, if

provided, is by means of DTMF signalling

Environment Classes

- ETS 300 019: Environmental conditions and tests for telecommunication equipment:
  - Part 1-1: Storage
  - Part 1-2: Transportation
  - Part 1-3: Environmental conditions

Eco Design

ISO 14040: Environmental management – Life cycle assessment – Principles and framework (1997)

2.3.9 S0 Interface Module

2.3.9.1 Hardware description

2.3.9.1.1 Overview

The S0 Interface Module allows an S0 bus (2 B + 1 D channels) to be connected to the Alcatel-Lucent OmniPCX Office Communication Server via a UA link. This bus allows S0 terminals (S0 sets, PCs equipped with an S0 interface, Fax G4, modem, etc.) to be connected.

The S0 Interface Module can be used alone or combined with an Alcatel-Lucent 9 series set.

Note:

The S0 Interface Module is also compatible with Alcatel Reflexes sets

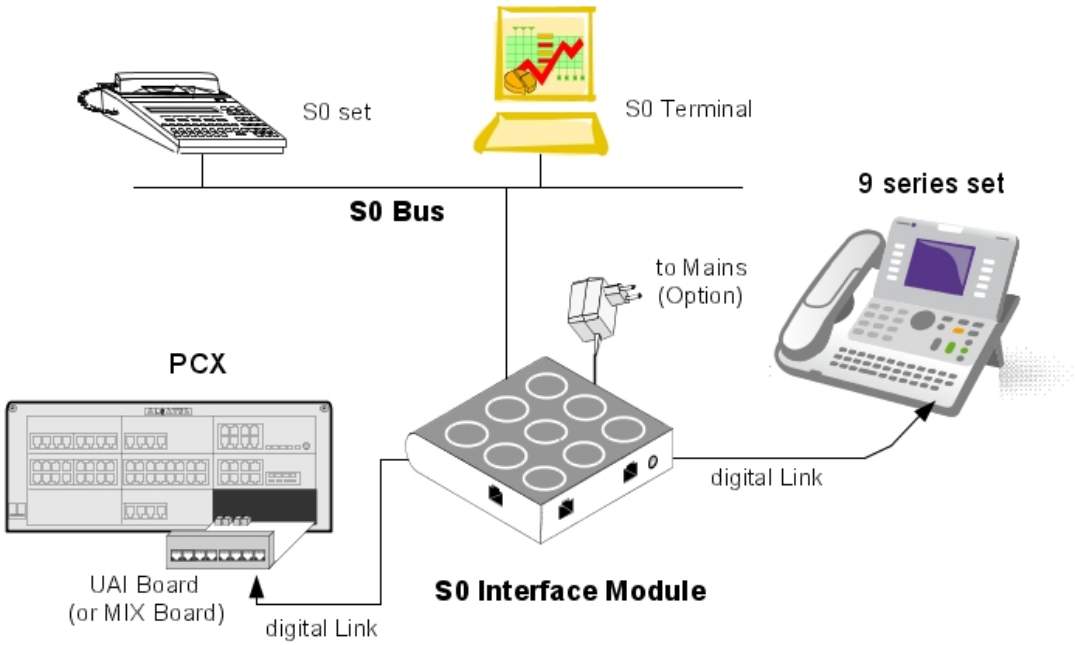


Figure 2.117 : Example of Configuration with an S0 Interface Module

The S0 module provides an S0 bus supplying power. An external power supply (230V AC/48V DC adapter) is required.

There are two possible operating modes on the S0 bus:

- Non permanent layer: layer 1 must be set up by the calling end (PCX or terminal) at the start of each call; layer 1 is shut down at the end of the call
- Permanent layer: operation of the S0 bus depends on the direction in which the initial call was set up:
  - If the call was set up from the PCX to the terminal, layer 1 is kept when the call ends.
  - If the call was set up from the terminal to the PCX, layer 1 is shut down at the end of the call. It must be set up again for the following call. If operation is incompatible with the terminal used, there are two possible solutions: Either layer 2 is kept, this prevents layer 1 being shut down, or, layer 1 is set up from the PCX by making a call to the terminal. The call does not need to get through.

2.3.9.1.2 Compliant Standards

Safety Requirements

- EN60950: European requirements
- UL 1950: US requirements
- CAN/CSA-C22.2 No 950-95: Canada

ECM

- EN55022: Limits and methods of measurement of radio interference characteristics of information technology equipment
- EN55024: Limits and methods of measurement of immunity characteristics of information technology equipment
- FCC part15: US requirements

ISDN

- ETS 300 012: Basic user-network interface layer 1 specification and test principles
- TBR3: Attachment requirements for terminal equipment to connect to an ISDN using ISDN basic access
- ETS 300 047: Basic access-safety and protection
- I.430: Basic user-network interfaces layer 1 specification

Environment Classes

- ETS 300 019: Environmental conditions and tests for telecommunication equipment:
  - Part 1-1: Storage
  - Part 1-2: Transportation
  - Part 1-3: Environmental conditions

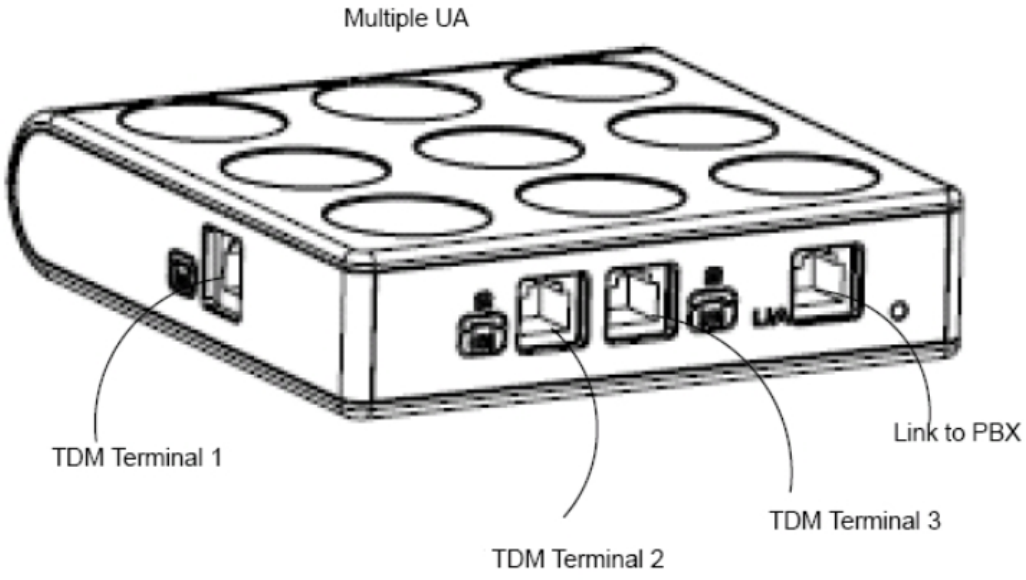
Eco Design

ISO 14040: Environmental management – Life cycle assessment – Principles and framework (1997)

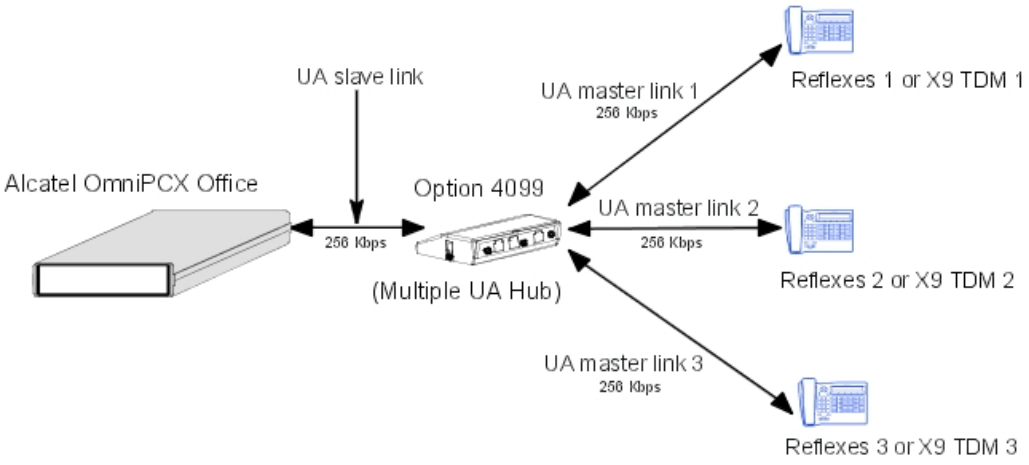
2.3.10 Multi-Reflexes 4099 Hub

2.3.10.1 Hardware description

The Multi Reflexes 4099 Option (also called Multiple UA Hub) connects up to 3 Alcatel Reflexes terminals or Alcatel-Lucent 9 series terminals to an Alcatel-Lucent OmniPCX Office Communication Server, using just one UA link. It simplifies the installation of additional Reflexes or Alcatel-Lucent 9 series terminals.



The Option 4099 (Multiple UA Hub) separates a UA slave link with three B channels into three UA master links with one B channel each.



The Option 4099 (Multiple UA Hub) is connected to the Alcatel-Lucent OmniPCX Office Communication Server just like any terminal, and the three UA terminals are connected to the option through RJ11-RJ11 cables. (By default, 1x3 m and 2x10 m)

The following terminals can be connected to an Option 4099:

- Alcatel Reflexes 2G sets with or without add-on modules (a maximum of 3 modules per

Option 4099)

- Alcatel Reflexes 3G sets with or without add-on modules or the 4091 CTI option (add-on modules and 4091 CTI option are mutually exclusive)
- Alcatel-Lucent 9 series terminals (4019, 4029, 4039 sets based on X9 protocol and using a UA link) with add-on or electronic add-on modules
- a 4088 adapter with a V24 4083 ASM board

The following terminals **cannot** be connected to an Option 4099:

- DECT 4070 IO/EO base stations
- Alcatel Reflexes 2G sets with options 4084 IS/ISW or 4085 AB
- Alcatel Reflexes 3G sets with options 4093 ASY-CTI, 4094 ISW, 4094 ISW-CTI or 4095 AP
- another Option 4099, between the Alcatel-Lucent OmniPCX Office Communication Server and the current Option 4099
- Alcatel 2G/3G or x9 option in TA mode (4093 IS/ISW or 4095 AP without set)

Maximum distances between Alcatel-Lucent OmniPCX Office Communication Server and sets

The line maximum length depends on the power required by each set and option, the voltage, the guaranteed minimum current delivered by Alcatel-Lucent OmniPCX Office Communication Server, the topology of connections and the line diameter:

- With a 0.4-mm cable: 325 m
- With a 0.5-mm cable: 505 m
- With a 0.6-mm cable: 730 m

Note:

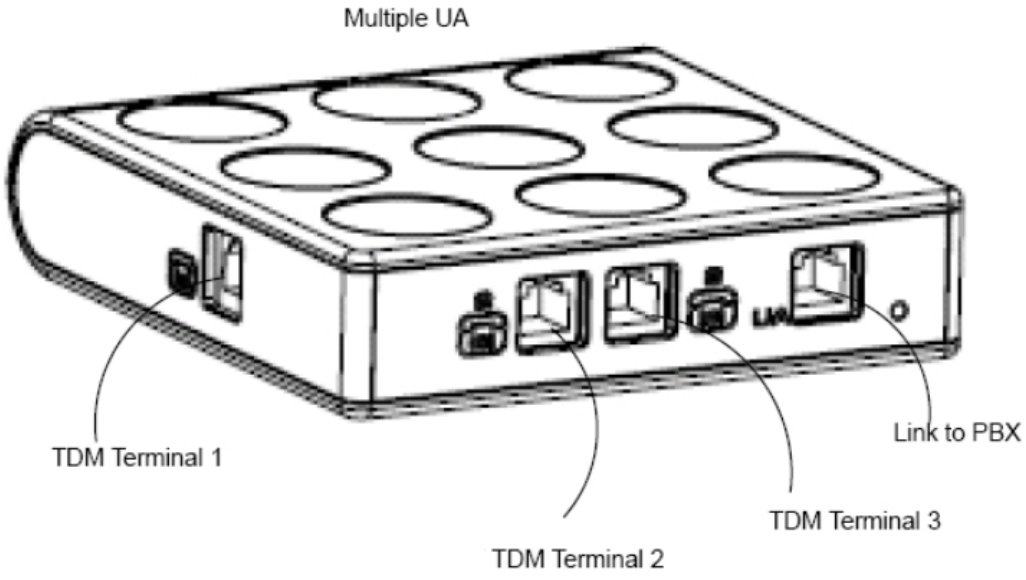
Put the hub near Alcatel-Lucent OmniPCX Office Communication Server to optimise the line length.

Power feeding constraints

Each terminal requires a minimum power and voltage to work properly.

The maximum power for hub and sets (3.5 W) is reached with the following configurations:

- 3 UA Alcatel-Lucent 9 series sets + 3 add-ons
- 3 UA sets + 1 CTI option
- 2 UA sets + 2 CTI options



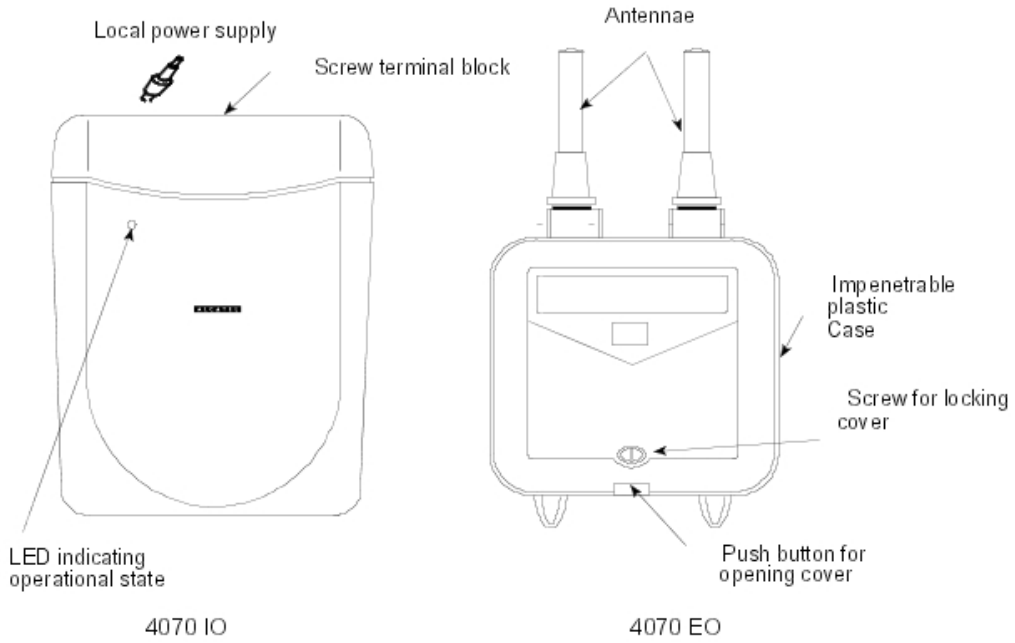
2.3.11 Base Stations

2.3.11.1 Hardware description

2.3.11.1.1 4070 IO/EO DECT BASES

The DECT 4070 IO/EO (internal/external) base station can be connected to:

- 1 UA interface: 3 DECT channels
- 2 UA interfaces: 6 DECT channels



Maximum connection distances with remote power supply:

- 600 m with SYT 0.5 mm cable
- 850 m with LY278 0.6 mm cable

Local Power Supply

It is possible to connect a local power supply (230V/42V – 150 mA adapter) to an accessible socket on the lower part of the 4070 IO/EO base.

The local power supply is used in the following cases:

- main power supply not authorized on the line's wires (depending on specific installation requirements)
- to increase the cable length between the interface and the station
- reduction in the system's electrical consumption.

When the external power supply is connected, the base passes automatically to local power supply mode. In the event of a power cut, the base is not supplied.

States of the correct operation LED

State of the base station	State of the LED
No power supply (local or remote) or fault on base	Off
Fault after auto-test, base not operational	On
Auto-test OK, base station operational. Normal operation for a base with 2 links.	1s on / 1 s off
Auto-test OK, base station operational. Normal operation for a base with one Master link only.	1s on / 200 ms off

Master link not connected, local power supply or slave link connected.	50 ms on / 50 ms off

Differences between 4070 and 4070 NG base stations

- Fast antenna diversity on 4070NG bases (for more details, see "Installing base stations" in the Mobility section.

2.3.11.1.2 4070 PWT BASES

The 4070 PWT (Personal Wireless Telecommunications) bases constitute an adaptation of the bases to the DECT standard for the North American market (essentially the United States).

The 4070 PWT bases are designed for an internal installation only (wall attachment) and they are mechanically identical to the 4070 IO bases. They conform to the "FCC part 15 A, B, C, D requirements" standards.

2.3.12 300/400 DECT Handset

2.3.12.1 Hardware description

2.3.12.1.1 Overview

Alcatel Mobile Reflexes 100 and Alcatel Mobile Reflexes 200 are extended with 2 new models:

- **Alcatel-Lucent 300 DECT Handset** : a handset with a black & white display. It offers a convenient solution for *basic* mobility needs.
- **Alcatel-Lucent 400 DECT Handset** : a handset with colour display. It offers a convenient solution for *intensive* mobility needs.

All Alcatel-Lucent 300 DECT Handset and Alcatel-Lucent 400 DECT Handset, like other DECT handsets, are intended to be carried by users roaming throughout the workplace. These two new handsets offer :

- access to all added value voice services of Alcatel-Lucent OmniPCX Office Communication Server telephone features.
- enhanced usability through functions like:
  - aesthetic renewal,
  - integrated antenna,
  - backlight display,
  - quality of audio reception,
  - vibrator,
  - great autonomy (Li-Ion technology),
  - belt clip availability.

Alcatel-Lucent 300 DECT Handset and Alcatel-Lucent 400 DECT Handset handsets operate in either:

- standard GAP mode, or
- advanced GAP (AGAP) mode.

Alcatel-Lucent 300 DECT Handset and Alcatel-Lucent 400 DECT Handset have the same features and interface as Alcatel Mobile Reflexes 200. For more information, see module Mobile Reflexes Handset - Services provided .

2.3.12.1.2 Characteristics

Handset characteristics

Features	Alcatel-Lucent 300 DECT Handset	Alcatel-Lucent 400 DECT Handset
Dimensions (mm)/(in)	120x45x22/4.72x1.77x0.87	120x45x22/4.72x1.77x0.87
Weight (gm)/(oz)	110/3.88	110/3.88
Volume (cm^3)	119	119
Graphic display (*)	96x48 Black&White	98x66 4096 colours
Loudspeaker	No	Yes
Multi-line management	Yes	Yes
Dial-by-name	Yes	Yes
Headset connection (standard wiring)	No	Yes
Backlight display	Yes	Yes
Backlight Keypad	No	Yes (blue)
Vibrator	Yes	Yes
Browser	Yes	Yes
Battery pack	Li-Ion	Li-Ion
Colour	Black	Black
Explosion proof	No	No
Belt clip	Yes (removable)	Yes (removable)
Talk / Standby time (h)	Up to 20 / 160	Up to 20 / 120

(*) screen content depends on the system used.

Characteristics of charging units, accessories and headsets

Charging units

Charging units for Alcatel-Lucent 300 DECT Handset and Alcatel-Lucent 400 DECT Handset are available in 2 models:

a. Basic desktop charger (included with the delivered handset):
This model is a charging base unit with no charge indicator LED. The handset displays the battery status. Power supply is independent from the charging base.

Figure 2.122 : Basic desktop charger

b. Dual desktop charger:
This model allows a handset battery and a spare battery to be charged simultaneously. It is intended for users who require long-term operational availability. It consists of a base with two compartments (handset and spare battery) and a charge indicator LED for the spare battery. Power supply is independent from the charging base.

Figure 2.123 : Dual desktop charger

Battery charger indicator:

- When the handset battery is empty (capacity between 0 - 33%), the battery status icon flashes to 50% of the load max.
- When the handset battery is half-empty (capacity between 33 - 66%), the battery status icon flashes to 50% of the load max.
- When the handset battery is full (capacity between 66 - 100%), the battery status icon does not flash but battery charging continues.

Handset battery charge time:

Two charging cycles are necessary to **fully charge** your handset battery: a rapid charging cycle and a slow one.

A rapid charging cycle of 2 hours charges the handset battery to 82% of its capacity. A slow charging cycle of one additional hour follows the rapid charging cycle and fully charges the handset battery.

The autonomy and life span of the handset battery depend on the usage mode and the environment conditions:

Life span Li-Ion: over 500 cycles with a capacity over 60% of the initial value.

Accessories and headsets

Accessories:

a. Charger bracket:
The Alcatel-Lucent 300 DECT Handset and Alcatel-Lucent 400 DECT Handset mobile

charger units have a "charger bracket" made of metal. The "charger bracket" offers the possibility of mounting the basic or dual charger on a wall.

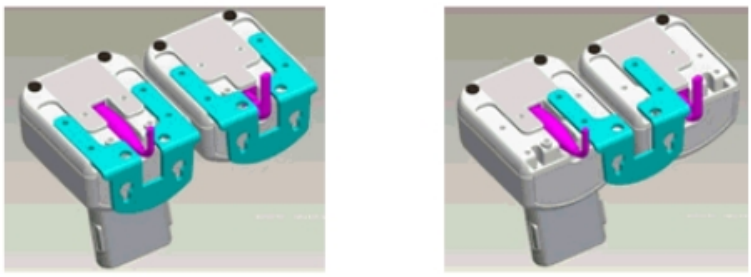


Figure 2.124 : Charger bracket

b. Pouch:
A pouch improves the durability of Alcatel-Lucent 300 DECT Handset and Alcatel-Lucent 400 DECT Handset in severe environments, especially against dust, spraying water and shocks.

Headsets:

The Alcatel-Lucent 400 DECT Handset handset has a standard wiring headset connection. When a headset is connected to a Alcatel-Lucent 400 DECT Handset handset, the microphone and loudspeaker are automatically switched off.

2.3.12.1.3 General view of handsets

and Alcatel-Lucent 400 DECT Handset are designed to suit voice requirements of employees roaming throughout the workplace.

They have similar interfaces. However, the Alcatel-Lucent 400 DECT Handset also has a headset connection (see figure : Alcatel-Lucent 400 DECT Handset).

Figure 2.125 : Alcatel-Lucent 300 DECT Handset

The Alcatel-Lucent 300 DECT Handset has:

1. bi-coloured LED,
2. black & white display screen with white/blue backlight,
3. loudspeaker,
4. correction key,
5. volume adjustment keys,
6. navigate/confirm dual- function key,
7. call management keys,
8. keypad with 12 keys,

(9) company directory key,

(10) microphone,

(11) vibrator management key,

(12) ON/OFF key.

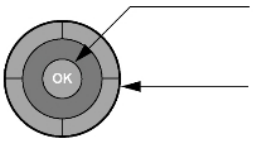
Figure 2.126 : Alcatel-Lucent 400 DECT Handset

The Alcatel-Lucent 400 DECT Handset has all the keys of the Alcatel-Lucent 300 DECT Handset. The Alcatel-Lucent 400 DECT Handset also has:

- one new key: (13) headset connection,
- a key functioning differently: (11) vibrator/group listening management key.

2.3.12.1.4 Keypad: description

The following table lists handset keys and their functions (see figure : Alcatel-Lucent 300 DECT Handset and figure : Alcatel-Lucent 400 DECT Handset).

KEY	Function
	Single press: - seizes line, - switches between calls.
	Long press: redials the last number.
	Single press: - releases line, - switches off ringing.
	Long press: locks/unlocks keypad, when handset is idle only.
	- confirms selection in a menu (icons or text), - navigates a menu or a list.
	moves in a menu (icons) or in a list (text) .
	Single press: - erases the last entered character, - displays the previous menu.
	Long press: erases a field.
	Single press: accesses company directory to "Dial by name" .
	Long press: displays the name and number in the directory.
 (300 DECT™)	Single press: No action.
	Long press: switches between ringer and vibrator, when set is idle only.
 (400 DECT™)	Single press: activates or deactivates group listening (during conversation).
	Long press: switches between ringer and vibrator, when set is in idle mode only.
	Single press: accesses the local menu (vibrator, ringer, keypad lock).
	Long press: switches the mobile on or off.

2.3.12.1.5 Handsets management

Alcatel Mobile Reflexes 100, Alcatel Mobile Reflexes 200, Alcatel-Lucent 300 DECT Handset and Alcatel-Lucent 400 DECT Handset are designed to be used with a Private Automatic Branch eXchange (PABX) and they:

- have the same status icon display.
- have the same call icon display.

- offer similar features.
  For more information on the features offered by Alcatel-Lucent 300 DECT Handset and Alcatel-Lucent 400 DECT Handset, see module Mobile Reflexes Handset - Services provided .
- have the same configuration.

  Note:
  During the installation procedure of Alcatel-Lucent 300 DECT Handset or Alcatel-Lucent 400 DECT Handset ***you must declare the handset in the appropriate frequency band (region) according to the country you find yourself in****.*

  Four frequency bands are specified:

  - *Region 1: Europe band: 10 frequencies 1881.792 to 1897.344 Mhz.*
  - *Region 2: USA/Canada band: 5 frequencies 1921.536 to 1928.448 Mhz with power adaptation.*
  - *Region 3: South America band: 10 frequencies 1912.896 to 1928.448 Mhz.*
  - *Region 4: China band: 10 frequencies 1902.528 to 1918.080 Mhz.*

  For more information on the installation procedure of Alcatel-Lucent 300 DECT Handset and Alcatel-Lucent 400 DECT Handset, see module Registering the handset - Operation .

2.3.13 Pimphony Reflexes

2.3.13.1 Hardware description

For more information, you can also consult the PIMphony documentation supplied with the CD ROM.

The standard Alcatel-Lucent OmniPCX Office Communication Server offering includes an integrated CTI server (TAPI 2.0) that opens up a broad range of third party CTI applications.

PIMphony Reflexes is a PC-based workstation equipped with the following PIMphony applications:

- PIMphony Basic (free of charge)
- PIMphony Pro (requires a software key)
- PIMphony Team (requires a software key)

	PIMphony Basic	**PIMphony Pro**	**PIMphony Team**
Complete set of telephony features	YES	YES	YES
Centralized call log	YES	YES	YES
Integration of Contact Handlers		YES	YES
"Visual Mailbox" interface		YES	YES
Unified messaging		YES	YES
Supervision features			YES
Assistant Feature			YES

For more information about the "Visual Mailbox", interface, consult " Visual Mailbox Interface" in the "Integrated Voice Server" section.

They are installed from the CD-ROM provided in each system.

PIMphony Pro and PIMphony Team are supplied on a Try and Buy basis. The user can test both applications free of charge for 2 months.

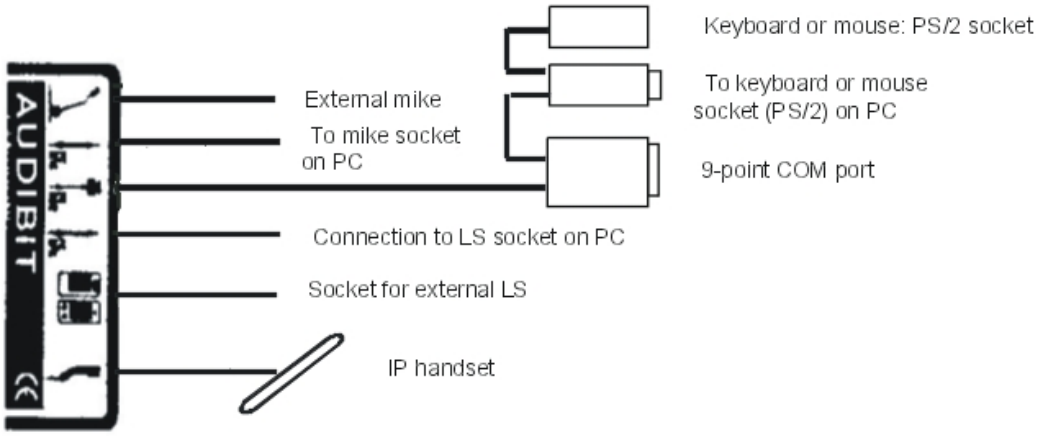
If PIMphony is emulating an IP workstation, it can be used via an IP Comfort handset.

Connecting the Comfort handset

To connect the Comfort handset you need a full duplex sound card.

This handset system uses the loudspeaker and external mike for hands-free operation.

The handset also supports automatic on-hook and off-hook detection via the COM port. This system requires a power supply, conveyed via the keyboard or mouse PS/2 connection.



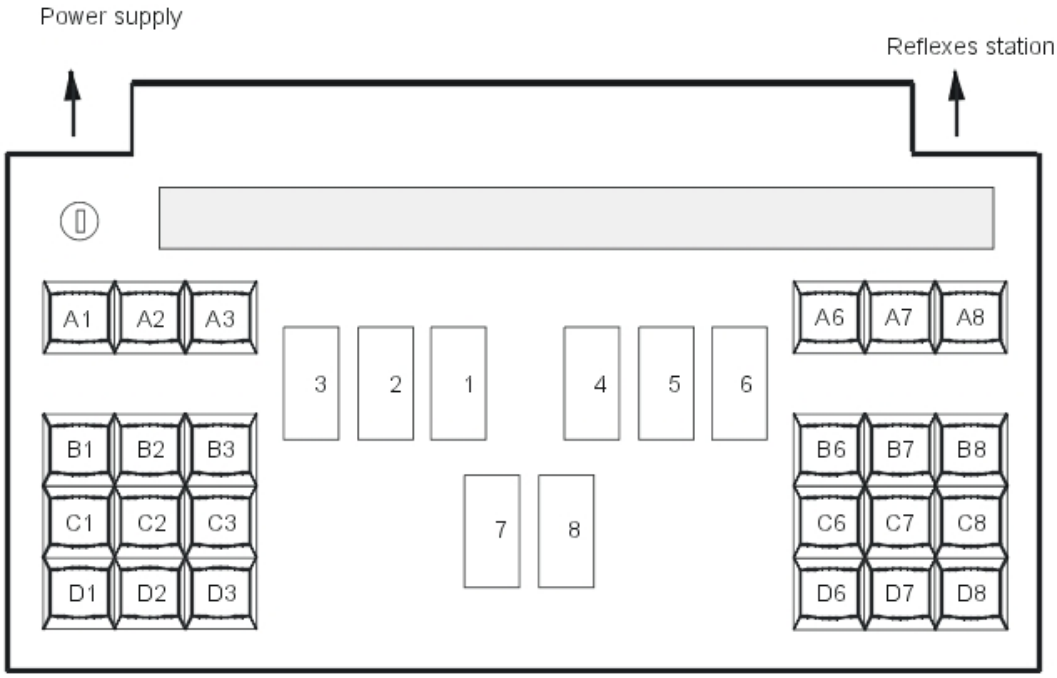
2.3.14 VBTEL Visually Impaired Op. Station

2.3.14.1 Hardware description

The VBTEL terminal is designed to act as a display for visually impaired operators, conveying the information presented on Reflexes terminals. There are 2 models:

- VBTEL 20: equipped with a piezoelectric Braille touchpad with 20 characters and 32 command keys.
- VBTEL 40: equipped with a piezoelectric Braille touchpad with 40 characters and 32 command keys.

The information read in Braille on the terminal enables the operator to use the system entirely via a Reflexes terminal; all the operations (dialing, transfers, line seizures, etc.) are performed from the Reflexes terminal.



Description

The on button is located at the top left of the terminal.

The groups of 12 keys on the right and left side of the terminal make up the command keyboard; the keys are designated by a row letter and a column number (columns 4 and 5 are not used).

The Braille keyboard, in the center, consists of 8 keys, of which the first 6 are the 6 Braille points in Perkins alphabetical order, the 2 others being the backspace (7) and space keys (8).

A set of 20 or 40 piezoelectric cells located above the Braille keyboard enables Braille characters to be displayed. Each cell contains 8 points: points 1 to 6 serve to form the 64 characters of the Braille alphabet; when points 7 and 8 are raised simultaneously, they represent the cursor.

2.3.15 Earlier Generation Sets

2.3.15.1 Hardware description

2.3.15.1.1 TERMINALS NOT SUPPORTED

The following terminals are not supported by Alcatel-Lucent OmniPCX Office Communication Server:

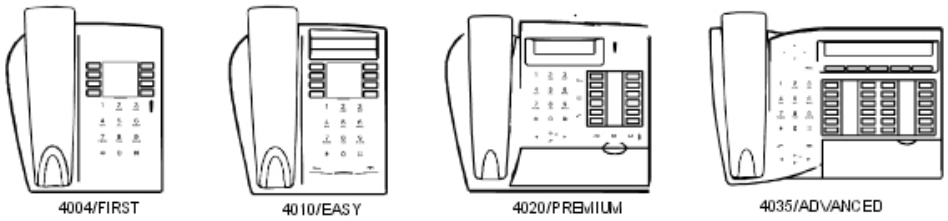
- Reflexes 1G sets
- DECT 4075, 4074B, 4074H and 4074 BEx mobile sets
- Alcatel-Lucent 160 sets
- Alcatel-Lucent 4120 sets (900A and 900B)

- Fast IP Reflexes, e-Reflexes sets and IP enabler

2.3.15.1.2 Reflexes 3G

TERMINAL FEATURES

FEATURE	DEDICATED DIGITAL SETS			
	First	Easy	Premium	Advanced
Handset	YES	YES	YES	YES
Loudspeaker	-	YES	YES	YES
Buzzer	YES	-	-	-
1 x 20 character display	-	YES	YES	-
2 x 40 character display	-	-	-	YES
Pictograms associated with programmable keys	-	-	12	24
Soft keys	-	-	-	5
Programmable keys	8	8	12	24
Fixed function keys	-	5	10	7
Navigator	-	-	-	YES
Numerical keypad keys	12	12	12	12
Green LED	YES	YES	-	-
Two-coloured LED	-	-	YES	YES
Internal alphabetical keyboard	-	-	YES	YES
4090M or 4090L add-on module	-	-	Optional	Optional
Optional modules (plugware)	External	External	Internal/External	Internal/External
Wall mounting	Integrated	Integrated	Optional	Optional
4097 CBL UA/DECT adapter	-	-	Optional	Optional



4097 CBL ADAPTER

Alcatel-Lucent Advanced sets can be equipped with a 4097 CBL UA/DECT adapter and can therefore communicate with the system over a DECT radio link. This device means you no longer have to worry about cabling constraints. An RS232 link is also recommended for CTI applications.

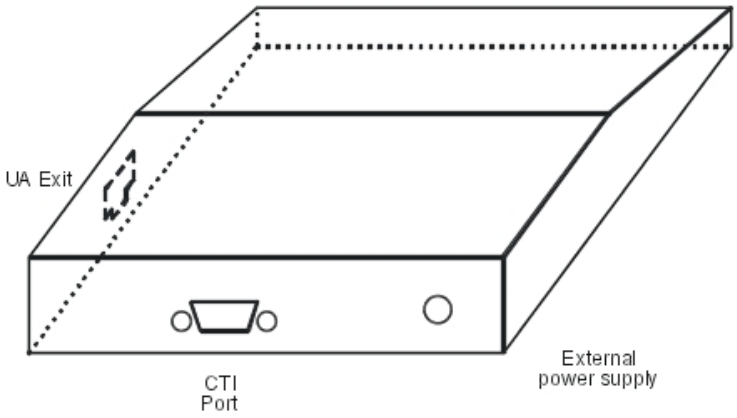
The Advanced set and its adapter are jointly called Advanced DECT/4036.

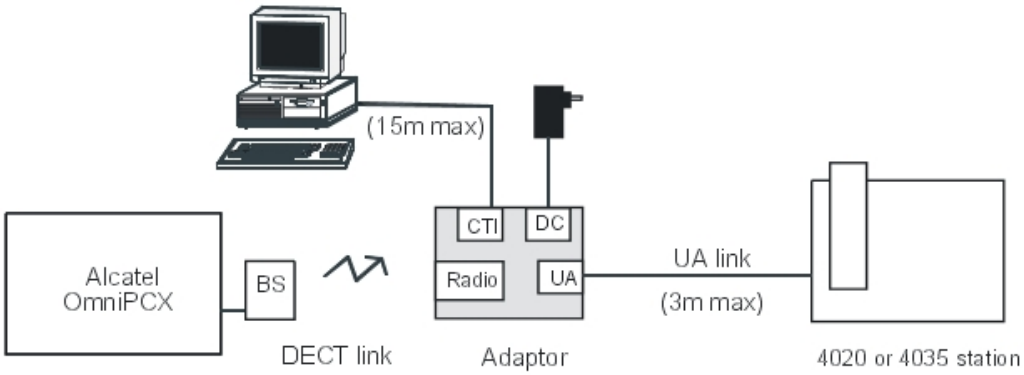
The 4097 CBL adapter is powered by a 220V AC/42V DC power adapter. This power adapter is also a power splitter. The base of the power socket must be positioned as close to the adapter as possible, and must also be easily accessible.

Note:

This adapter can also be used with an Alcatel Premium set (internal installation) or First or Easy sets (external installation).

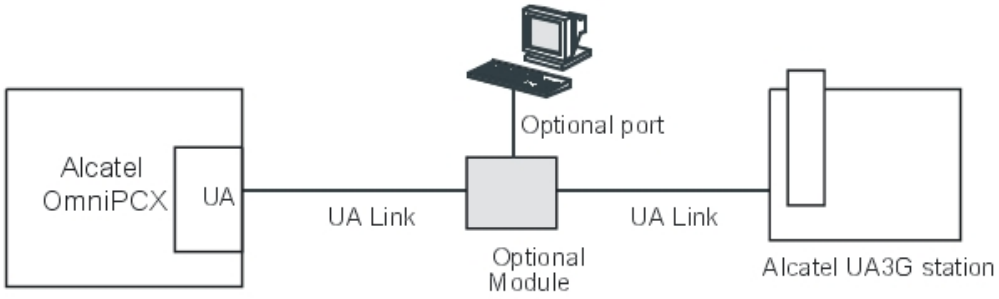
Connection





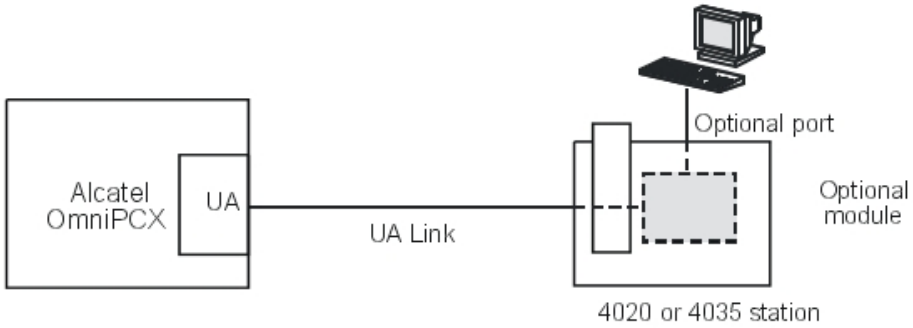
OPTIONAL MODULES (PLUGWARE)

The optional modules are modules which are inserted in the UA link, in series, between a PCX and a dedicated UA set. They provide an interface for connecting terminals to the system.



Note 1:
The optional modules can also be used with Reflexes2G sets (the previous generation).

Alcatel Premium and Advanced sets have a slot under the panel for the optional module.



The optional modules available are:

- 4093 ASY-CTI
- 4094 ISW
- 4095 AP

Note 2:
When the option is used in stand-alone as a TA (Terminal Adapter) interface, you have to move the red jumper to the other connector position inside the module.

4093 ASY-CTI module

This module allows the device to be connected to the system via a UA link (a PC-type peripheral device) by means of an RS232 link (CTI port) and a DTE data terminal (V24 port).

CTI Port

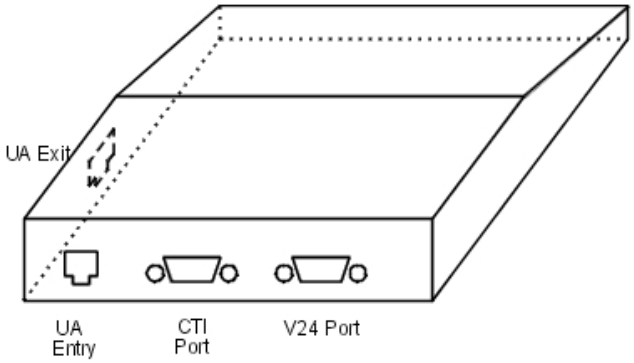
The RS232 serial link carries signalling (up to 9600 bit/s) and allows telephone operations such as call management and call monitoring.

The audio function is performed by the associated dedicated set.

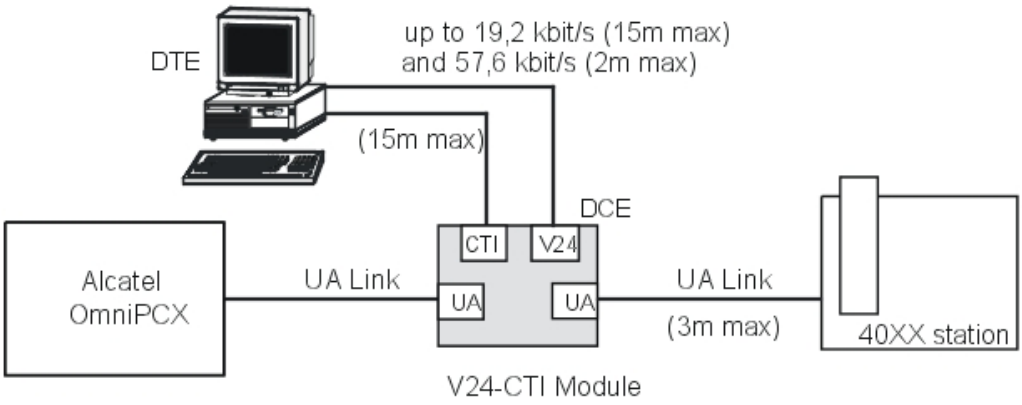
V24 Port

The V24 port is regarded as a DCE and supports asynchronous V24 transmission up to

19,200 bps (ECMA 102) and 57600 bps (V14e). The electrical interface conforms to ITTCC recommendation V28. This port is used to connect up the metering data management system (connection cable provided).



Connection



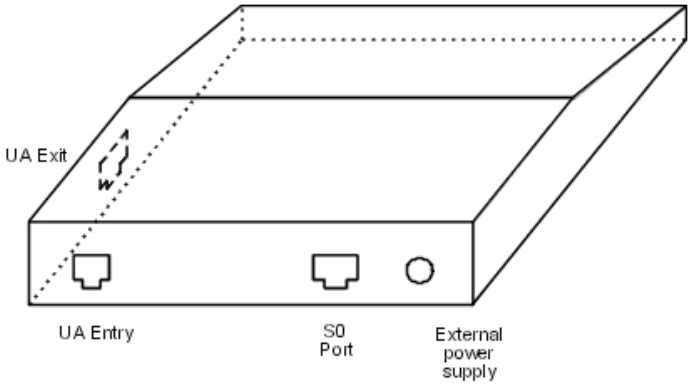
4094 ISW module

This module connects an S0 terminal to the system via a UA link.

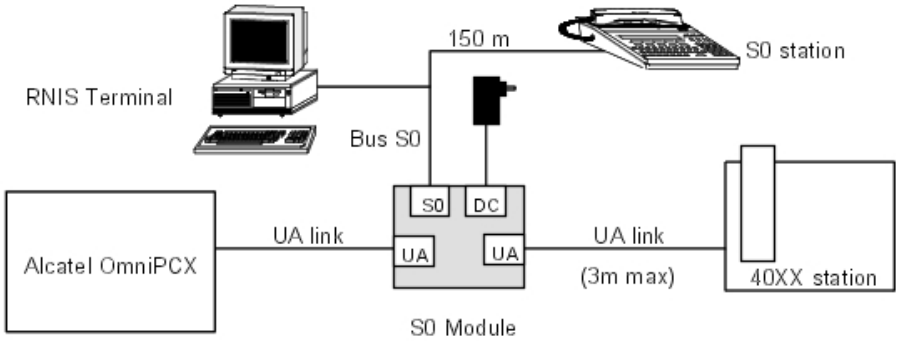
This optional module provides an S0 power bus which requires an external power supply (230V AC/42V DC adapter), allowing terminals without their own power supply (ISDN terminals, etc.) to be connected to the bus.

The power supply transformer serves as a sectioning mechanism for the S0 interface. It must therefore remain easily accessible.

The S0 bus can be a point-to-point or short passive bus covering 150 m (up to 5 terminals, of which a maximum of 2 may be powered remotely). Operation is not guaranteed in the event of a power outage.



Connection

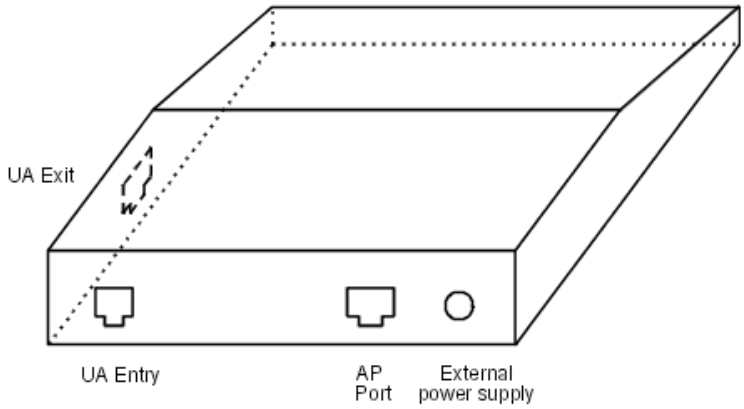


4095 AP module

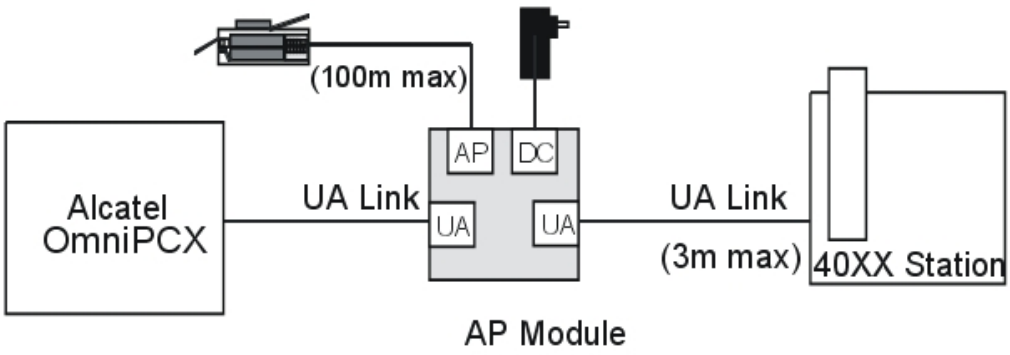
This interface connects an analog peripheral such as a modem, teletex or answering machine to the system via a UA link.

The optional module supplies the terminal (DTMF signalling, ringer) and therefore requires an external power supply (230V AC/30V DC power adapter).

The power supply transformer serves as a sectioning mechanism for the AP interface. It must therefore remain easily accessible. Operation is not guaranteed in the event of a power outage.



Connection



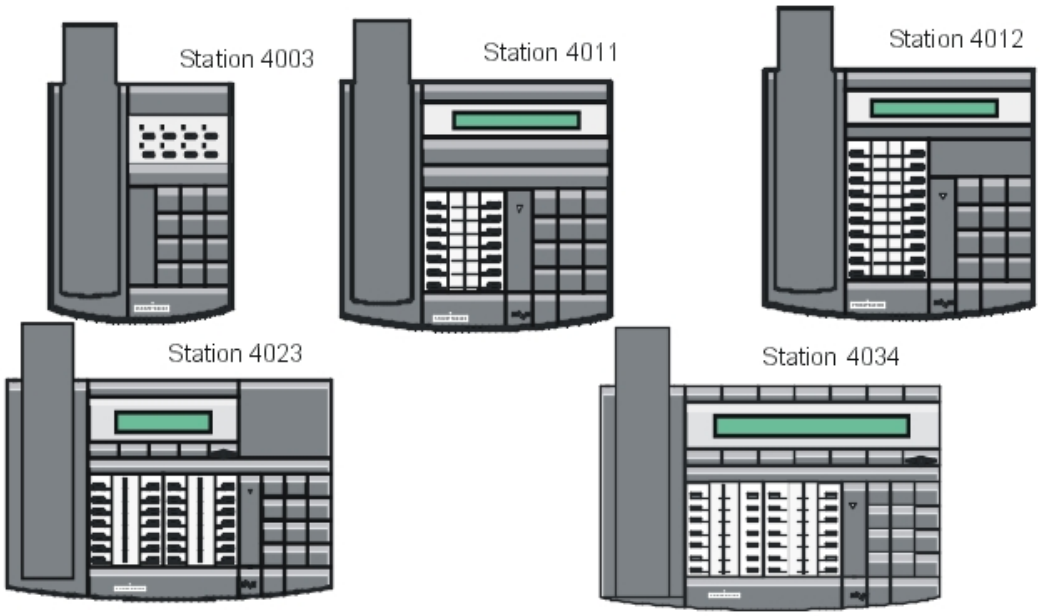
2.3.15.1.3 Reflexes 2G 40XX* SETS

Reflexes terminals from the 2G range are supported by Alcatel-Lucent OmniPCX Office Communication Server for migration purposes.

*Depending on country/distribution network

FEATURE	Characteristics				
	4003	4011	4012	4023	4034
Handset	YES	YES	YES	YES	YES
Loudspeaker	YES	YES	YES	YES	YES
Display	-	1 x 20	1 x 20	2 x 20	2 x 40
Pictograms	-	2 x 7	2 x 10	4 x 7	4 x 7
Soft keys and arrows	-	-	-	3 + 1	10 + 1
Programmable keys	5	6	10	18	18
Fixed function keys	3	10	12	12	12
Numerical keypad keys	12	12	12	12	12

3-coloured LED	-	YES	YES	YES	YES
4087 IFA internal alphabetical keyboard	-	-	-	YES	YES
4087 EFA external alphabetical keyboard	-	-	Optional	Optional	Optional
Interface: 4083 ASM or 4083 PCT, 4084 IS/ISW or 4085 AB	-	-	Optional	-	Optional
4081L or 4081 M add-on module	-	-	Optional	Optional	Optional
Wall mounting	Optional	-	-	-	-



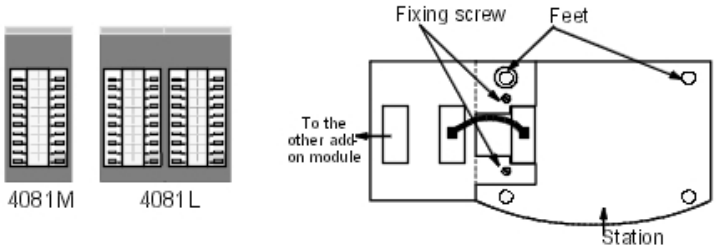
2.3.15.1.4 MOUNTING THE ADD-ON MODULES

A kit (a 10-cm cable with two 8-pin modular jacks) connects the 4081M or 4081L add-on modules to 4012, 4023, and 4034 sets (there is no limit to the number of add-on modules in the system).

Procedure

- Turn the set and the module upside down
- Connect the cable to the set and the module
- Join the module to the set using the 2 screws provided in the kit

The same method is used to connect the 2 modules to each other.

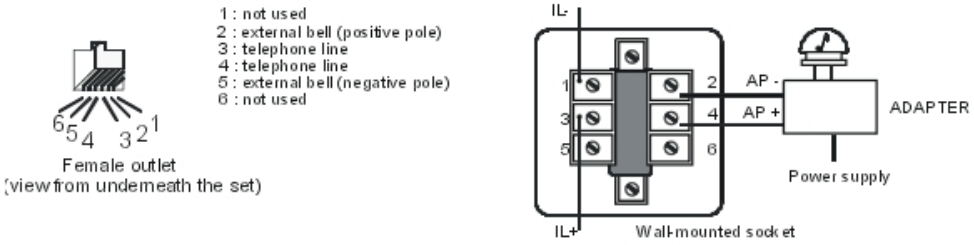


2.3.15.1.5 CONNECTING AN EXTERNAL BELL

It is possible to connect, on the wall-mounted socket, an external call reinforcing bell to 4011, 4012, 4023 and 4034 sets.

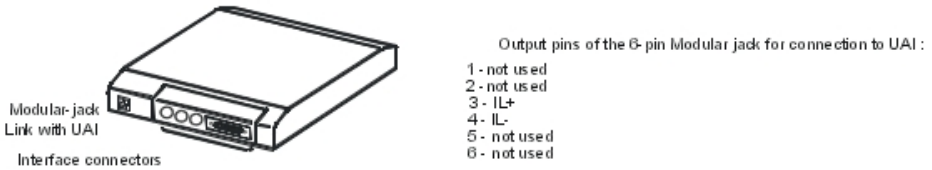
The standard connecting cable is 3 m long and has 2 conductors. To connect an external ringer, replace this cable with an optional cable, 5 m long with 4 conductors.

Available power: 2 mA under 5V (an adapter is required).



2.3.15.1.6 CONNECTING THE 4088 ADAPTER

The 4088 adapter is connected directly to an Alcatel-Lucent UA set interface and enables the installation of an optional 4083 ASM, 4083 PCT, 4084 IS/ISW or 4085 AB board.



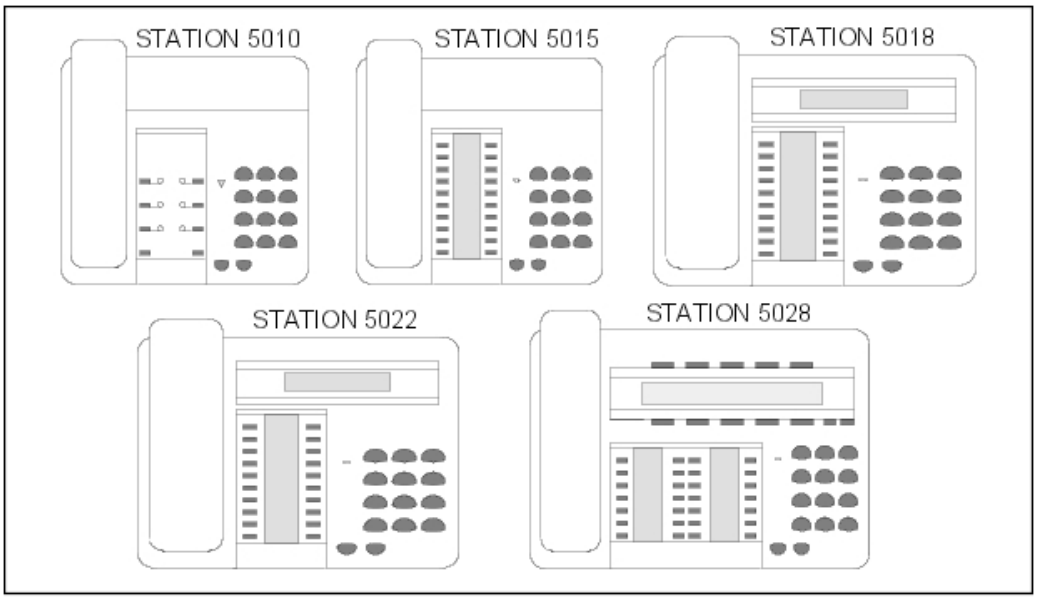
2.3.15.1.7 Reflexes 2G 50XX * SETS

Reflexes terminals from the 2G range are supported by Alcatel-Lucent OmniPCX Office Communication Server for migration purposes.

*Depending on country/distribution network

FEATURE	Characteristics				
	5010	5015	5018	5022	5028

Handset	YES	YES	YES	YES	YES
Loudspeaker	YES	YES	YES	YES	YES
Display	-	-	1 x 20	1 x 20	2 x 40
Pictograms	-	2 x 10	2 x 10	2 x 10	4 x 7
Soft keys and arrows	-	-	-	-	10 + 1
Programmable keys	5	10	10	10	18
Fixed function keys	5	12	12	12	12
Numeric keypad keys	12	12	12	12	12
LED	YES	YES	YES	YES	YES
Internal alphabetical keyboard	-	-	-	-	YES
External alphabetical keyboard	-	-	Optional	-	Optional
V24/MAC PC 5083, S0 (2B + D) 5081/5082 or Z 5088 interface	-	-	Optional	-	Optional
40-key add-on module	-	-	Optional	-	Optional



2.3.15.1.8 OPTIONS FOR UA 2G SETS

4012, 4034, 5022 and 5028 sets on the Alcatel-Lucent OmniPCX Office Communication Server system can take an optional interface that plugs into the rear of the set:

- 4083 (or 5083) ASM : V24 - MAC/PC option
- 4083 PCT : PC option
- 4084 (or 5081/5082) IS/ISW : S0 - MAC/PC option
  S0 (2 B channels and 1 D channel) is available via a 4084 IS/ISW option installed on a 40XX set which is connected to a DLC16 board (16, 8 or 4 devices).
  S0* (1 B channel and 1 D channel) is available via a 4084 IS/ISW option installed on a

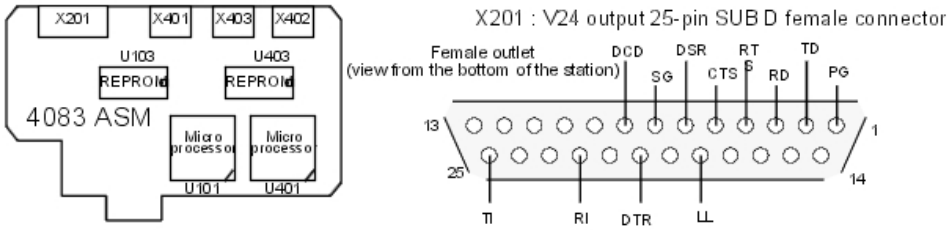
40XX set which is connected to a DLC4/8 board with an S01B daughter board.

- 4085 (or 5088) AB : Z option

Connecting V24 and MAC/PC terminals

V24 terminals are connected using the X201 connector of board 4083 ASM installed in the set.

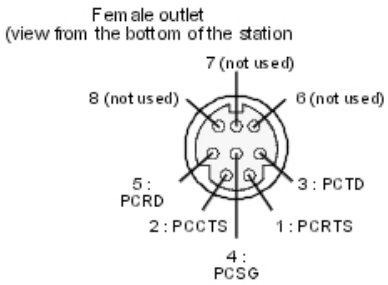
MAC/PC terminals are connected using connectors X401, X402 and X403 of boards 4083 ASM and 4084 IS.



Function	Circuit	Signal
Protection ground	101	PG
Transmitting data	103	TD
Receiving data	104	RD
Request to send	105	RTS
Clear to send	106	CTS
Data set ready	107	DSR
Signalling ground	102	SG
Carrier detection	109	DCD
Local loop	141	LL
Data terminal ready	108/1, 2	DTR
Call indicator	125	RI
Test indicator	142	TI

Maximum distances between terminal and set: 15m at 19200 bps 2 m at 57600 bps

X401: 8-pin Jack connector for PCs



Pin	Signal	Function	Circuit
1	PCRTS	Request to send	105
2	PCCTS	Clear to send	106
3	PCTD	Data transmission	103
4	PCSG	Signalling ground	102
5	PCRD	Data reception	104
6			
7			
8			

X402, X403: 4-pin Jack connector for Macs

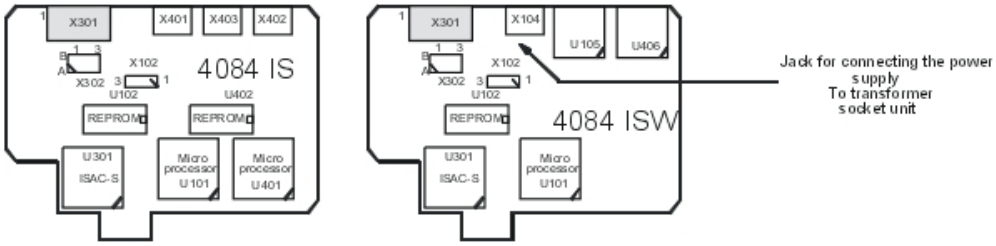
The maximum length of the ADB link is 5 m.

These two connectors enable the terminal and keypad to be connected separately.

Connecting S0 terminals

Options 4084ISW and 4084 IS enable the connection of S0 terminals supplied remotely or otherwise.

The terminals are connected using the 8 pin connector (X301) of boards 4084 IS and 4084 ISW. The type of bus is specified by the positioning of the X102 connector jumpers. X302 defines the termination resistance of the 2 connection pairs.



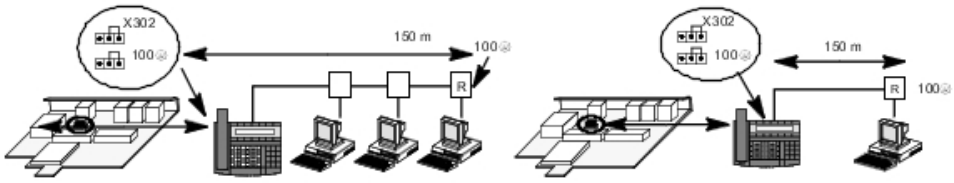
X104: connector for the power supply

- 1: - 48 V - 2: + 48V

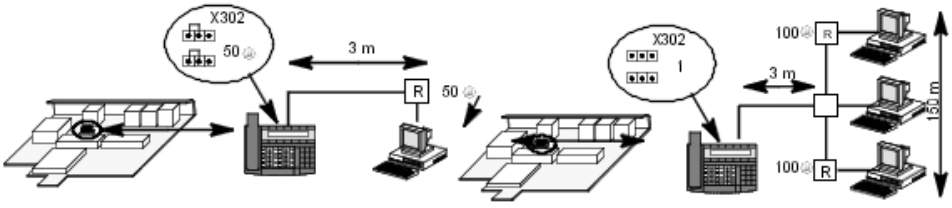
X301: connector for the S0 bus

- 1 and 2 - not used - 5 - TX -
- 3 - RX + - 6 - RX -
- 4 - TX + - 7 and 8 - not used

Short passive bus Long point-to-point bus (X102 across 1-2) (X102 across 2-3)



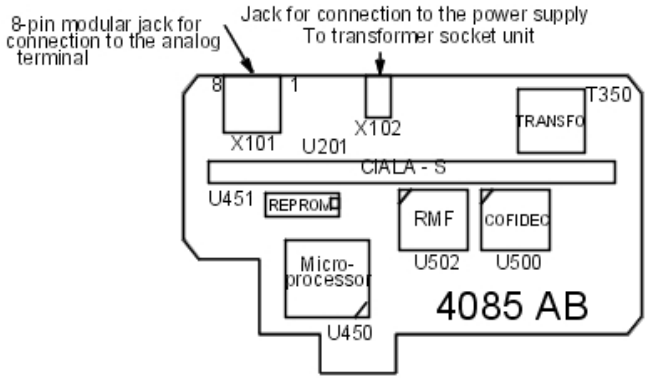
Short point-to-point bus Extended bus (X102 across 1-2) (X102 across 2-3)



Connecting analog terminals

The Z station interface is of type TNV (Telecommunication Network Voltage) with an electrical power supply. The connection distance of an analog terminal to this interface is limited to 20 meters.

The user of a set connected to this interface has the same operation capabilities as a user using a classic Z interface (restriction: the set's Message LED cannot be used).



X101: 8-pin modular jack for connection to the analog terminal

- 1: GND - 5: L2 line wire
- 2: not used - 6: not used
- 3: not used - 7: not used
- 4: L1 line wire - 8: not used

X102: connector for the power supply

- 1: - 48 V - 2: + 48V

Various terminal cables

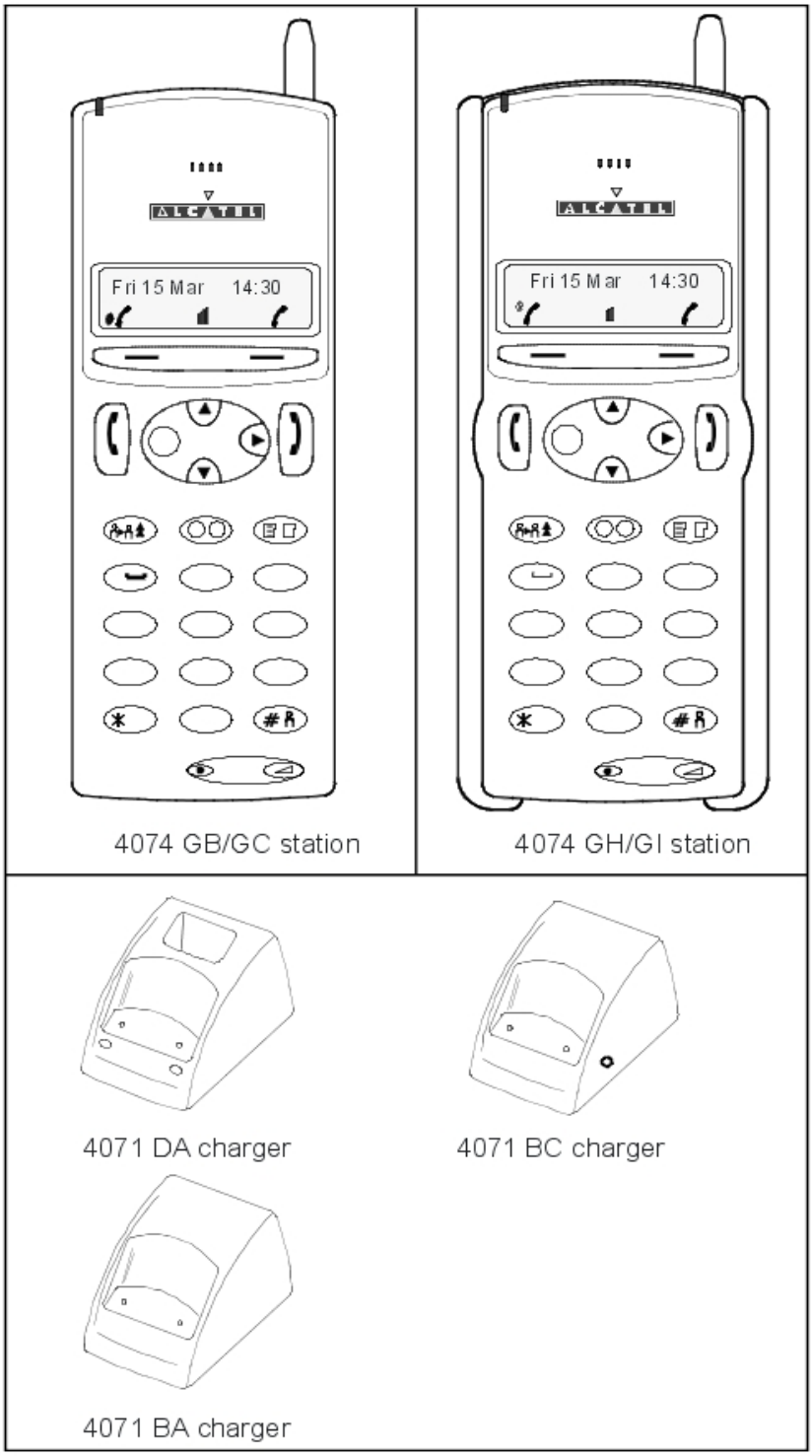
The cables below can be used to connect terminals to UA sets (references 3AK, etc represent the group of 5 cables described in the table).

CABLE	CONNECTORS	REFERENCE	LENGTH
S0	8 pin modular jack - 8 pin modular jack	1AB 04521 0024	3 m
V24 DCE	25 pin SUBD plug - 25 pin SUBD jack	1AB 05412 0016	2 m
V24 DTE	25 pin SUBD plug - 25 pin SUBD plug	1AB 05412 0018	2 m
PC	8 pin mini din plug - 9 pin SUBD jack	1AB 07871 0003	2 m
MAC	4 pin mini din plug - 4 pin mini din plug	9191500	2 m

2.3.15.1.9 DECT 4074 HANDSETS

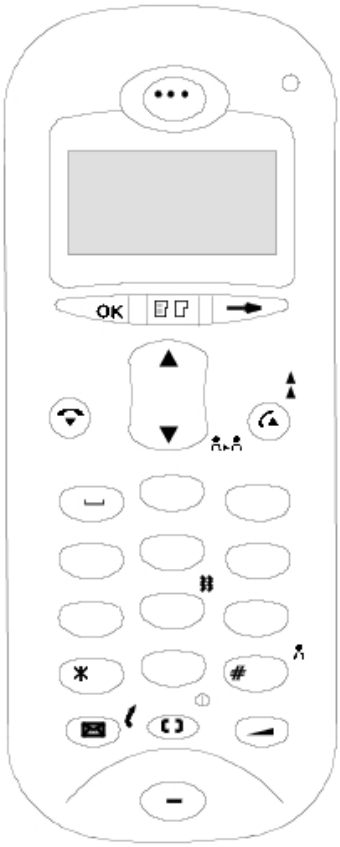
FEATURE	DECT HANDSETS			
	4074 GB	4074 GH	4074GI	4074GC
Handset with adjustable volume	YES	YES	YES	YES
ON/OFF switch (or keys)	YES	YES	YES	YES

16 character display	YES	YES	YES	YES
Numeric keypad keys	12	12	12	12
Line keys	2	2	2	2
Programmable keys	2	2	2	2
Navigator keys	YES	YES	YES	YES
Headset socket	--	YES	YES	--
Keypad backlighting	--	YES	YES	--
Protective cover	--	YES	YES	--
Integrated vibrator	--	--	YES	YES
Charger	4071BA 4071DA	4071DA	4071 DA	4071BC
Hands free	--	--	--	YES



2.3.15.1.10 4073 GS SMART DECT HANDSET

FEATURE	4073 GS SMART
Handset	YES
On/Off Key	YES
Display: 2 x 16 alphanumeric characters + 1 line of 8 icons	YES
Numeric keypad keys	12
Navigator keys	YES
Function keys	8
Vibrator	YES



Chapter 3

User Services

3.1 Meet Me Conference

3.1.1 Basic description

3.1.1.1 Basic Technical Description

The Meet Me Conference is a new feature that allows up to 6 people to form a group, join a bridge and hold a discussion.

One member of the group is in charge of organizing the conference and of "opening the bridge'. This person is "the Master of the Conference". The other members are the "Participants in the Conference".

The "Master" dials a code dedicated to the feature. This code is referred to as "Activate Meet Me".

The "Participant" dials a code dedicated to the feature. This code is referred to as "Join MeetMe".

Activation of the conference requires the authentication of the conference master (EDN + user password + access code). The user password cannot be the default user password. It has to be changed personally by the user. If the user password is the default one, the activation is refused.

The "Master" also defines the 4 digit access code the group members (the participants) will need to enter to take part in the discussion.

The "Master" then broadcasts the access code to the participants. This access code is the authentication of the conference participants. The participants have to enter the code to "join the bridge" and be accepted in the conference.

If the bridge is not yet open, the participants are queued and stay waiting for the opening of the bridge, external callers listen to Music On Hold (MOH), internal callers listen to waiting tones. See: § Participant waiting

A 5 minute-timer is enabled to release the call if the participants wait too long.

When participants are waiting for the bridge to open, the procedure of “join a conference” is activated one by one for all the waiting participants.

Both the Master and the participants can be internal or external subscribers.

The Meet Me Conference feature can run on both the Advanced and Premium systems.

3.1.1.1.1 Participant waiting

When the Meet Me Conference bridge is not open, participants have to queue for availability. They will be connected to the bridge as soon as the "Master" opens it.

Detailed description

- The default maximum waiting time is 5 minutes, the connection is then released.
- Use OMC to configure the timer: System Miscellaneous - Memory Read/Write - Timer Labels: ParWaitTime.
- 5 participants maximum can wait for the "Master" to open the Meet Me Conference bridge.

Any additional connection attempt is refused.

- The voice prompt “The conference bridge is not yet open” is played as soon as a participant has to wait.
- While waiting, external callers listen to the MOH, internal callers listen to the waiting tones and can see the “Please wait” message.
- Both types of callers have to hold on, Metering is enabled during the waiting time.
- Callers have to wait until the "Master" has been checked.
- If the" Master" opens the bridge and closes it quickly, all waiting callers are released by the system.
- If no “Media resources are free”, the “emergency” procedure takes over: the call is released without any indication, even if it is an incoming call.
- If there is no licence, the call is released. The system does not make participants wait.

3.1.1.1.2 NDDI analogue trunk support

OmniPCX Office R6 supports Non Direct Dialling In (NDDI) analog trunk. When a caller uses analogue trunk, the calling address is received by the system. The operator, the Automated Assistant, the MLAA or Pimphony applications, etc. can transfer any incoming call to the conference bridge.

The called party transfers the call to the bridge under some conditions.

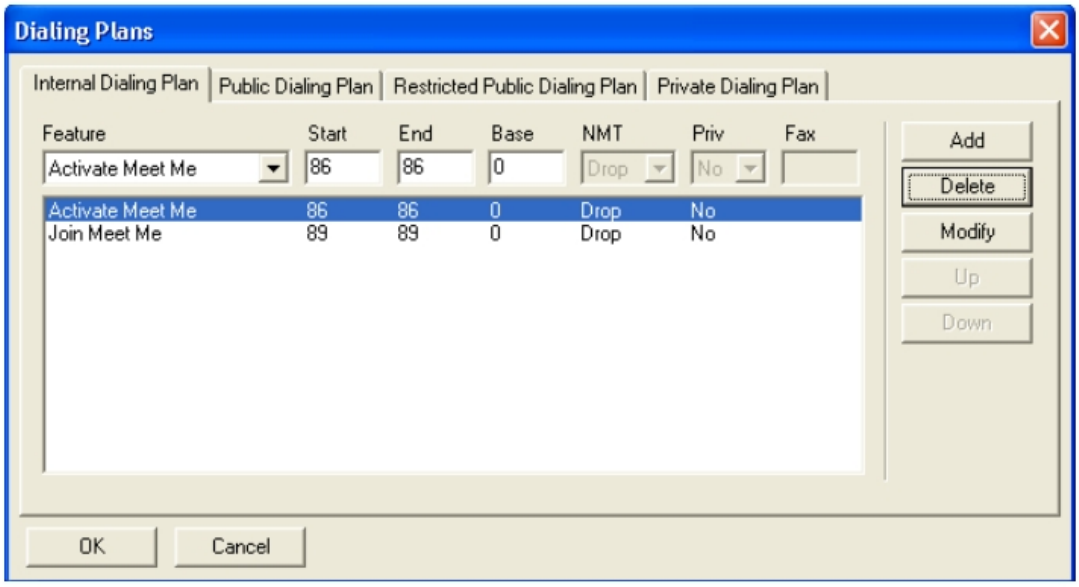
- The call to the bridge is authorised as a second call. But this call cannot be put on hold or parked. Features like broker (See: module Three Party Calls - Overview § Broker) or 3-party conference are still refused.
- Transfer is allowed only during the alerting phase. The transfer is handled like an “unsupervised transfer”. The resulting ringing call between requester, if it is external, and the bridge is supervised by the system by a 24 second-timer. This external caller will then be routed to the general level.
- If the request is internal, there is no supervision of the transferred call. It keeps the ringing state until the system connects.
- Management of the metering and counters are processed by the system, as for any normal unsupervised transfer.
- No special software key or special function is required to activate this kind of transfer.
- For AA processing, the codes to activate or to join a bridge are accepted as destinations for the “free dialling function” or for the “transfer to sub/group” service.
- In case of MLAA processing, you can reach the codes to enable a bridge or to join it by the “free dialling” service or the “direct transfer to” service.

3.1.1.1.3 Dialling plan

There are now 2 new functions in the Main, DDI (Direct Dialling In) and ATL dialling plans:

- Activate Meet Me: Used only by the Master to open a bridge.
- Join Meet Me: Used by any participant to join a bridge.

The feature codes are configured as well as:



The values in "Start" and "End" with "Base = 0" define the numbering scope of the feature.

The installer must configure the feature codes. No entries in both the MAIN and DDI dialling plans are defined by default.

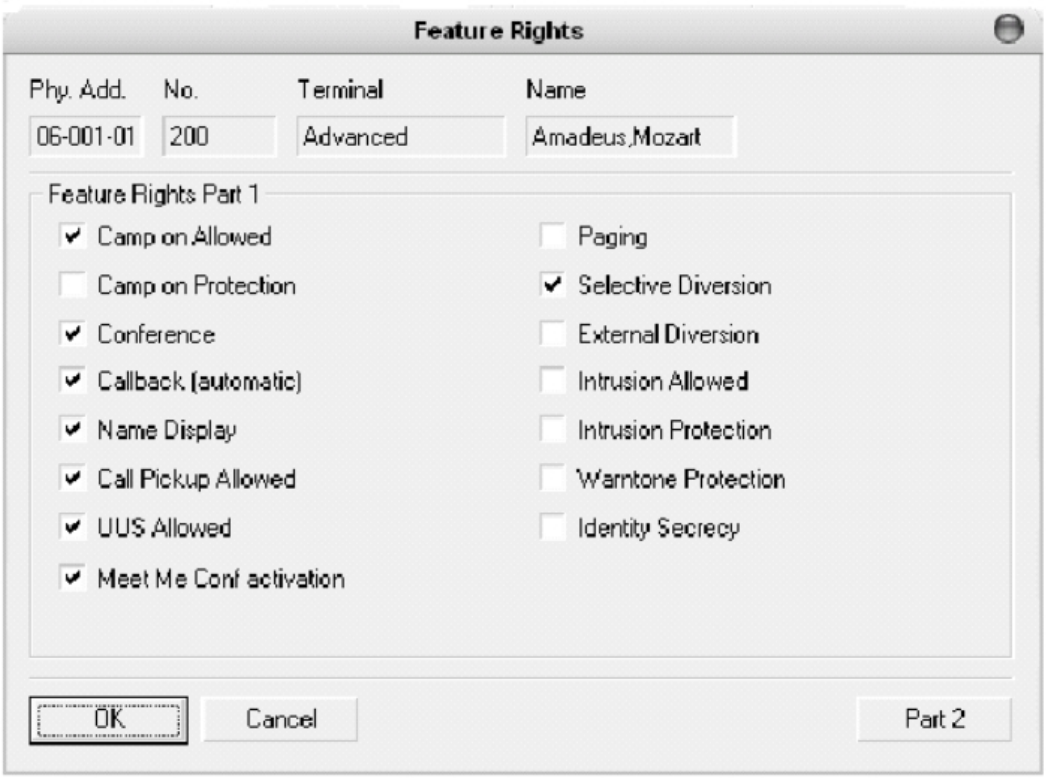
3.1.1.1.4 Feature rights

In the User/Base station list, you can configure the user feature right to authorize the Meet Me Conference activation.

The feature right authorizes a user to be the Master of the Meet Me conference.

No right differentiates the authorization of activation of the conference by means of an internal call or of an external call.

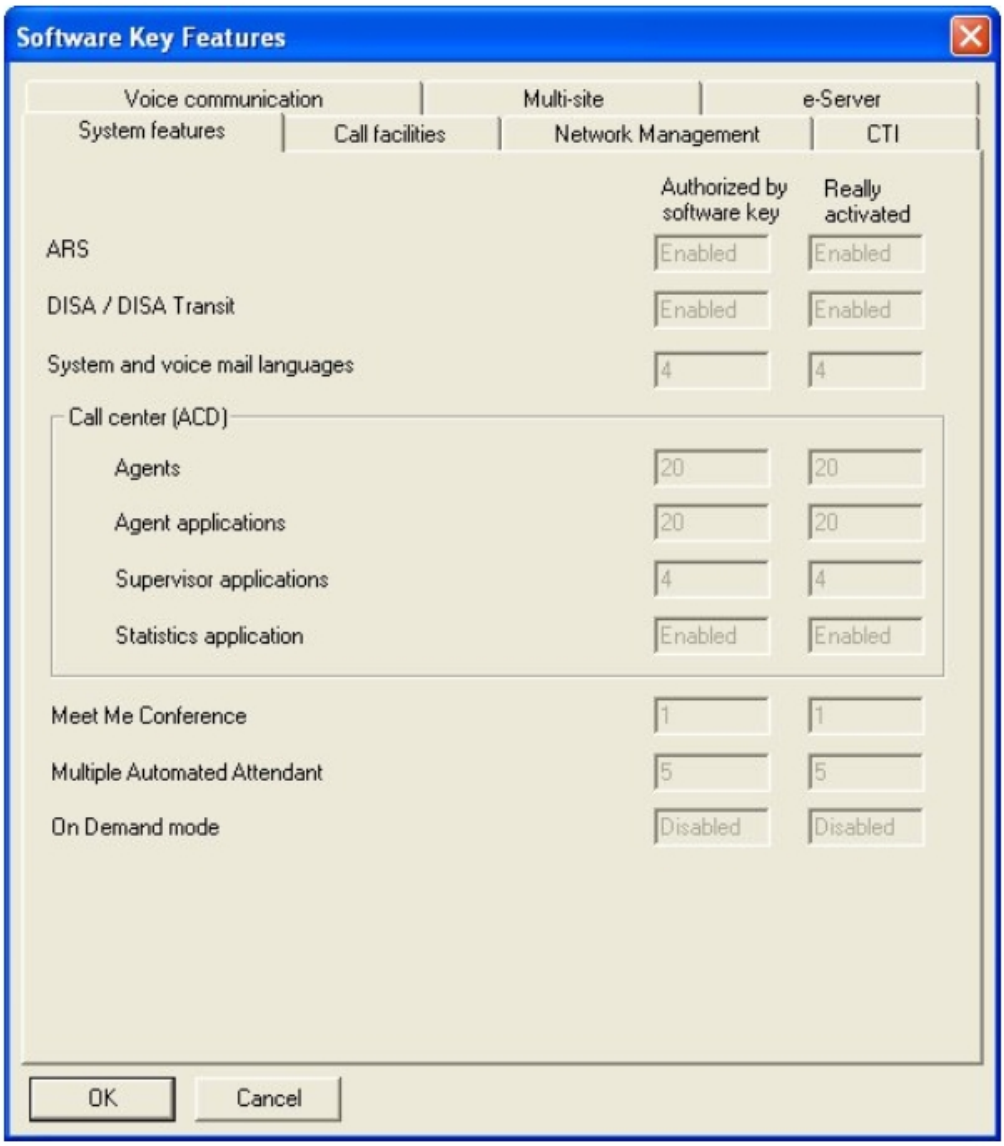
A check box has been added to the Feature Rights window in Part 1 to enable or to disable the Meet Me Conference.



3.1.1.1.5 Meet Me Conference Licence

In the Software Key Features screen, in the System features tab, the item Meet Me Conference specifies if the Meet Me Conference is authorised by the software key: Value 0 = feature disabled, value 1 = feature enabled.

The number of Meet-me conferences, which are activated simultaneously, depends on the licence. The default value is 0; the maximum value is 1.



3.1.1.1.6 Restrictions

In OmniPCX Office Version 5.1:

- Transfer to the Conference Bridge is not possible.
- Calls from NDDI analogue trunks cannot reach the conference bridge. But calls from DDI (simulated or not) on analogue trunks or trunks that use DDI analogue protocol (e.g.: DDI trunks, T1_CAS, PCM R2) **CAN** reach the conference bridge.
- The Conference Bridge cannot be activated or joined by the Voice Management Unit or the Automated Attendant.
- Metering is minimal: Tickets are generated only for external incoming calls. Tickets show

the dialled number of the Conference as the dialled destination.

- PIMphony display does not work with "Meet Me Conference".
- Booking the Bridge is not managed by any application or mechanism.

In OmniPCX Office Version 6.0:

- The NDDI analogue trunk supports Meet-me conference. An incoming call can be transferred to the conference bridge by the operator, the AA or PIMphony applications, etc.

3.2 Resource Key

3.2.1 KeysFunctions

3.2.1.1 Overview

3.2.1.1.1 DESCRIPTION

A resource key is used to take a line in order to make or receive a call.

When a station has at least two resource keys, it is said to be **multiline**. In this mode, the user presses the resource key associated with the correspondent he wants to contact (using the shuttle call function, for example). Multiline stations can also operate in **Key system** or **PCX** mode.

A station which does not have resource keys is said to be **monoline**. These resources (3) are "virtual". In this mode, the user enters a code programmed in the "Features in Conversation" table, to activate a function such as a shuttle call.

Characteristics of the different modes:

Type of subscriber	**Normal**		
Mode	Monoline	Key system	PCX
Default resource keys	3 "virtual" resource keys	2 RGMints (**) n (*) RSPs (**)	2 RGMints (**) 2 RSBs (**)
Simultaneous management	1 conversation 1 hold 1 camp-on	1 conversation (n+1) holds + camp-ons	1 conversation 3 holds + camp-ons

(*) n = number of analogue lines and B channels (within the station key limit).

(**) see explanation overleaf.

3.2.1.2 Configuration procedure

3.2.1.2.1 CONFIGURATION

- Programming the resource keys on each station:

- by OMC (Expert View): **Subscribers/BasestationsList -> Subscribers/Basestations List -> Details -> Keys**.
- by MMC-Station: **Subscriber -> Key**.

- Programming the monoline, multiline, "key system" or "PCX" mode:

- by OMC (Expert View): **Subscribers/Basestations List -> Subscribers/Basestations List -> Profiles**.
- by OMC (Easy view): **Subscriber profiles**
- by MMC-Station: **TerPro**.

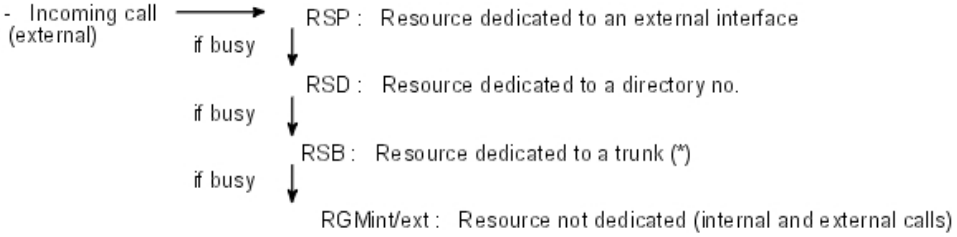
- Authorize or cancel selection of an RSB if the external call arrives on a line which does not belong to the trunk programmed for this key:

- By OMC (Expert View):
  System Miscellaneous -> Memory Read/Write -> Misc. Labels -> SelRSBsig.
- By MMC-Station: **Global -> Rd/Wr -> Address s -> "SelRSBsig" -> Return -> Memory**

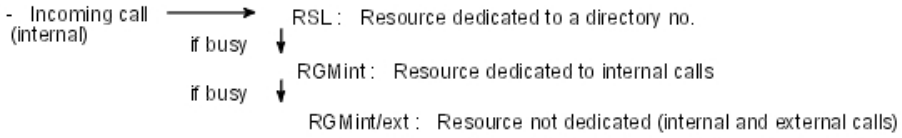
3.2.1.3 Operation

3.2.1.3.1 ACTIVATION/USE

Incoming, the system uses the resource keys in the following order of priority:



(*) Default operation (see section: "Configuration")



Outgoing, a call can be made:

- without pressing a resource key (the system selects the most appropriate key as soon as the user dials)
- by pressing a resource key (before dialing the number), whether:
  - for an **external** outgoing call:
  - an RSD (dedicated to a trunk or an "Automatic Route Selection")
  - an RSB (dedicated to a trunk or an "Automatic Route Selection")
  - an RSP (dedicated to an external interface)
  - an RGO (dedicated to outgoing calls)
  - an RGMint/ext (not dedicated)
  - for an **internal** outgoing call:
  - on an RSL (dedicated to a directory no): the system automatically dials the programmed number
  - an RGMint (dedicated to internal calls)

- an RGO (dedicated to outgoing calls)
- an RGMint/ext (not dedicated)

Note:
The MMC-Station labels RGI, RGO and RGM (MMC station) are equivalent to RGX in OMC (+ definition of "Call Sense" field).

More details about the abbreviations RGM, RGO, RSL, etc. can be found in the glossary.

3.2.1.3.2 ADDITIONAL INFORMATION

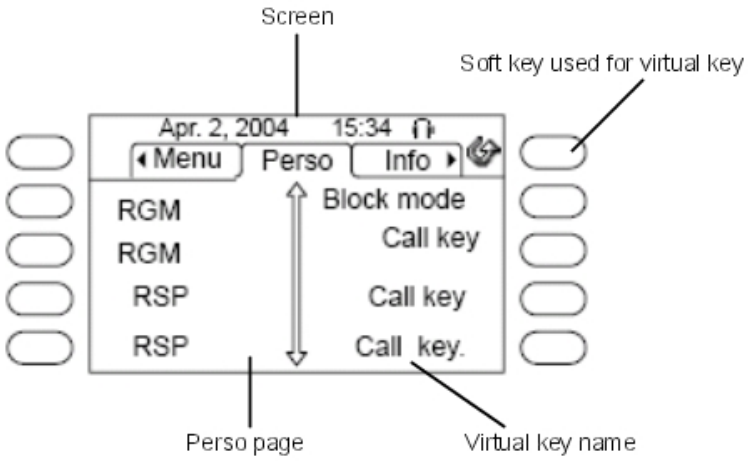
- A resource key manages only one communication at a time.
- Z and First Reflexes stations are monoline; all other stations are multiline.
- The Reflexes 2G 4003 can be either monoline or multiline.

3.2.2 Keys Operating Modes

3.2.2.1 PROFILES FOR Alcatel-Lucent IP Touch 4038 Phone, Alcatel-Lucent 4039 Digital Phone, Alcatel-Lucent IP Touch 4068 Phone STATIONS

These Alcatel-Lucent 8 series/Alcatel-Lucent 9 series stations display 40 virtual keys through 5 pages (Up and Down keys) of two columns with 4 virtual keys each.

Example of virtual keys on the Perso page:



RGM: General Mixed Resource
RSP: Physical Resource

3.2.2.1.1 Key system modes

- All countries except USA

Page	Key	Operator		Secretary		Manager		Normal	
1	**UPK 1 / 2**	Mode N/R	Ope Div	RSL Manager	Screening	RSL Secretary	Screening	Call ()	Call ()
	Virt. keys 1 / 2	RGM (INT/EXT)	Block Mode	RGM (INT/EXT)	Block Mode	RGM (INT/EXT)	Block Mode	RGM (INT/EXT)	Block Mode
	Virt. keys 3 / 4	RGM (INT/EXT)	Call ()	RGM (INT/EXT)	Call ()	RGM (INT/EXT)	Call ()	RGM (INT/EXT)	Call ()
	Virt. keys 5 / 6	Call ()	Call ()	RSP 1	Call ()	RSP 1	Call ()	RSP 1	Call ()
	Virt. keys 7 / 8	Call ()	Call ()	RSP 2	Call ()	RSP 2	Call ()	RSP 2	Call ()
n	**Virt. keys n / n+1**	Call ()	Call ()	RSP n	Call ()	RSP n	Call ()	RSP n	Call ()
5	**Virt. keys 33 / 34**	Call ()	Call ()	RSP 15	Call ()	RSP 15	Call ()	RSP 15	Call ()
	Virt. keys 35 / 36	Call ()	Call ()	RSP 16	Call ()	RSP 16	Call ()	RSP 16	Call ()
	Virt. keys 37 / 38	Call ()	Call ()	RSP 17	Call ()	RSP 17	Call ()	RSP 17	Call ()
	Virt. keys 39 / 40	Call ()	Call ()	RSP 18	Call ()	RSP 18	Call ()	RSP 18	Call ()

Note 1:

UPK = User Programmable Key; RGM = General Mixed Resource; RSL = (Internal) Line Resource; RSP = Physical Resource

- USA

Page	Key	Operator		Secretary		Manager		Normal	
1	**UPK 1 / 2**	Manual Hold	Transfer	Manual Hold	Transfer	Manual Hold	Transfer	Manual Hold	Transfer
	Virt. keys 1 / 2	RGM (INT/EXT)	DND	RGM (INT/EXT)	DND	RGM (INT/EXT)	DND	RGM (INT/EXT)	DND
	Virt. keys 3 / 4	RGM (INT/EXT)	Mode N/R	RGM (INT/EXT)	RSL Manager	RGM (INT/EXT)	RSL Secretary	RGM (INT/EXT)	Call ()
	Virt. keys 5 / 6	RGM (INT/EXT)	Ope Div	RGM (INT/EXT)	Screening	RSP 1	Screening	RSP 1	Call ()
	Virt. keys 7 / 8	RGM (INT/EXT)	Call ()	RGM (INT/EXT)	Call ()	RSP 2	Call ()	RSP 2	Call ()
n	**Virt. keys n / n+1**	Call ()	Call ()	RSP n	Call ()	RSP n	Call ()	RSP n	Call ()
5	**Virt. keys 33 / 34**	Call ()	Call ()	RSP 13	Call ()	RSP 13	Call ()	RSP 13	Call ()
	Virt. keys 35 / 36	Call ()	Call ()	RSP 14	Call ()	RSP 14	Call ()	RSP 14	Call ()
	Virt. keys 37 / 38	Call ()	Call ()	RSP 15	Call ()	RSP 15	Call ()	RSP 15	Call ()
	Virt. keys 39 / 40	Call ()	Call ()	RSP 16	Call ()	RSP 16	Call ()	RSP 16	Call ()

Note 2:

UPK = User Programmable Key; RGM = General Mixed Resource; RSL = (Internal) Line Resource; RSP = Physical Resource

3.2.2.1.2 PCX mode

In general, sets in PCX mode do not have RSP keys. All remaining free keys are assigned a Call function.

- All countries except USA

Page	Key	Operator		Secretary		Manager		Normal	
1	**UPK 1 / 2**	Mode N/R	Ope Div	RSL Manager	Screening	RSL Secretary	Screening	Call ()	Call ()
	Virt. keys 1 / 2	RGM (INT/EXT)	Block Mode	RGM (INT/EXT)	Block Mode	RGM (INT/EXT)	Block Mode	RGM (INT/EXT)	Block Mode
	Virt. keys 3 / 4	RGM (INT/EXT)	Call ()	RGM (INT/EXT)	Call ()	RGM (INT/EXT)	Call ()	RGM (INT/EXT)	Call ()
	Virt. keys 5 / 6	RGM (INT/EXT)	Call ()	RGM (INT/EXT)	Call ()	RGM (INT/EXT)	Call ()	RGM (INT/EXT)	Call ()
	Virt. keys 7 / 8	RGM (INT/EXT)	Call ()	RGM (INT/EXT)	Call ()	RGM (INT/EXT)	Call ()	RGM (INT/EXT)	Call ()
n	**Virt. keys n / n+1**	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()
5	**Virt. keys 33 / 34**	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()
	Virt. keys 35 / 36	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()
	Virt. keys 37 / 38	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()
	Virt. keys 39 / 40	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()

Note 1:

UPK = User Programmable Key; RGM = General Mixed Resource; RSL = (Internal) Line Resource

- USA

Page	Key	Operator		Secretary		Manager		Normal	
1	**UPK 1 / 2**	Manual Hold	Transfer	Manual Hold	Transfer	Manual Hold	Transfer	Manual Hold	Transfer
	Virt. keys 1 / 2	RGM (INT/EXT)	DND	RGM (INT/EXT)	DND	RGM (INT/EXT)	DND	RGM (INT/EXT)	DND
	Virt. keys 3 / 4	RGM (INT/EXT)	Mode N/R	RGM (INT/EXT)	RSL Manager	RGM (INT/EXT)	RSL Secretary	RGM (INT/EXT)	Call ()
	Virt. keys 5 / 6	RGM (INT/EXT)	Ope Div	RGM(INT/EXT)	Screening	RSP 1	Screening	RSP 1	Call ()
	Virt. keys 7 / 8	RGM(INT/EXT)	Call ()	RGM (INT/EXT)	Call ()	RGM (INT/EXT)	Call ()	RGM (INT/EXT)	Call ()
n	**Virt. keys n / n+1**	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()
5	**Virt. keys 33 / 34**	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()
	Virt. keys 35 / 36	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()
	Virt. keys 37 / 38	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()
	Virt. keys 39 / 40	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()	Call ()

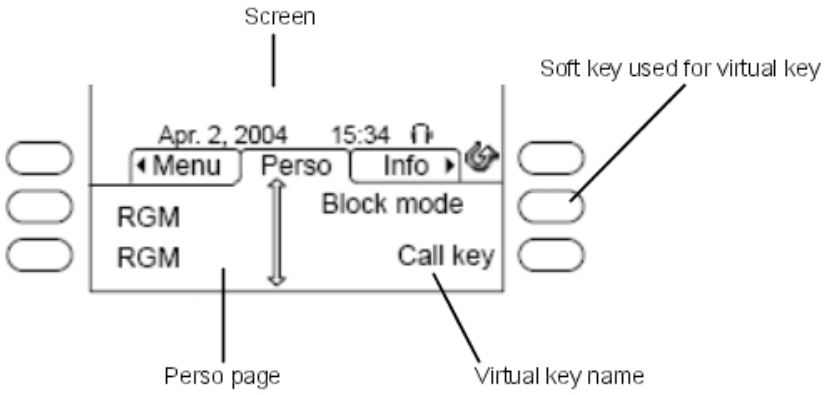
Note 2:

UPK = User Programmable Key; RGM = General Mixed Resource; RSL = (Internal) Line Resource

3.2.2.2 PROFILES FOR Alcatel-Lucent IP Touch 4028 Phone/Alcatel-Lucent 4029 Digital Phone STATIONS

These Alcatel-Lucent 8 series/Alcatel-Lucent 9 series stations display 40 virtual keys through 10 pages (Up and Down keys) of two columns with 2 virtual keys each.

Example of virtual keys on the Perso page:



RGM: General Mixed Resource

3.2.2.2.1 Key system mode

Same as Alcatel-Lucent IP Touch 4038 Phone, Alcatel-Lucent 4039 Digital Phone, and Alcatel-Lucent IP Touch 4068 Phone stations (see corresponding section), except that there are 10 virtual pages made of 2 columns with 2 virtual keys each, instead of 5 virtual pages made of 2 columns with 4 virtual keys each.

3.2.2.2.2 PCX mode

Same as Alcatel-Lucent IP Touch 4038 Phone, Alcatel-Lucent 4039 Digital Phone, and Alcatel-Lucent IP Touch 4068 Phone stations (see corresponding section), except that there are 10 virtual pages made of 2 columns with 2 virtual keys each, instead of 5 virtual pages made of 2 columns with 4 virtual keys each.

3.2.2.3 PROFILES FOR Alcatel-Lucent IP Touch 4018 Phone/Alcatel-Lucent 4019 Digital Phone STATIONS

These stations come with 6 programmable keys.

3.2.2.3.1 Key system mode

Key system mode is never used with these stations.

3.2.2.3.2 PCX mode

- All countries except USA

Prog. key
RGM (INT/EXT)
RGM (INT/EXT)
CF-U (M)
Conference
Transfer

Call ()

- USA

Prog. key
RGM (INT/EXT)
RGM (INT/EXT)
CF-U (M)
Conference
Manual Hold
Transfer

3.2.2.4 PROFILES FOR MOBILE SETS

The Alcatel-Lucent IP Touch 310/610 WLAN Handsets are multiline sets that have the same behavior and services asdigital sets.

3.2.2.4.1 Key system mode

Key system mode is never used on MIPTs.

3.2.2.4.2 PCX mode

An MIPT set is never initialised as Operator.

- Calls are selected through the "Line" key.
- A fixed key is dedicated to the Dial by Name feature.
- The "FCN" key is used locally.
- There are four contextual soft keys: SK1 left (Ok), SK1 right (not used, mapped to SK1 left), SK2 left (Clear), SK2 right (Back).
- Power On/Power Off are executed by a long press on Off hook/On hook keys.

3.3 Trunk Groups

3.3.1 Overview

3.3.1.1 DESCRIPTION

Trunk groups are used to make calls to the network. A trunk group is made up of at least one analog line or B channel.

Each bundle has:

- a directory number defined in the main numbering plan
- a management type: cyclic or sequential
- barring and traffic sharing link categories (see "Link Categories")

3.3.1.2 ADDITIONAL INFORMATION

- The maximum number of trunk groups in a system is 120.
  - 1 main trunk group
  - the others being secondary trunk groups
- The maximum number of lines or channels in a trunk group is 120.
- The total number of lines/channels across all the trunk groups must not exceed 500.
- The trunk group with index 120 may be reserved for Operator Groups (see "Operator stations").
- For an outgoing call, an analog line with predetermined routing (LRP) can be used either exclusively or in priority by the destination user of this LRP.

3.3.2 Configuration procedure

3.3.2.1 CONFIGURATION

- Configuring the trunk groups:

- by OMC (Expert View): **External Lines -> Trunk Groups -> Details**
- by MMC-Station: **TrGp**

- Defining the trunk group management type:

- by OMC (Expert View): **External Lines -> Trunk groups**
- by MMC-Station: **TrGp**

- Modifying the default traffic sharing link categories (value 1 to 16):

- by OMC (Expert View):
  - for the users: **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Barring**
  - for the trunk groups: **External Lines -> Trunk Groups -> Details -> Link-Cat**
- by MMC-Station:
  - for the users: **Subscr -> BarTyp (last 2 values)**
  - for the trunk groups: **TrGp ->** Catego

- Modify the "Traffic Sharing Matrix", if necessary, using OMC (Expert View):

System Miscellaneous -> Traffic Sharing and Barring -> Traffic Sharing Matrix

- To specify whether or not to authorize all the users to seize an analog line with predetermined routing for outgoing calls:

- by OMC (Expert View): **System Miscellaneous -> Memory Read/Write -> Misc. Labels -> "TonPrRng"**
- by MMC-Station: **Global -> Rd/Wr -> Address -> "PRIOR_LRP" -> Return -> Memory**

3.3.3 Operation

3.3.3.1 ACTIVATION/USE

To make a call to the network, a user can:

- dial a trunk group number
- press an RSD or RSB resource key (see "Resource keys")

If connection between the user and the trunk group is authorized (analysis of barring and traffic sharing link categories: see "Link Categories" and "Barring"), the system selects a line (or channel) in the trunk group as follows:

Management type	cyclic	sequential
Trunk line used in the trunk group	1st free line following the last selected	1st free line (*), in the programmed order

(*) Priority is given to "outgoing" lines, then "mixed lines".

3.4 HuntingGroup

3.4.1 Overview

3.4.1.1 DESCRIPTION

Creating Hunt Groups makes it possible to call several stations using a single directory number; a single member of the group answers the call for the whole group.

Each group has:

- a directory number defined in the main dialling plan
- a parallel, circular or serial management type

3.4.1.2 ADDITIONAL INFORMATION

- The maximum number of groups in a system is 50 (Hunt Groups + Broadcast Groups + Pickup groups).
- The maximum number of stations in a group is 32.
- The maximum number of calls camped onto a Hunt Group is equal to the number of members in the group.
- A Hunt group cannot be in auto-answer mode (also called Intercom mode).

3.4.2 Configuration procedure

3.4.2.1 CONFIGURATION

- Configuring the groups:

• by OMC (Expert View): **Hunt Groups** • by MMC-Station: **Groups -> User or Subscr**

- Defining the group management type:

- by OMC (Expert View): **Hunt Groups**
- by MMC-Station: **Groups -> User or Subscr**

- To authorize immediate group forwarding or unavailability/withdrawal (see "Forwarding") of group calls from the last member of a group (only with OMC (Expert View)):

System Miscellaneous -> Feature Design ->"Disconnect Last Group Member Allowed"

- Defining the dynamic routing parameters of a group:

- by OMC (Expert View): **Hunt Groups -> Dyn. Rout.**
- by MMC-Station: **Groups -> Hunt -> DynRou**

- To authorize external calls to camp on the group, (OMC only):

- call arriving on an analog interface (TL, ATL, DID, etc): **External Lines -> Protocols -> Parameters -> "Ringing Mandatory": deselect the box to authorize holding**
- call arriving on a digital interface (T0, T2, etc): **System Miscellaneous -> Feature Design -> "Call waiting/Automatic Camp-on": select the box to authorize camp-on**

- To define the response in the event of failure – OMC (Expert View) only:

- call arriving on an analog interface (TL, ATL, DID, etc): **External Lines -> Protocols -> Parameters -> from "Reaction on missing incoming digit" to "Reaction on out of service"**
- call arriving on a digital interface (T0, T2, etc): **External Lines -> Incoming Call Handling**

- To define whether the Hunt Group is still considered free, depending on its status:

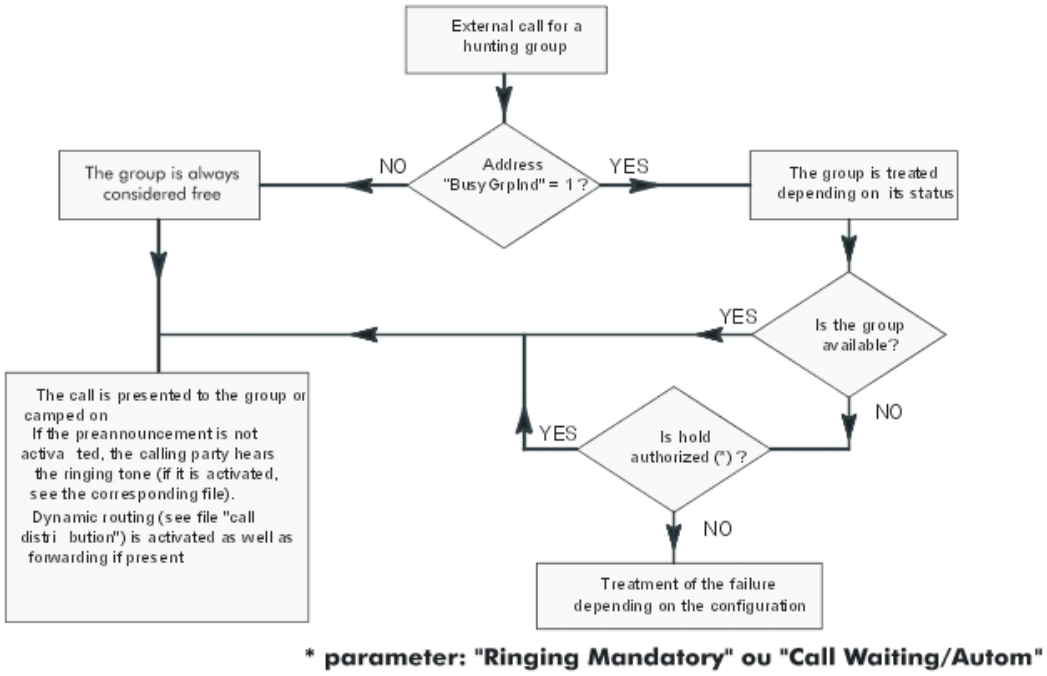
- by OMC (Expert View): **System Miscellaneous -> Memory Read/Write -> Misc. Labels -> "Busy Group indication"**
- by MMC-Station: **Global -> Rd/Wr -> Address -> "Busy Group indication" -> Return -> Memory**

3.4.3 Operation

3.4.3.1 ACTIVATION/USE

The system makes the stations ring as follows:

Management type	Parallel	Circular	Serial
Stations rung	all the free stations in the group	the first free station following the last selected	the first free station in the programming order
The call is camped on	on all busy stations	on all the stations in the group, if all are busy	
A busy station goes into idle status	the call with the highest priority is presented		
To answer a call	go off-hook or press Handsfree or the "Group Supervision" programmed key		



3.5 Operator Group

3.5.1 Overview

3.5.1.1 DESCRIPTION

An operator station basically makes it possible to distribute calls arriving on the network. This station has the following properties:

- camp-on always authorised
- barge-in (intrusion) always authorised
- access to certain programming features

Any station connected to the system (excepted multi-sets) can be an Attendant Station, but, to have all the features of an Attendant, the station must:

- be part of an Attendant group
- have one of the "Attendant" profiles (see "Resource keys" and "Station profiles"):

Attendant profile in mode ...	Key system	PCX
Resource keys	2 RGMints n RSPs (*)	2 RGMints 2 RSBs dedicated to the internal trunk group 1 RAV (**)

Function keys	Group supervision Normal/Restricted mode	Group supervision Normal/Restricted mode
LED (***)	Traffic overload	Traffic overload

(*) n = number of external interfaces; to monitor all the system's external interfaces, connect add-on modules to each attendant station.

(**) Virtual Access Resource: used only for camped-on calls.

(***) The "overload" LED only applies to stations with a three-colour LED (Alcatel-Lucent 8/9 series set and Reflexes range with the exception of 4003); it indicates:

- ORANGE, On: level 1 traffic overload, 1 or more call(s) camped on
- ORANGE, blinking: presence of a system message indicating a serious equipment fault or several less serious system messages

Attendant groups are managed in parallel.

All Attendant groups have the same call numbers (a single Attendant group is active during any particular time range (see "Time Ranges")).

An Attendant group can have:

- stations
- the general bell (or ringer) (see "Connection of a general bell")
- 1 redirection message (see "Automatic Welcome /Pre-announcement")
- VMU accesses

Default Attendant group

This group (index 8):

- is available no matter what the time range
- can have up to 8 members including the general bell
- comes into service ... (see "Activation/Use")

General level

The general level is made up of:

- the Attendant group active in the applicable time range (may include the general bell)
- stations with the "General Monitoring" feature activated (see "Call Monitoring")

It is activated automatically:

- via the dynamic routing mechanism (see "Call distribution")
- via the attendant recall mechanism (when a user's station on an external call is switched off or the activation of a service has failed)
- in accordance with the predefined settings, in the case of a misdial, or when an ISDN access is completely busy.

By default, the following are programmed:

- Attendant groups are managed in parallel.
- Attendant groups of index 1 and 2, including the first station of the first board recognised by the system

- the default group (index 8) including:
  - the first station of the first board recognised by the system
  - the general call bell

3.5.1.2 ADDITIONAL INFORMATION

- The maximum number of Attendant groups in a system: 8, default Attendant included.
- The maximum number of stations in an Attendant group: 8.
- Forwarding of the last member of the Attendant group (except for the default Attendant group) can be authorised by programming.
- The destination of an immediate forwarding of Attendant group calls (see "Forwarding") does not have the characteristics of an Attendant.
- An Attendant group cannot be in auto-answer mode (also called Intercom mode).

3.5.2 Configuration procedure

3.5.2.1 CONFIGURATION

- Configuring the Attendant groups:

• by OMC (Expert View): **Attendant Group List** • by MMC-Station: **Groups -> AttGrp**

- Modifying the internal call number of the Attendant groups:

• by OMC (Expert View): **Dialling -> Internal Dialling Plan** • by MMC-Station: **NumPln -> IntNum**

- Programming the external call number of the Attendant groups (N.B.: base identical to that of an internal call number):

• by OMC (Expert View): **Dialling -> Public Dialling Plan** • by MMC-Station: **NumPln -> PubNum**

- Programming the Attendant profile:

• by OMC (Expert view): **Users/Base stations List -> Users/Base stations List -> Profiles** • by MMC-Station: **TerPro -> Attend**

- Assigning an Attendant group to each time range:

• by OMC (Expert view): **Time Ranges** • by MMC-Station: **TimeRa**

- To authorize the immediate group forwarding or unavailability/withdrawal (see "Forwarding") of group calls from the last member of a group (with OMC only):

System Miscellaneous -> Feature Design -> "Disconnect last Group Member allowed"

- Defining the dynamic routing parameters (see "Call distribution") for an Attendant group:

- by OMC (Expert view): **Attendant Group List -> Dyn. Rout.**
- by MMC-Station: **Groups -> AttGrp -> DynRou**

- To authorize external calls arriving on an analog interface (ATA, APA, or NDDI) to camp on the group (or prevent them from doing so) – OMC (Expert View) only:

External Lines -> Protocols -> Parameters -> "Ringing Mandatory":

- To authorize external calls arriving on a digital interface (T0, T2, etc), to camp on the group (or prevent them from doing so) – OMC (Expert View) only:

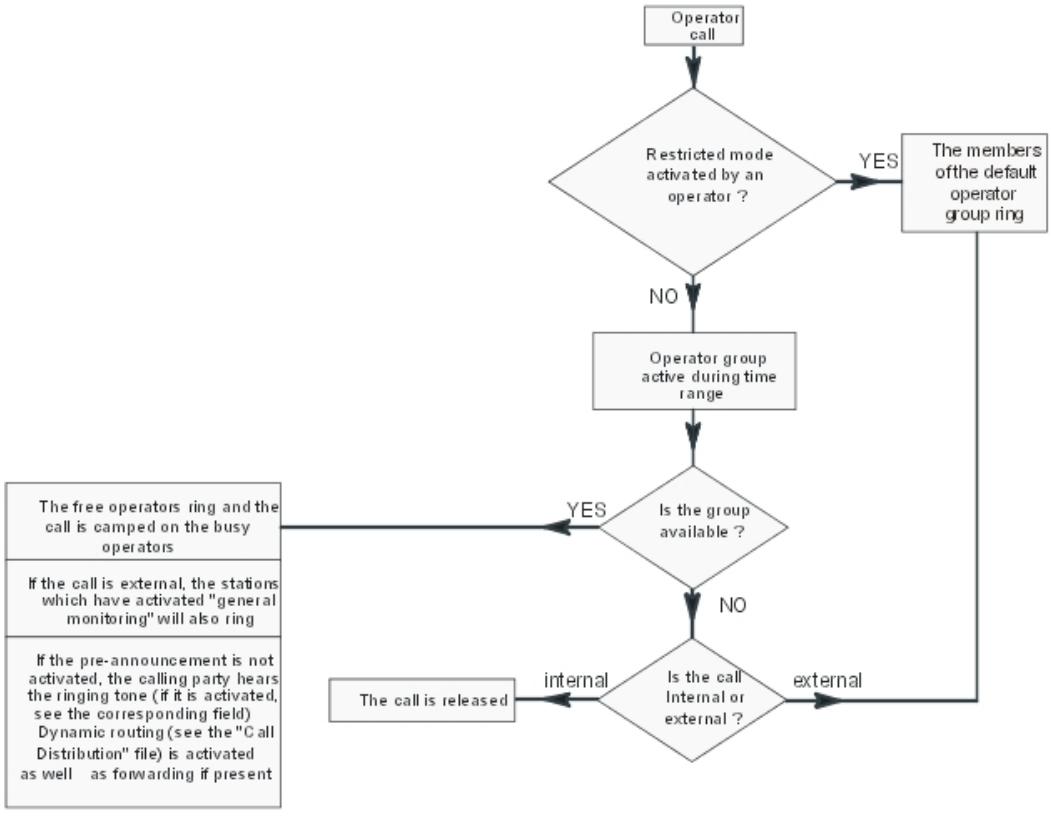
System Miscellaneous -> Feature Design -> "Call Waiting/Automatic camp-on"

- To define the response in the event of failure – OMC (Expert view) only:

- call arriving on an analog interface (TL, ATL, DID, etc): **External Lines -> Protocols -> Parameters -> from "Reaction on missing incoming digit" to "Reaction on out of service"**
- call arriving on a digital interface (T0, T2, etc): **External Lines -> Incoming Call Handling**

3.5.3 Operation

3.5.3.1 ACTIVATION/USE



3.6 Link Categories

3.6.1 Overview

3.6.1.1 DESCRIPTION

Link categories enable the system to authorize or inhibit connection between an internal user and a network subscriber.

There are 3 types of link category:

- speed dial rights: access to the collective speed dial numbers
- barring link category: access to dialing prefixes
- traffic sharing link category: access to bundles (see also file "Bundles")

Link categories are attributed as follows:

Type of Link Category	**Class**	**Class**	**Barring LC**	**Traffic sharing LC**
Attributed to ...	each station	each speed dial number	- each station - each trunk group	- each station - each trunk group
...depending on the mode, normal or restricted...	1 value per mode	1 value per mode	1 value per mode	1 value per mode
...and the type of comm. (voice or data)	1 value per type of communication	1 value per type of communication	1 value per type of communication	-
Value	authorized or unauthorized, for each class in the collective speed dial list	0 to 8 (*)	1 to 16	1 to 16

(*) Collective speed dial numbers with class = 0 are emergency numbers to which all of the stations have access.

3.6.2 Configuration procedure

3.6.2.1 CONFIGURATION

- Modifying the default speed dial rights:

- by OMC (Expert View):
  - for the users: **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Collective Speed Dial**
  - for access: **External Lines -> List of Accesses -> Details -> Speed Dial**
- by MMC-Station:
  - for access: **Access** -> **RepEnt**

- Modifying the default barring link categories:

- by OMC (Expert View):
  - for the users: **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Barring**
  - for the trunk groups: **External Lines -> Trunk Groups -> Details -> Link-Cat**
  - for access: **External Lines -> List of Accesses -> Details -> Link-Cat.**
- by MMC-Station:
  - for the users: **Subscr -> BarTyp**
  - for the trunk groups: **TrGp ->** Catego
  - for access: **Access -> Catego**

- Modifying default traffic sharing link categories:

- by OMC (Expert View):
  - for the users: **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Barring**
  - for the trunk groups: **External Lines -> Trunk Groups -> Details -> Link-Cat**
  - for access: **External Lines -> List of Accesses -> Details -> Link-Cat.**
- by MMC-Station:
  - for the users: **Subscr -> BarTyp (last 2 values)**
  - for the trunk groups: **TrGp -> Catego (last 2 values)**
  - for access: **Access -> Catego** (last 2 values)

- To modify the "Barring Matrix" – OMC (Expert View) only:

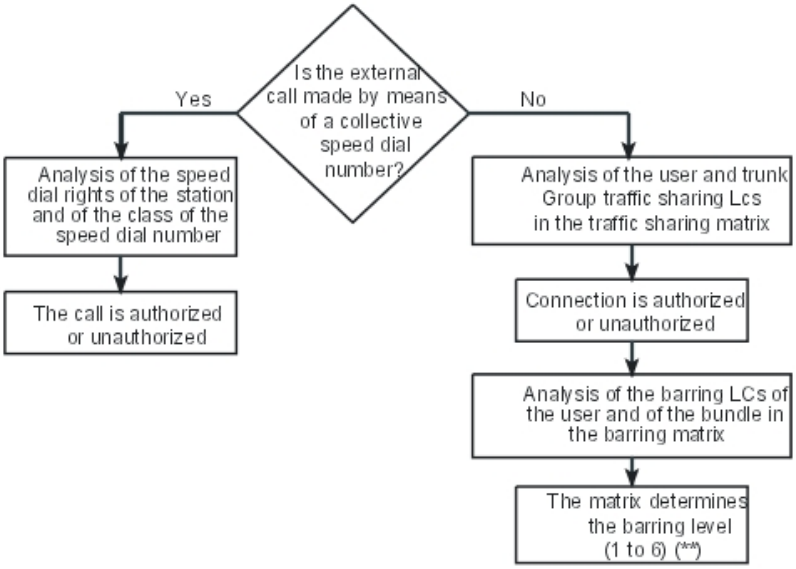
Barring -> Barring Matrix

- To modify the "Traffic Sharing Matrix" – OMC (Expert View) only:

Barring -> Traffic Sharing Matrix

3.6.3 Operation

3.6.3.1 ACTIVATION/USE



(**) See "Restrictions"

3.6.3.2 ADDITIONAL INFORMATION

- Special case – transit: a call arriving on DLTx/Tx/TL is automatically routed by the system to a DLTx/Tx/TL trunk group. In this case, the line used for the incoming call acts as a gateway with respect to restrictions; its own link category is used rather than that of the trunk group to which it belongs.
- The emergency numbers predefined in the software on leaving the factory are valid regardless of the restriction operations.

3.7 Barring

3.7.1 Overview

3.7.1.1 DESCRIPTION

Barring comes into effect after the system has authorized connection between the user and the entered trunk group (following analysis of the traffic sharing link categories: see "Link Categories").

Barring makes it possible to define whether an internal user (or an access, in the case of transit) is authorized to make a call to the network, or not (other than by using the collective speed dial numbers), depending on the prefix (i.e. the first few digits) of the called number.

To do this, the system uses barring link categories (see "Link Categories") and barring tables.

The system has 6 barring tables, numbered 1 to 6: each table corresponds to a level of barring and can have "authorized" or "unauthorized" prefixes.

The system also uses two barring counters, C1 and C2:

- C1 states the maximum number of authorized digits if an authorized prefix has been

recognized or if there is no authorized prefix in the level of barring associated with the call. The default value is 22.

- C2 states the maximum number of digits authorized if the dialed prefix is not programmed in the level of barring associated with the call., while this level has at least one authorized prefix. The default value is 4.

3.7.2 Configuration procedure

3.7.2.1 CONFIGURATION

- Modifying the default barring link categories:

- by OMC (Expert View):
  - for the users: **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Barring**
  - for the trunk groups: **External Lines -> Trunk Groups -> Details -> Link-Cat**
  - for access: **External Lines -> List of Accesses -> Details -> Link-Cat.**
- by MMC-Station:
  - for the users: **Subscr -> BarTyp**
  - for the trunk groups: **TrGp ->** Catego
  - for access: **Access -> Catego**

- To modify the "Barring Matrix" – OMC (Expert View) only:

Barring -> Barring Matrix

- Creating barring tables (adding a "!" authorizes or inhibits a complete barring level) – OMC (Expert View) only:

Barring -> Barring Tables

- To authorize or deny access to the network by transfer, for each station – OMC (Expert View) only:

Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Features -> "Transfer to External"

- To authorize or deny access to the network, for each station – OMC (Expert View) only:

Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Features -> "Private Subscriber"

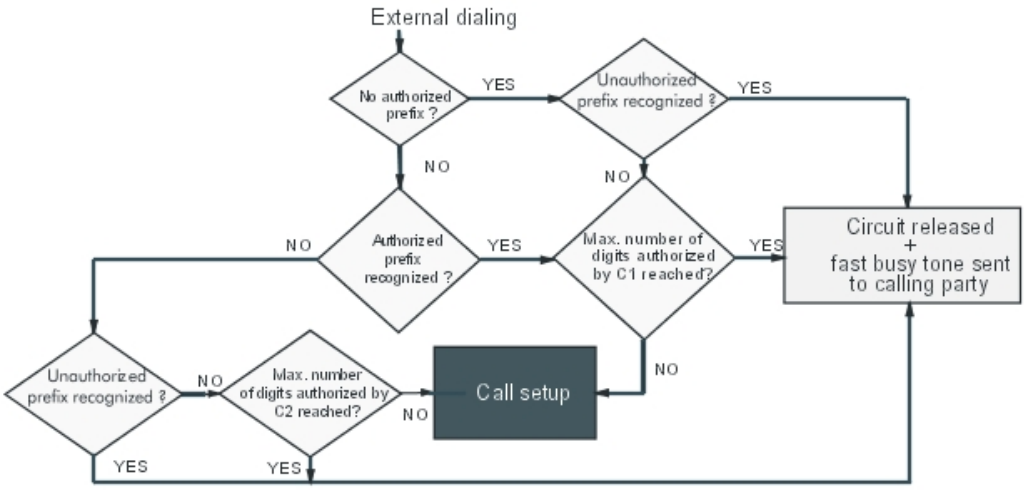
- To modify the length of barring counters – OMC (Expert View) only:

Barring -> Barring Tables

3.7.3 Operation

3.7.3.1 ACTIVATION/USE

Having determined the barring level of a call, the system compares the requested number as it is being dialed, with the prefixes in the table associated with this level of discrimination:



3.7.3.2 ADDITIONAL INFORMATION

- The 6 prefix tables altogether (or barring levels) can have over 100 prefixes.
- Each prefix has a maximum of 10 digits (0 to 9, * and #).
- A private subscriber cannot be connected to the network (nor receive calls from or make calls to the network).
- The emergency numbers predefined in the software on leaving the factory are valid regardless of the barring mechanisms.

3.8 End of Dialling Detection

3.8.1 Overview

3.8.1.1 DESCRIPTION

On analog trunk lines, end of dialing detection makes it possible to define the moment when the system can release the DTMF receivers and carry out the bi-directional switching of the line.

The system uses the end of dialing prefix table to ascertain the length (number of digits) of the numbers transmitted. A counter, equal to or superior than 0, is associated with each prefix.

When a prefix has not been configured in this table, the system uses a reference counter.

On digital trunk lines, the trunk sends a message telling the system to carry out the two-way switching. By default, the system carries out this commutation after a time-out simulating going off-hook.

3.8.1.2 ADDITIONAL INFORMATION

- Maximum number of prefixes in the table of end of dialing prefixes: 20.
- Maximum number of digits per prefix: 6.

- This mechanism does not concern lines or trunks declared in the system as being connected behind a PCX.

3.8.2 Configuration procedure

3.8.2.1 CONFIGURATION

- Programming the end of dialing prefix table:

• by OMC (Expert View): **Numbering -> End of Dialing Table** • by MMC-Station: **EODPfx -> EODial -> Prefix**

- Modifying the reference counter value on all analog lines:

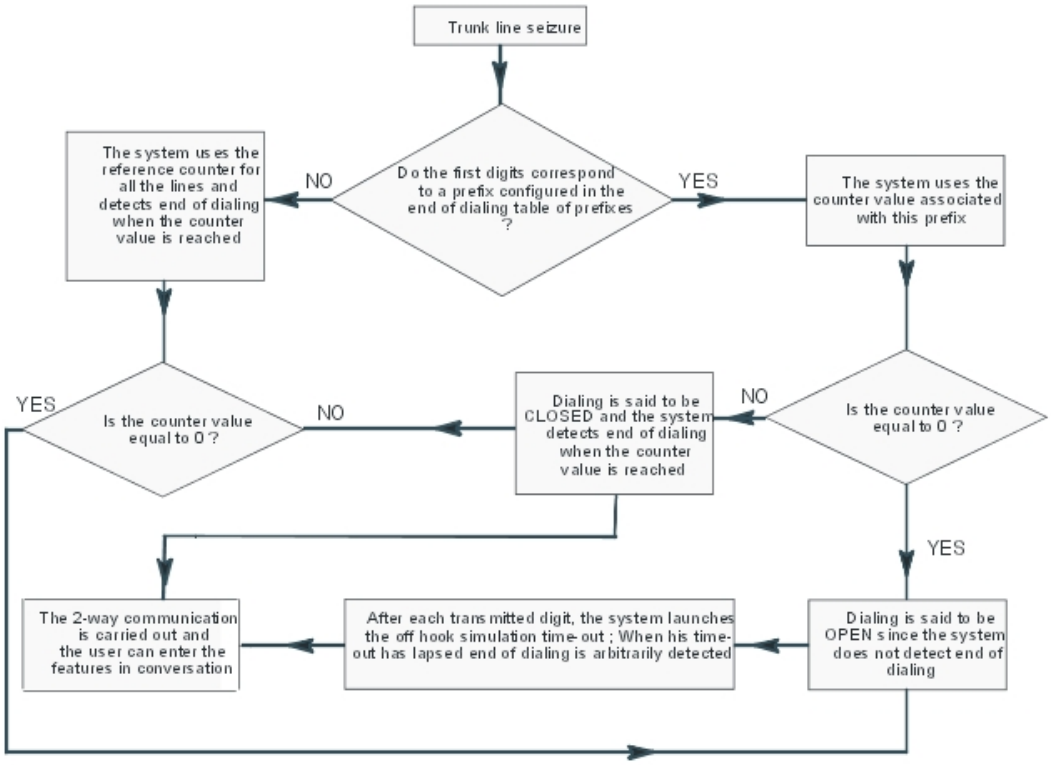
• by OMC (Expert View): **Numbering -> End of Dialing Table** • by MMC-Station: **EODPfx -> EODial -> RefCnt**

- Modifying the off hook simulation time-outs:

• call on an analog interface (TL, ATL, DDI, etc): **External Lines -> Protocols -> Analog Trunks -> Timers -> Modify**
• call on a digital interface (T0, T2, etc):
  • by OMC (Expert View): **System Miscellaneous -> Memory Read/Write -> Timer Labels -> "OffHookSim"**
  • by MMC-Station: **Global -> Rd/Wr -> Timer -> "OffHookSim" -> Return -> Memory**

3.8.3 Operation

3.8.3.1 ACTIVATION/USE



3.9 Splitting

3.9.1 Overview

3.9.1.1 DESCRIPTION

The splitting mechanism enables a user to dial a number on an analog trunk line or behind a PCX, without having to wait for any dialing splits.

It is accessed:

- by manual dialing
- by automatic dialing (last number redial, temporary memory number, speed dial number)

Splitting can be of two types:

- tone detection: TONE in the splitting prefix table
- pause: PAUSE in the splitting prefix table.

The mechanism applies at three levels:

- During line seizure:
  - if the splitting is TONE, dialing is possible as soon as the PCX has recognized the tone transmitted by the trunk during a validation time-out. If, after expiry of a time-out, no tone has been recognized, the system releases the line.

  - if the splitting is PAUSE, dialing is transmitted after expiry of a programmable time-out, (different for private or public trunk lines).

- Intermediary splitting prefixes:
  Dialing according to the prefixes in the splitting prefix table, is transmitted after tone detection or after a splitting time-out with the same principles as for the line seizure.
- Splitting prefixes defined in the personal or collective speed dial numbers:
  A personal or collective speed dial number can have one splitting character (symbolized by "!"). The splitting method used (TONE or PAUSE) is the one programmed in the splitting prefix table.

3.9.1.2 ADDITIONAL INFORMATION

- Maximum number of prefixes in the table of splitting prefixes: 16.
- Maximum number of digits per prefix: 4.

3.9.2 Configuration procedure

3.9.2.1 CONFIGURATION

- Programming the line seizure type of splitting:

• by OMC (Expert View): **Numbering -> Splitting Table** • by MMC-Station: **EODPfx -> EODial -> Split -> TonDet**

- Programming or modifying the splitting prefix table:

• by OMC (Expert View): **Numbering -> Splitting Table** • by MMC-Station: **EODPfx -> EODial -> Split -> prefix**

- To modify the pause time-out – OMC (Expert View) only:

External Lines -> Protocols -> Analog Trunks -> Timers -> Modify -> "Pause after Seizure Trunk", "Pause after Seizure Main/Sat", "Pause Fractioning" (Part 2)

- To modify the tone detection time-out – OMC (Expert View) only:

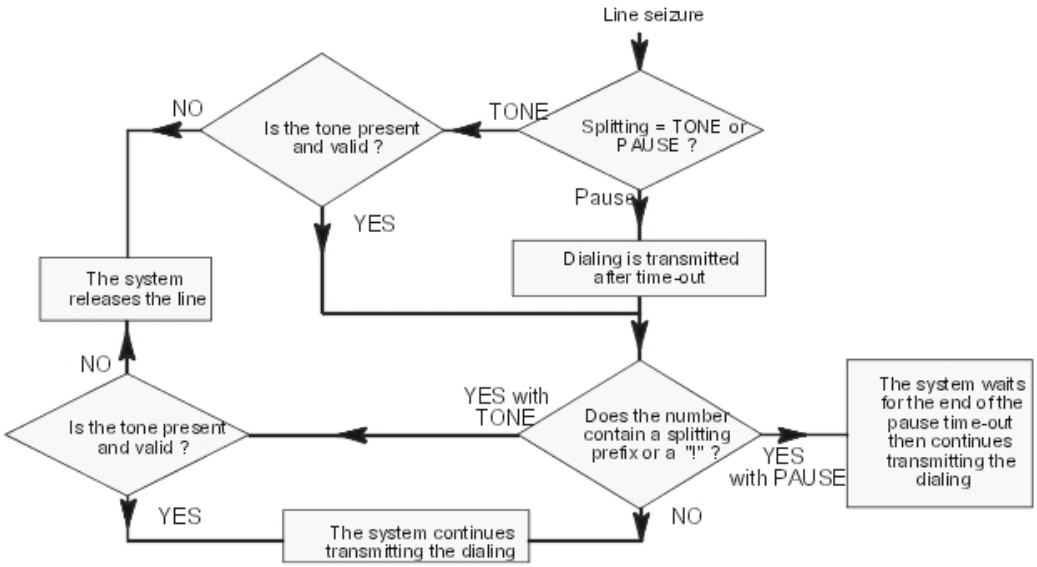
External Lines -> Protocols -> Analog Trunks -> Timers -> Modify -> "Tone Detection"

- To modify the tone non-detection time-out – OMC (Expert View) only:

External Lines -> Protocols -> Analog Trunks -> Timers -> Modify -> "TO if no Tone Detection"

3.9.3 Operation

3.9.3.1 ACTIVATION/USE



3.10 Call Distribution

3.10.1 Overview

3.10.1.1 DESCRIPTION

The system can automatically re-route:

- a call from the network and destined for the active Operator Group, or the default Operator Group (see "Operator stations")
- a call arriving from the network and currently in transit
- a DDI call (Direct Dialing Inward) from the network and destined for a station or a Hunting Group
- an external call on a "personalized" or "reserved" line: all calls arriving on a personalized external line are routed directly to a station or Hunting Group, depending on the system's normal or restricted mode. Furthermore, a "personalized" line may be "reserved", i.e. a call on this line can neither be picked up nor monitored
- an internal call
- a call from the private network

The system treats simultaneous calls destined for an Operator Group according to the following priorities:

- external hold recall, delayed or otherwise
- internal hold recall, delayed or otherwise
- external callback
- external call

- internal callback
- call from an operator station
- internal call
- Operator Group call
- Hunting Group call

The system routes an **internal** incoming call depending on the following criteria:

- directory number of the destination station programmed in the main numbering plan
- type of call: private or not
- station accessible or not
- destination station resource keys (see "Resource keys")
- status of the resources: free or busy (see "Resource keys")
- features active on the destination set: internal forwarding (see "Forwarding"), monitoring (see "Call Monitoring"), filtering (see "Manager/secretary screening"), external forwarding (see "External Forwarding")
- dynamic routing parameters programmed for a resource, the station or the hunting group

The system routes an **external** incoming call depending on the following criteria:

- PCX forwarding activated by an operator (see "PCX forwarding")
- system in normal or restricted service (see "Normal / restricted service (system level)")
- dissuasion message programmed in the active Operator Group (see "Automatic welcome")
- welcome message transmitted or not (see Automatic Welcome (Pre-announcement))
- destination station directory number: programmed in the public, private numbering plan (see "Incoming transit") or main only
- type of call: for a private subscriber or not
- station accessible or not
- destination station resource keys (see "Resource keys")
- status of the resources: free or busy (see "Resource keys")
- features active on the destination set: internal forwarding (see "Forwarding"), monitoring (see "Call Monitoring"), filtering (see "Manager/secretary screening"), external forwarding (see "External Forwarding")
- dynamic routing parameters programmed for a resource, the station or the hunting group
  NB: the dynamic routing programming on a resource key is duplicated on all the resources of the same type. To cancel this programming, erase all the keys of this type and re-program.

3.10.1.2 ADDITIONAL INFORMATION

- The sub-address and User to User Signaling (UUS) are not re-routed after a forwarding, a transfer or a call pick-up.
- When dynamic routing is active but D1 or D2 is not programmed, or T1 or T2 is not used, the system moves onto the next stage.
- The active and default Operator Groups may contain both integrated voice mail accesses

(see corresponding file).

- Calls from the private network are handled with the INTERNAL call dynamic routing parameters.

3.10.2 Configuration procedure

3.10.2.1 CONFIGURATION

- Configuring a "personalized" line i.e. a line with predetermined routing:

- by OMC (Expert View):
  - complete the DDI numbering plan: **Numbering -> Public Numbering Plan**
  - associate the number programmed in the DDI numbering plan with the appropriate line in normal and/or restricted mode: **External Lines -> List of Accesses -> Details -> Call-Dist.**
- by MMC-Station:
  - complete the DDI numbering plan: **NumPln -> PubNum**
  - associate the number programmed in the DDI numbering plan with the appropriate line in normal and/or restricted mode: **Access -> CalDis**

- Configuring a "reserved" line by attributing the feature "private subscriber" to the DDI number programmed for a personalized line:

- by OMC (Expert View): **Numbering -> Public Numbering Plan**
- by MMC-Station: **NumPln -> PubNum**

- Defining the dynamic routing parameters for a resource key:

- by OMC (Expert View): **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Keys -> Resource Key -> Dyn. Rout.**
- by MMC-Station: **Subscr -> Keys -> Modify -> Resou -> DynRou**

- Defining the dynamic routing parameters for a station:

- by OMC (Expert View): **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Dyn. Rout.**
- by MMC-Station: **Subscr -> DynRou**.

- Defining the dynamic routing parameters for a Hunting Group:

- by OMC (Expert View): **Hunting Groups -> Dyn. Rout.**
- by MMC-Station: **Groups -> Hunt -> DynRou**.

- To select the active Operator Group with the general call ringer as level 2 destination:

- by OMC (Expert View): check the **Gen. Bell to Gen. Level.** box in the "Dynamic Routing" window
- by MMC-Station: **GenBel** so that the display indicates "GENBELL" in capital letters

- To choose between the called party mail box and the automated attendant as destination level 1 when D1 is the directory number of the group containing the two voice mail accesses:

- by OMC (Expert View): **VMU as Auto. Attendant (level 1)**:
  - box selected: the automated attendant is called in D1
  - box not selected: the destination station's mail box is called in D1
- by MMC-Station: **VMUBeh -> Level 1**:
  - Level 1 = Auto-Sec: the automated attendant is called in D1
  - Level 1 = Message: the destination station's mail box is called in D1

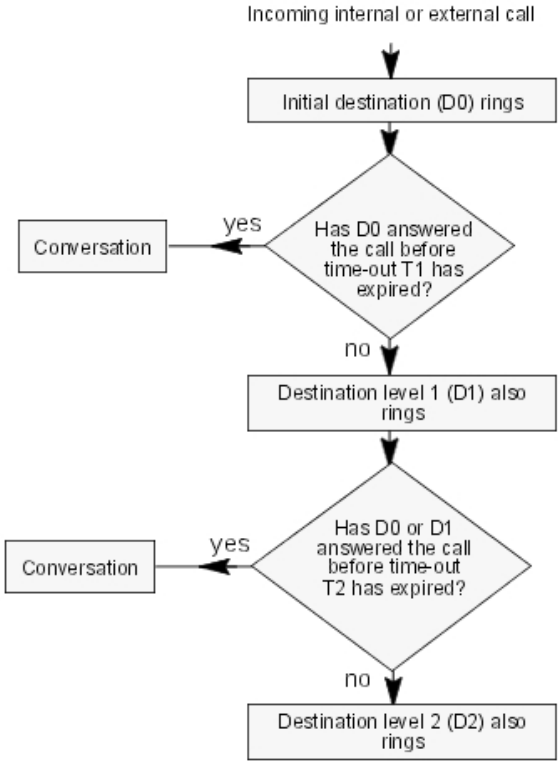
- To choose between the called party mail box and the automated attendant as destination level 2 if the voice mail belongs to the Operator Group called in D2:

- by OMC (Expert view): **VMU as Auto. Attendant (level 2)**:
  - box selected: the automated attendant is called in D2
  - box not selected: the destination station's mail box is called in D2
- by MMC-Station: **VMUBeh -> Level 2**:
  - Level 2 = Auto-Sec: the automated attendant is called in D2
  - Level 2 = Message: the destination station's mail box is called in D2

3.10.3 Operation

3.10.3.1 ACTIVATION/USE

Dynamic forwarding general principle



The initial destination D0 can be:

- a station
- a Hunting Group
- the general level (see "Operator stations")

If D0 is a station or a Hunting Group:

- D1can be a station, a Hunting Group, the voice mail unit (mail box or automated attendant) or a collective speed dial number
- D2 is the active Operator Group (see "Operator stations") with (only if the call is external) or without the general call ringer programmed in this group

If D0 is the general level:

- D1 can be a station, a Hunting Group or a collective speed dial number
- D2 is the default Operator Group (see "Operator stations") with (only if the call is external) or without the general call ringer programmed in this Hunting Group

Dynamic routing and call forwarding (see "Forwarding")

3.11 Time ranges

3.11.1 Overview

Prior to R2.0, the current time range was defined by the current hour during the day. Starting with R2.0, the time ranges depend also on the day of the week and on holidays. This new set-up offers more flexibility by allowing different time ranges, depending on whether the company is closed (weekend, holidays) or open.

Note:

Since the system time range enhancement implemented in R2.0, time ranges for restricted mode are no longer available in the subscriber details (only for R1.1).

3.11.1.1 DESCRIPTION

A day can be divided into a maximum of 7 time ranges each varying in duration. The time ranges allow the definition of:

- **the system's operating mode: N/R** (see sheet "Normal/restricted service"). This mode is used in the mechanisms of call distribution, discrimination, traffic sharing and integrated voice server (Automated Attendant and Audiotex). The system's operating mode is also used to define each user's operating mode (starting with R2.0, the mechanism described on the sheet "Normal/restricted service" is no longer used).
- **the active OS group** (see "Operator stations" and "Specific operator services"): one of 8 possible OS groups assigned to each time range.
- **the OS group's call forwarding state:** configured for each time range with the same recipient for all ranges.

Time ranges are also used in pre-announcement and welcome messages functions.

3.11.2 Configuration procedure

- To modify time ranges by OMC (Expert View) only:

• By OMC (Expert view): **Time ranges -> Start, N/R mode, Att. Grp., Att.div.**

56 time ranges may be configured: 7 (by day) x 8 (days of the week + holidays).

Note 1:

By default, only data for the first 2 time ranges are defined from Monday to Friday; the default values vary by country.

The list of holidays is completely independent from the list defined in the ARS mechanisms.

The data defined for a day (time ranges and pre-announcement) may be copied in order to assign them to one or several other data.

- Inhibiting, station by station, the switch to restricted service by time ranges (the station remains in normal service):

• by OMC (Expert View): **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Features -> Part 2 -> Inhibition Time ranges** .

Note 2:

The “Inhibit” flag makes it possible to remain in normal service in case the system switches to restricted service by operator command (N/R mode key).

3.12 Normal and Restricted Service

3.12.1 Overview

3.12.1.1 Description

System's operating mode: normal or restricted service is used in the following mechanisms:

- call distribution
- network lines discrimination
- network lines traffic sharing
- assignment of network lines for transmission of collective speed dial numbers
- Automated Attendant: normal service corresponds to the Automated Attendant opening hours, restricted service corresponds to the closing hours. Depending on the time, the following services have different parameters: company's welcome message, * question, language choice, direct call, menu and sub-menus configuration, default function, etc.
- Audiotext: normal service corresponds to the Audiotex opening hours, restricted service corresponds to the closing hours. Depending on the time, the following services have different parameters: * question, language choice and information message identifier.

Switching from NORMAL MODE to RESTRICTED MODE and vice versa depends on the following parameters:

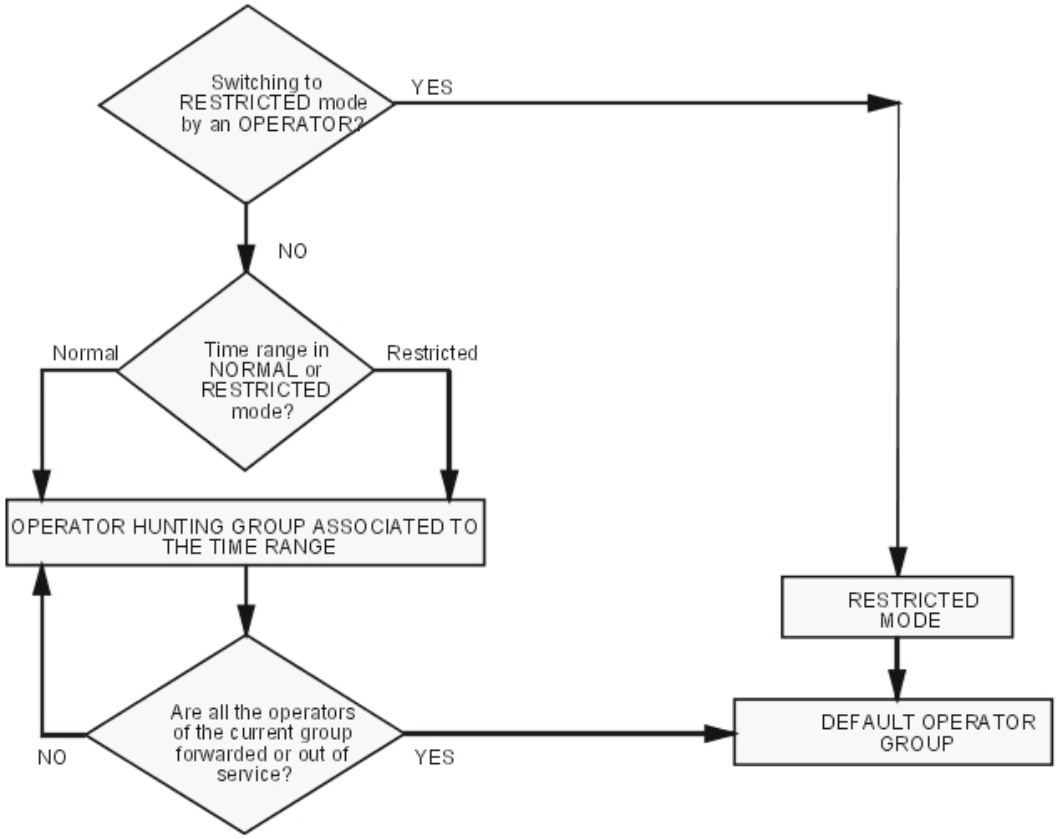
- the time (and therefore the time range)
- the Normal/Restricted mode function on the Operator Station

3.12.1.2 Additional Information

When the switchover to restricted mode is carried out from an Operator Station, users who do not have "Inhibition Flag" feature rights are forced into "user" restricted mode.

3.12.2 Operation

3.12.2.1 Activation/Use



3.13 Call Forwarding on System Restricted Use

3.13.1 Overview

3.13.1.1 FORWARDING OF ALL EXTERNAL INCOMING CALLS

The system is made up of two public numbering plans, one of which is used in normal service while the other is used in restricted service.

The restricted public numbering plan can be configured in such a way that certain DDI numbers are redirected to external destinations (using the group directory or the ARS mechanism) while others (Fax for example) reach their intended internal destinations.

3.13.2 Configuration procedure

3.13.2.1 Configuring the public numbering plan in restricted mode

The public numbering plan for restricted service mode can contain a maximum of 99 entries (0 by default).

- by OMC (Expert View): **Numbering -> Restricted numbering plan**
- by MMC-Station: **NumPln** -> **ResNum**

The configuration (beginning and end of range, base, NMT) is identical to that of the public numbering plan for normal service mode (PubNum).

If the destination of the DDI number is the same in normal and in restricted service, the 2 numbering plans must have the same configurations.

For more details, see “Numbering Plans" in the MMC-Station section.

3.13.3 Operation

3.13.3.1 Activation/Deactivation

Forwarding can be activated/deactivated from any station with an **N/R Mode** key. After pressing this key, dial the operator code.

Note:

It can also be activated by configuring the time ranges.

3.13.3.2 Example of use

Normal service public numbering plan

Start	End	Base	Feature
120	170	120	Set
200	230	200	Set
500	525	500	Hunting Group

Restricted service public numbering plan

Start	End	Base	Feature
120	170	120	Set
200	210	0	Collective Speed Dial
211	211	10	Collective Speed Dial
212	212	10	Collective Speed Dial
213	230	200	Set
500	524	500	Hunting Group
525	525	10	Collective Speed Dial

Internal numbering plan

Start	End	Base	Feature
8000	8010	0	Collective Speed Dial

Collective Speed Dial

Speed dial number	Level	Called number
8000	8	59242
8001	8	59243
.....	..	.....
8009	8	59251
8010	8	59252

In this example, the public numbering plan for restricted service uses the collective speed dial table.

The numbers 120 to 170 and 213 to 230 keep their normal destinations when the system is in restricted service mode, as do calls to the range 500 to 524.

The external incoming calls to stations 200 to 209 are forwarded to the destinations defined by the first 10 entries in the collective speed dial table (8000 to 8009). Calls to numbers 210, 211, 212 and calls to group 525 are forwarded to the destination defined by the entry 8010 in the collective speed dial table.

3.14 Normal and Restricted User

3.14.1 Overview

3.14.1.1 NORMAL AND RESTRICTED SERVICE - USER LEVEL

The normal/restricted service configuration for each user and for each time range is no longer available starting with R2.0; the system's normal/restricted operating mode is used (see sheet “Time ranges”).

3.14.1.1.1 Description

Depending on the time range, the system operates in either normal or restricted mode. The service mode affects the way in which the system distributes incoming calls and controls users" outgoing calls.

The installer can also configure the operation in "user" restricted mode for each station and in each time range. ; starting with R2.0, this option is no longer available.

3.14.1.1.2 Additional Information

A station in **restricted** service and **unlocked** (see "Station comfort features", "Telephone services" section) switches to user normal service when the code for **unlocking** the station is entered: this station can no longer be switched to restricted service but it can be locked.

Starting with R2.0, a noteworthy address "**LockBypass**" allows to override this mechanism:

- LockBypass = 1 (default value): mechanism described above
- LockBypass = 0: a user in restricted service mode who unlocks his locked station, switches back to restricted service (as opposed to normal service); the user therefore has no means of switching from restricted service to normal service.

3.14.2 Configuration procedure

3.14.2.1 Configuration

- Define the time ranges during which a station operates in restricted service:

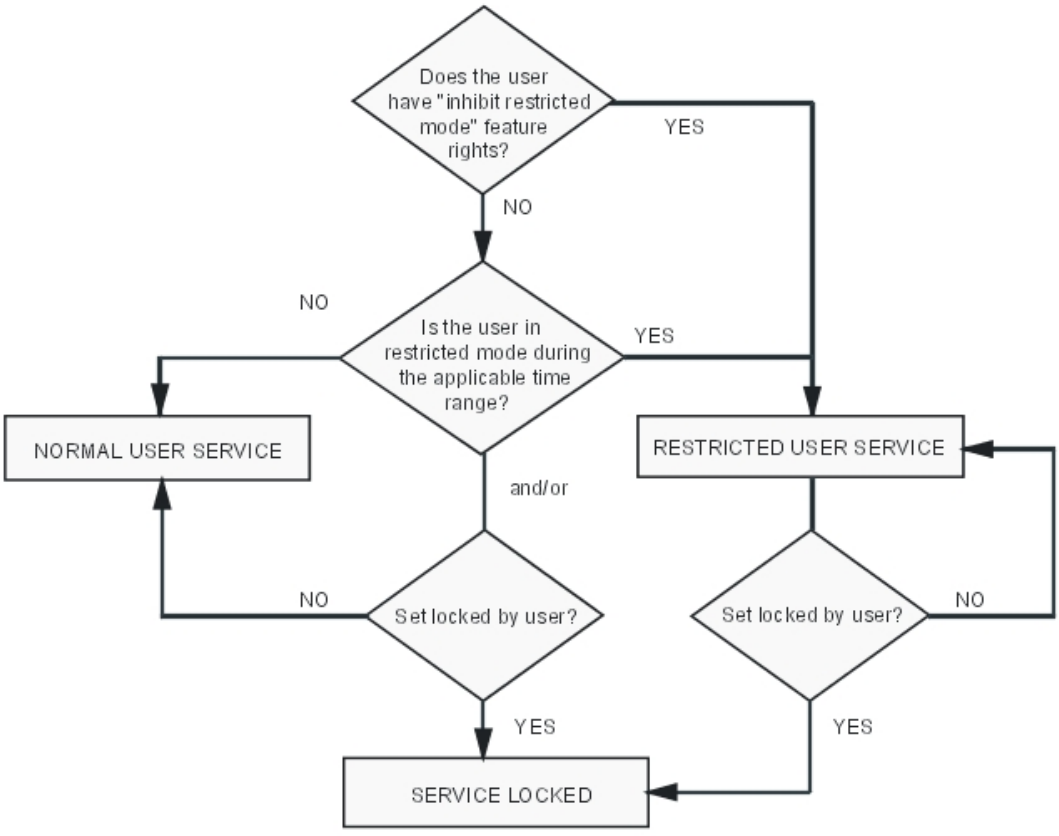
• by OMC (Expert View): **Subscribers/Base stations List** -> **Subscribers/Base stations List** -> **Details** -> **Barring** -> **"Time Ranges (outgoing traffic)"**

- To specify whether or not to inhibit the switch to restricted service when the system is switched to restricted service by an operator; see "Specific operator station services", in the "Telephone services" section:

• by OMC (Expert View): **Subscribers/Base stations List** -> **Subscribers/Base stations List** -> **Details** -> **Features** -> **"Inhibition Flag"**

3.14.3 Operation

3.14.3.1 Activation/Use



3.15 Automatic Welcome

3.15.1 Overview

3.15.1.1 DESCRIPTION

This feature makes it possible to send a spoken message to a network caller before connecting the caller to a called party. The called party can be:

- a station
- a Hunt Group (see "Hunt Groups")
- an Attendant Group (see "Attendant stations")

The message can be sent to the caller either:

- before the destination station rings: this is mode 1
- while the destination station is ringing: this is mode 2

and, either:

- only if the called party is busy
- no matter what status the called party is in: free or busy

The system allows you to play up to 8 pre-recorded messages. These messages can be:

- welcome messages
- redirection messages (also called "dissuasion messages": if a greeting message is member of the active attendant group, the system plays the message to the caller and releases the call)
- voice prompts (for DISA transmit for example)

The pre-announcement can be defined for:

- 15 DID numbers (individual pre-announcement)
- all the system's users (general pre-announcement)

The installer can allocate a maximum of one message for each of the 7 time ranges.

3.15.1.2 ADDITIONAL INFORMATION

- Duration of default music-on-hold: 16 s
- Maximum duration of the customisable music-on-hold: 2 min by default and up to 10 min with a hard disk
- Maximum duration of a redirection (dissuasion) message: 16 s
- Maximum number of pre-announcement messages: 8
- The automatic welcome is not activated when the called party has activated text answering or paging
- An empty Hunt Group can no longer use the Automatic Welcome service.
- The automatic welcome only concerns voice type calls.
- The automatic welcome does not concern calls from the private network
- In mode 1, an external call released by the caller before being presented to the initial destination, is not recorded in the repertory of unanswered calls.

- An external call on an analogue line, received with transmission of the welcome message and remaining unanswered, is released by the system after a time-out.
- Call charge units arriving during the transmission of the welcome message are assigned to the called party.
- Under no circumstances will the external call receive two welcome messages.
- An error message appears on the station display when the automatic welcome cannot transmit the message to the incoming call.

3.15.2 Configuration procedure

3.15.2.1 CONFIGURATION

- Selecting the source for the please wait music:

• by OMC (Expert View): **System Miscellaneous -> Messages and Music -> Music on Hold** • by MMC-Station: **Voice -> MusSrc -> Stndrd, VoicPr or Tape**

- Recording RAM welcome and dissuasion messages – MMC-Station only:

Voice -> RecMsg -> Msg1 to Msg8 -> Record

- Listening to recorded RAM welcome and dissuasion messages – MMC-Station only:

Voice -> RecMsg -> Msg1 to Msg8 or Music -> Listen

- Defining DDI numbers, for individual pre-announcement:

• by OMC (Expert View): **Numbering -> Numbering Plans -> Public Numbering Plan** • by MMC-Station: **NumPln -> PubNum**

- Assigning welcome messages:

• by OMC (Expert View): **Misc. Subscribers -> Pre-announcement** • by MMC-Station: **PreAnn -> Add -> Msg**

- Defining the pre-announcement mode (none, mode 1 or mode 2) depending on the time range:

• by OMC (Expert View): **Misc. Subscribers -> Pre-announcement** • by MMC-Station: **PreAnn -> Add -> Mode**

- To define whether the message is sent only if the called party is busy, or regardless of status, depending on the time range – OMC (Expert View) only:

Subscribers Misc. -> Preannouncement

- To modify the pre-announcement time-outs:

• by OMC (Expert View): **Subscribers -> Pre-announcement -> Timers** • by MMC-Station: **Global -> Rd/Wr -> Timers -> "AnsMsgTim" -> Return -> Memory**

- To select transmission of ringing tone or "please wait" music (for a free station):

- by OMC (Expert View): **System Miscellaneous -> Memory Read/Write -> Misc. Labels -> "TonPrRng"**
- by MMC-Station: **Global -> Rd/Wr -> Address -> "TonPrRng" -> Return -> Memory**

- To select transmission of ringing tone or "please wait" music for a busy station:

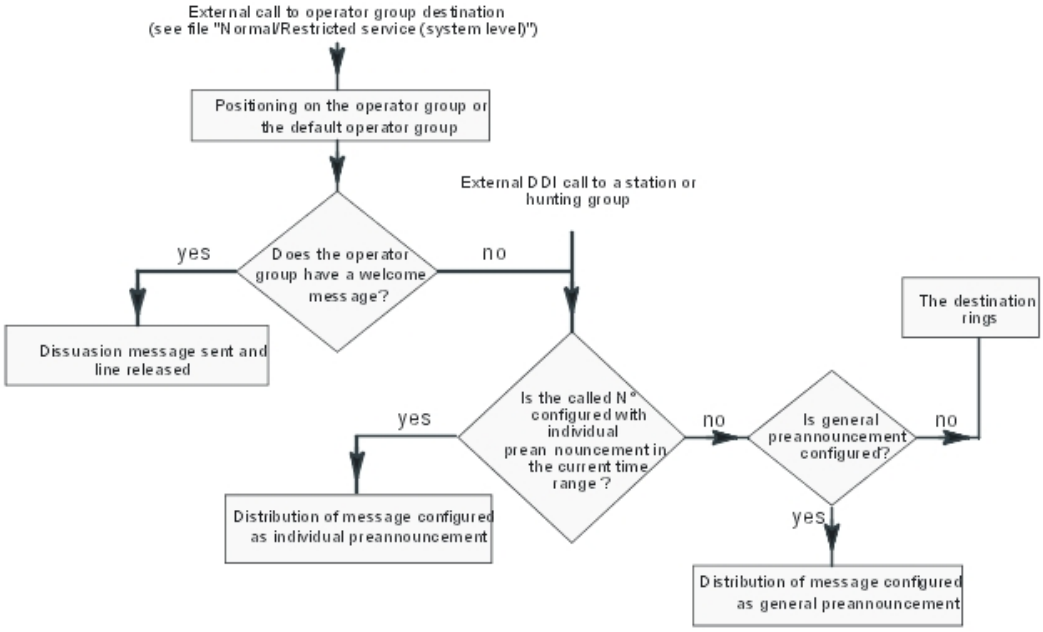
- by OMC (Expert View): **System Miscellaneous -> Memory Read/Write -> Misc. Labels -> "TonPrCmp"**
- by MMC-Station: **Global -> Rd/Wr -> Address -> "TonPrCmp" -> Return -> Memory**

- To select transmission of ringing tone or "please wait" music for a Hunting Group (free or busy):

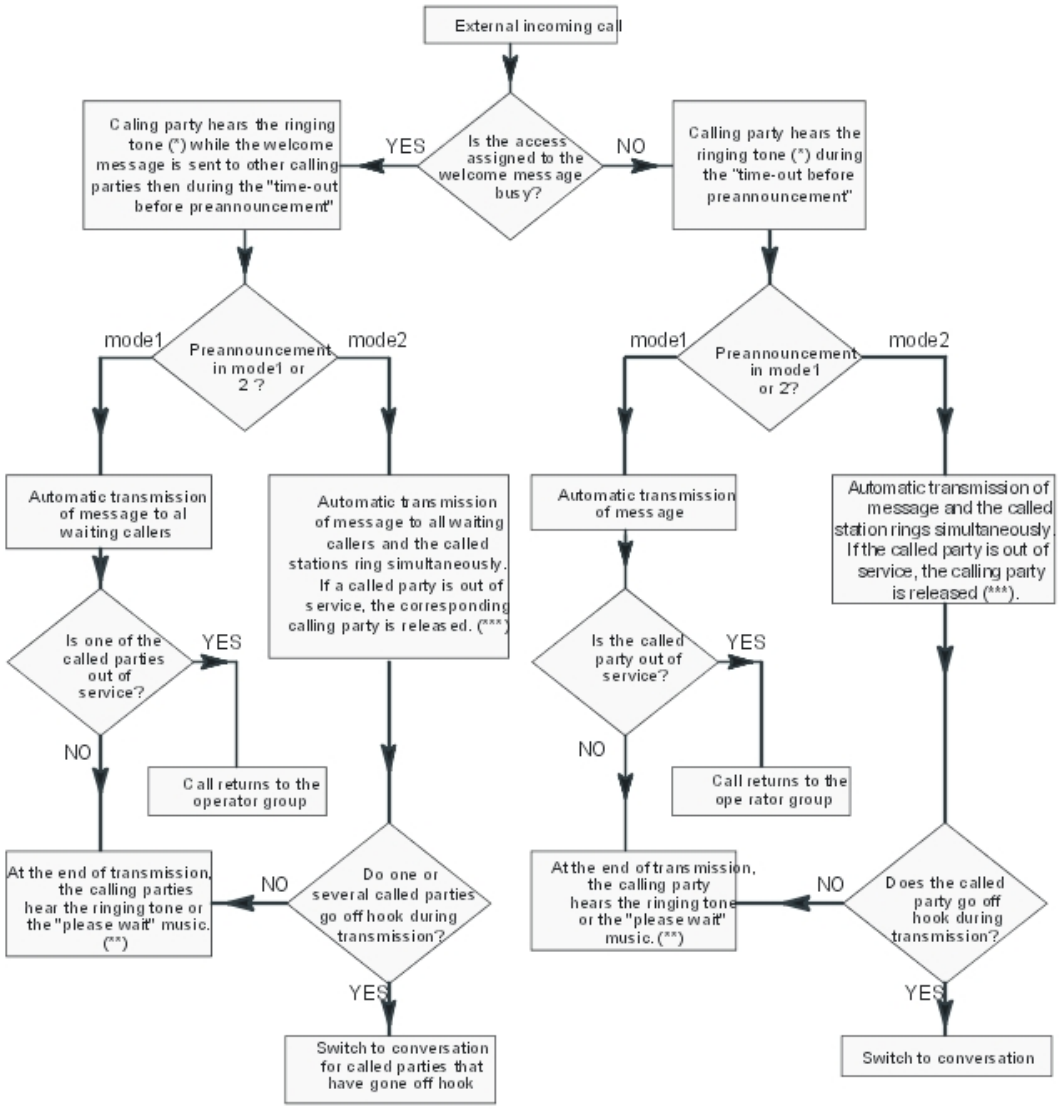
- by OMC **System Miscellaneous -> Memory Read/Write -> Misc. Labels -> "TonPrGrp"**
- by MMC-Station: **Global -> Rd/Wr -> Address -> "TonPrGrp" -> Return -> Memory**

3.15.3 Operation

3.15.3.1 ACTIVATION/USE



Tree diagram operational after the system has determined the type of pre-announcement:



(*) sent by the public exchange

(**) The ringing tone or the "please wait" music is heard: - by a caller on an analog TL up until the "Release after pre-announcement (norm or restr mode)" time-out has lapsed - by a caller on digital access up until the called party goes off hook.

(***) ISDN calls only

3.16 Direct Dialling Inwards

3.16.1 Recovery

3.16.1.1 Overview

DDI numbers can:

- contain up to 8 digits.
- use the numbering recovery mechanism described below.

3.16.1.1.1 NUMBERING RECOVERY

Description

When, in an existing installation, a new range of DDI numbers needs to be added, and the new sequence allocated by the public exchange overlaps the existing range, the installer can make use of the "DDI with more than 4 digits" mechanism.

Example:

Consider an existing system with the DDI numbers (XX = any possible "intercity prefix", "intercity code" and "recall prefix" – these can vary from country to country):

- XX 1 41 23 40 10 to XX 1 41 23 40 19 assigned to stations 120 to 129
- XX 1 41 23 41 00 to XX 1 41 23 41 19 assigned to stations 130 to 149

The exchange allocates the new range XX 1 41 33 40 15 to XX 1 41 33 40 24: these numbers are assigned to stations 150 to 159.

As described below, the numbering plan does not allow:

- use of the whole DDI range available; in actual fact, in order to route a DDI number to a called station, the system only analyzes the last 4 digits of the number received from the network and the DDI sequences XX 1 41 23 40 10 and XX 1 41 33 40 15 have in common, the range of the last 4 digits 40 15 to 40 19.
- transmission of the exact number of the caller (see "ISDN services") since the system would require two installation numbers (XX 1 41 23 and XX 1 41 33) in order to operate correctly, which is impossible.

Additional Information

- Maximum number of entries in the modification table of DDI numbers: 18
- Maximum number of digits for an entry in the modification table of DDI numbers: 16.
- Maximum number of digits in a substitution number: 4.

3.16.1.2 Configuration procedure

3.16.1.2.1 Configuration

- Configuring the installation number:

• by OMC (Expert View): **Numbering -> Installation Numbers** • by MMC-Station: **Global -> InsNum -> Public**

- Filling in the substitution table:

• by OMC (Expert View): **Numbering -> DDI Number Modification Table** • by MMC-Station: **Num Pln -> PubNMT**

- Completing the DDI numbering plan:

- by OMC (Expert View): **Numbering -> Public Numbering Plan**
- by MMC-Station: **NumPln -> PubNum**

3.16.1.3 Operation

3.16.1.3.1 Activation/Use

Functional analysis

A "DDI with more than 4 digits" mechanism is based on the analysis of all the received digits. They are modified using a substitution table and analyzed by the Public numbering plan. Programming such a mechanism requires you to have a global view of your DDI sequences.

Procedure to follow

- check the DDI sequences
- deduce the installation number by removing the "intercity prefix", "intercity code" if found
- deduce the minimum number of digits required to cover the DDI ranges
- analyze the remaining digits and create the DDI modification table
- configure the DDI numbering plan
- activate the mechanism

Application using the above example

- DDI sequences:
  - 1st sequence: 1 41 23 40 10 to 1 41 23 40 19 for stations 120 to 129
  - 2nd sequence: 1 41 23 41 00 to 1 41 23 41 19 for stations 130 to 149
  - 3rd sequence: 1 41 33 40 15 to 1 41 33 40 24 for stations 150 to 159
- Deduction of the installation number:
  Digits 1 41 are common to the 3 sequences of DDI numbers: these 3 digits will make up the installation number. THE "INSTALLATION NUMBER" FIELD CAN BE LEFT EMPTY IF THERE IS NO COMMON DIGIT.
- Deduction of the minimum number of digits to cover the DDI ranges:
  1 or 2 digits, at least, are necessary in order to join a series of stations.
  - 1st sequence: 1 41 23 40 1 **0** to 1 41 23 40 1 **9**: 10 stations with 1 digit (0 to 9)
  - 2nd sequence: 1 41 23 41 **00** to 1 41 23 41 **19**: 20 stations with 2 digits (00 to 19)
  - 3rd sequence: 1 41 33 40 **15** to 1 41 33 40 **24**: 10 stations with 2 digits (15 to 24)
- analysis of the remaining digits (by removing the installation number and the digits necessary to cover the DDI ranges) and creation of the DDI modification table:
  - 1st sequence: 1 41 **23 40 1**0 to 1 41 **23 40 1**9
  - 2nd sequence: 1 41 **23 41** 00 to 1 41 **23 41** 19
  - 3rd sequence: 1 41 **33 40** 15 to 1 41 **33 40** 24

  The remaining digits are to be replaced by the substitution digits ,which, themselves, will be analyzed in the DDI numbering plan. To do this, apply the following rule:
  Minimum number of digits to cover the DDI range + Length of the substitution number = 4 (i.e. the maximum number of digits as defined in the DDI numbering plan).
  For example, one can:
  - for the 1st sequence: substitute "23 40 1" by "810" (in fact, "810" + 1 digit from 0 to 9 = 4 digits)

- for the 2nd sequence: substitute "23 41" by "82" (in fact, "82" + 2 digits from 00 to 19 = 4 digits)
- for the 3rd sequence: substitute "33 40" by "83" (in fact, "83" + 2 digits from 15 to 24 = 4 digits)

- Creation of the DDI numbering plan (from the DDI numbers modification table):

Function	Begin	End	Base
Station	--	**9**	120
Station	--	--	130
Station	--	--	150

Result of the above example

The DDI number received from the network (here, XX 1 41 33 40 20) is analyzed by the system as follows:

- removal of any intercity prefix, etc... as well as the installation number: leaves the number 33 40 20.
- analysis of this number in the substitution table (the mechanism being authorized, this analysis is carried out automatically for all DDI numbers received): the system deducts the number 8320
- analysis of the DDI number thus obtained in the DDI numbering plan: the system makes station 155 ring.

3.17 Class Compatibility

3.17.1 Overview

3.17.1.1 DEFINITION

This feature allows information (from the public ISDN network, public analog trunks - APA and AMIX boards - or internal system network) to be presented on analogue CLASS terminals connected to Alcatel-Lucent OmniPCX Office Communication Server.

In idle, when ringing or during a call, analogue CLASS terminals have access to:

- date and time of the system
- CLIP (calling line identification)
- calling line identification restriction management
- caller's name (if available in the system directory)
- management of the Message LED

3.17.1.2 HARDWARE REQUIREMENTS

CLASS terminals connected to SLI boards.

3.17.2 Configuration procedure

3.17.2.1 CONFIGURATION

- Specifying the analog station as a CLASS terminal:

- by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Classiq. (class)**
- by MMC-Station: **Subscr** -> **Termnl** -> **Class**

- Activating the name display:

- by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Features** -> **Name Display**

3.18 VN7 Compatibility

3.18.1 Overview

3.18.1.1 VN7 COMPATIBILITY

This section lists the compatibilities between Alcatel-Lucent OmniPCX Office Communication Server and version VN7 of the French ISDN network (RNIS).

3.18.1.1.1 BASIC CALLS

Basic calls (incoming and outgoing) are supported on the S0 and T0/T2 accesses.

3.18.1.1.2 ADDITIONAL SERVICES

The compatibility of additional services varies according to whether the service is required on the user side (S0) or on the network side (T0/T2)

Service	S0 side compatibility	T0/T2 side compatibility
AOC-E Advice Of Charge at the End of the call	YES	NO
AOC-D Advice Of Charge During the call	YES	YES
CLIP/CLID Calling Line Identification Presentation	YES	YES
DDI Direct Inward Dialing	YES	Not applicable
MSN Multiple Subscriber (User) Number	YES (in Point-to-Multipoint)	YES
TP Terminal Portability	Not applicable	YES (locally, on the same access)
SUB Sub-Address	YES (limited to 4 digits)	YES (limited to 4 digits)

CW Call Waiting	NO	NO
HOLD	NO	YES
MCID Malicious Call Identification	YES (Alcatel-Lucent 8/9 series sets, Reflexes and S0 terminals)	YES
UUS1 User to User Signalling	YES (limited to 32 characters)	YES (limited to 32 characters)
CFB Call Forwarding on Busy	NO	NO
CFU Call Forwarding Unconditional	YES (in Point-to-Point)	YES
CFNR Call Forwarding on No Reply	NO	NO
CD Call Deflection	YES (in Point-to-Multipoint)	NO
CCBS Call Completion on Busy Subscriber	YES (in Point-to-Point)	NO
3PTY 3 Party conference	NO	NO
ECT Explicit Call Transfer	NO	NO
CNIP Caller Name Identification Presentation	NO	NO

3.19 Specific Numbering Plan

3.19.1 Detailed description

3.19.1.1 SPECIFIC NUMBERING PLANS

3.19.1.1.1 8 DIGIT NUMBERING PLANS

Station and hunting group call numbers, as well as collective speed dial numbers, can have up to 8 digits.

3.19.1.1.2 STAR NUMBERING

To use a 2, 3 or 4-figure default numbering plan, you can choose between a country-specific numbering plan or a generic numbering plan in which most codes (service codes or Features in Conversation) start with *; this structure provides several ranges for allocating DDI numbers to sets.

The default star numbering plans are described in the following pages.

Configuration

- To select the default numbering plan:

- by OMC (Expert View): **Numbering -> Default Numbering Plan**
- by MMC-Station: **NumPln -> Nbdigi**

Note:
The default numbering plan can also be selected using OMC Easy View once the system is running.

Codes common to all countries

Internal numbering plan

Functions	2-digit	3-digit	4-digit
Cancel all forwardings	#21	#21	#21
Cancel "follow me" forwarding	#27	#27	#27
Immediate call forwarding	* 21	* 21	* 21
Forward on busy	* 22	* 22	* 22
Do Not Disturb	* 23	* 23	* 23
Forward to pager	* 24	* 24	* 24
Group call forwarding	* 25	* 25	* 25
Disconnect from group	* 26	* 26	* 26
Rejoin the group	# 26	# 26	# 26
Follow-me	* 27	* 27	* 27
Selective forwarding	* 28	* 28	* 28
Cancel callback	# 5	# 5	# 5
Voice Mail Unit (secret code)	**6	**6	**6
Voice Mail Unit (secret code)	*#6	*#6	*#6
Redial last number	**0	**0	**0
Room status	* 70	* 70	* 70
Lock/unlock	* 71	* 71	* 71
Appointment reminder (prog.)	* 72	* 72	* 72
Protect against intrusion	* 73	* 73	* 73
Replace set	* 78	* 78	* 78
Move set	* 79	* 79	* 79
Individual call pick-up	* 81	* 81	* 81
Pick up group	* 82	* 82	* 82
General Call Answer	* 83	* 83	* 83
Parked call retrieval	* 84	* 84	* 84
Programming mode	* 87	* 87	* 87
Text mail	* 88	* 88	* 88

Group broadcast	* 01 to *08	* 01 to *08	* 01 to *08
Subscriber calls	10 to 79	100 to 799	1000 to 7999
Seize secondary trunk groups	* 50 to *53	* 500 to *534	* 500 to *534
Hunting Group calls	* 54 to *59	* 540 to *565	* 540 to *565
Collective speed dial	8000 to 8999	8000 to 8999	8000 to 8999

Feature code table

Consulting camped calls	* 9	* 9	* 9
Trunk line allocation	#11 to #17	#11 to #17	#11 to #17
Trunk allocation + MTR	#21 to #27	#21 to #27	#21 to #27
Call Parking	* 84	* 84	* 84
Malicious call identification	* 89	* 89	* 89
Cancel enquiry	* 1	* 1	* 1
Shuttle	* 2	* 2	* 2
Conference	* 3	* 3	* 3
Intrusion	* 4	* 4	* 4
Automatic callback request	* 5	* 5	* 5
DTMF end-to-end signaling	* 6	* 6	* 6
Main PCX recall (calibrated loopbreak)	* 7	* 7	* 7

Country specific

Operator call and main trunk group seizure

Different codes for operator calls and for seizing the main trunk group apply in each country. This results in different ranges of subscriber numbers.

Country	OS call	Seize trunk group	2/3/4-digit subscriber	Paging type
Austria	10	0	11/110/1100	prefix
Australia	9	0	10/100/1000	prefix
Belgium	11	0	12/120/1200	suffix
Switzerland	11	0	12/120/1200	prefix
Germany	10	0	11/110/1100	prefix
Denmark	9	0	10/100/1000	prefix
Spain	9	0	10/100/1000	suffix
Finland	9	0	10/100/1000	suffix
France	9	0	10/100/1000	suffix
Britain	0	9	10/100/1000	suffix
Greece	10	0	11/110/1100	prefix
Ireland	10	0	11/110/1100	prefix
Italy	9	0	10/100/1000	prefix

Netherlands	9	0	10/100/1000	prefix
Norway	9	0	10/100/1000	prefix
Portugal	9	0	10/100/1000	prefix
Sweden	9	0	10/100/1000	prefix
SMBI	10	0	11/110/1100	prefix

Paging type

Paging can be by prefix or by suffix.

Paging by prefix: the internal numbering plan has to have 2 codes: one for the "Prefix Paging Activation" function and one for the "Paging Answer Selective" function.

Paging by suffix: a "paging answer general " code is added to the internal numbering plan and a "suffix paging activation" code is added to the features plan.

Paging by suffix: Internal numbering plan entries

Function	2-digit	3-digit	4-digit
Answer paging general	* 85	* 85	* 85

Paging by suffix: features plan entries

Function	2-digit	3-digit	4-digit
Suffix paging activation	* 86	* 86	* 86

Paging by prefix: internal numbering plan entries

Function	2-digit	3-digit	4-digit
Answer paging selective	* 85	* 85	* 85
Prefix paging activation	* 86	* 86	* 86

3.20 Alternative CLIP and COLP Numbers

3.20.1 Overview

3.20.1.1 Overview

Alternative CLIP/COLP number is used to send a specific CLIP/COLP number instead of the usual CLIP/COLP number. The typical calling number is a concatenation of installation (system) number and DDI set (extension) number.

There are several types of alternative numbers:

- Alternative system CLIP number
- Alternative user CLIP/COLP number
- Alternative access CLIP/COLP number (as of R7.0)

Definitions:

- **CLIP** (Calling Line Identification Presentation): identification number sent by the caller

when making an outgoing ISDN (or VOIP) call.

- **COLP** (Connected Line Presentation): identification number returned by the called party to the caller when an ISDN (or VOIP) call is received. Some public networks do not allow COLP numbers.

Note 1:

Some public networks do not allow CLIP or COLP numbers outside their numbering plan.

Note 2:

*On VoIP trunks, the CLIP/COLP alternative number is only valid if the **VoIP route** is a public route. The **Net** parameter of the ARS configuration must be set to **Pub**. In all other cases, the non alternative public number is sent.*

3.20.1.2 Description

3.20.1.2.1 Alternative System CLIP Number

In this case, the alternative CLIP number is defined for all users of the Alcatel-Lucent OmniPCX Office Communication Server. Whether the set is making a call or receiving a call, the remote party receives the same CLIP number.

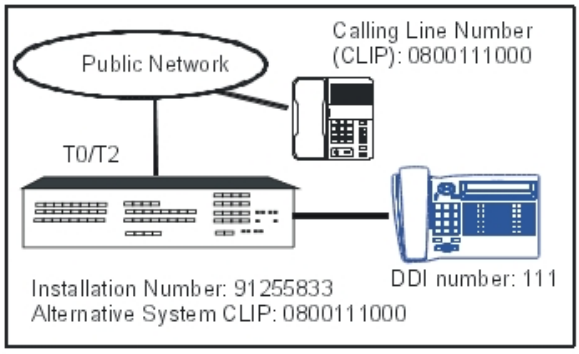


Figure 3.20 : CLIP Number with Alternative System Number

Example of use:

It enables a company with several sites to send always the same number to external called parties.

3.20.1.2.2 Alternative User CLIP/COLP Number

In this case, the alternative CLIP/COLP number is defined for a specific user. When this set is making a call or receiving a call, the remote party receives the specific CLIP/COLP number.

The CLIP or COLP number is a concatenation of the installation number and alternative user number.

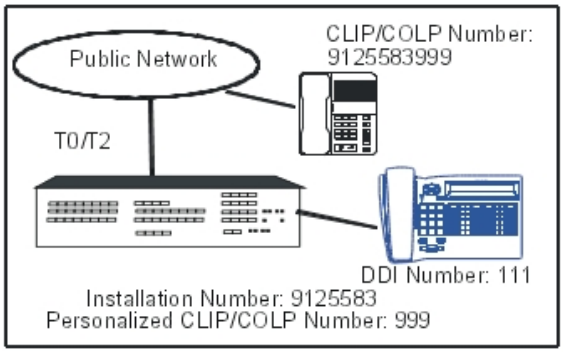


Figure 3.21 : CLIP/COLP Number with alternative User Number

Example of use:

To hide the actual identity of a set: in a group of sets, all sets are configured with an alternative number to the DDI number of the group. Remote parties see the DDI number of the group but the actual number of the calling set is hidden.

3.20.1.2.3 Alternative Access CLIP/COLP Number

Alternative access numbers allow to send a specific CLIP/COLP number for each ISDN or VOIP access on which the feature is enabled.

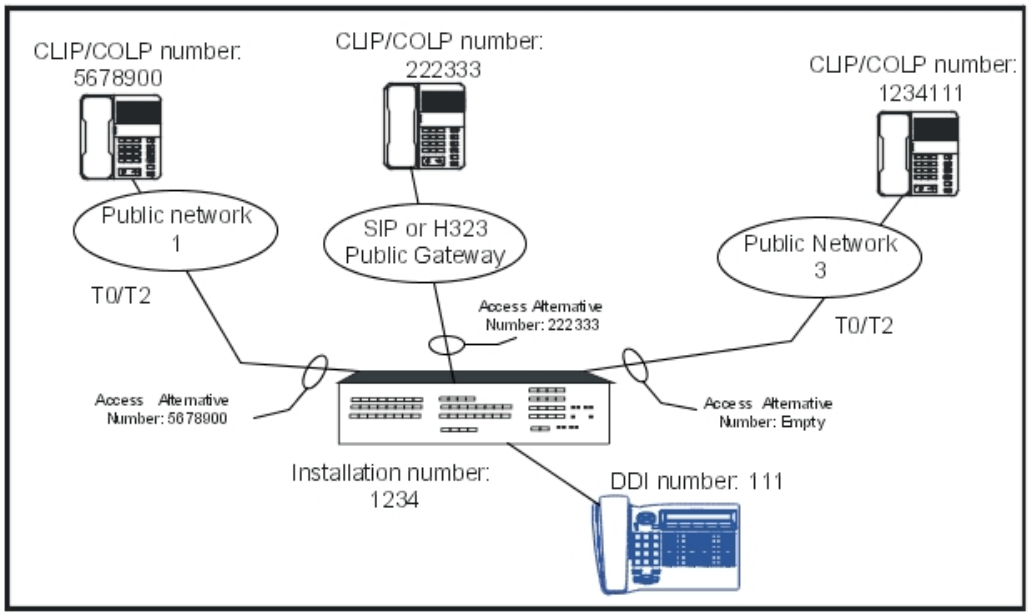


Figure 3.22 : Configuration Example of CLIP/COLP Alternative Access Number

This feature can be required when several public networks are connected to the Alcatel-Lucent OmniPCX Office Communication Server. Some public networks do not allow CLIP or COLP numbers outside their numbering plan.

3.20.1.2.4 Interactions

When several types of alternative numbers are configured, for each call, a system rule selects the number transmitted to the remote party. The priority among the matching alternative numbers is as follows :

1. Alternative access number
2. Alternative system number
3. Alternative user number

3.20.1.3 Configuration

3.20.1.3.1 Alternative System CLIP Number

1. Select in OMC: **Numbering** > **Installation Numbers**
   Select in MMC: **Global** > **InsNum**
2. Review/modify the following attributes:

Alternative System CLIP (in OMC) **AltCLI** (by MMC)	Enter the alternative system CLIP number (22 digits maximum) When this parameter is empty, the alternative system feature is disabled. *Note:* *The CLIP number sent to the remote party must be compatible with the company's subscription.* *Some public networks do not allow CLIP numbers outside their numbering plan.*

3. Confirm your entries

3.20.1.3.2 Alternative User CLIP/COLP Number

1. Select in OMC only: **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** ->**Misc**
2. Review/modify the following attributes:

Alternative CLIP/COLP number (in OMC only)	Enter the alternative user CLIP/COLP number (8 digits maximum) The CLIP/COLP number sent to the remote party is a concatenation of the installation number and the number entered here. When this parameter is empty, the alternative user feature is disabled. *Note:* *The CLIP/COLP number sent to the remote party must be compatible with the company's subscription.* *Some public networks do not allow CLIP or COLP numbers outside their numbering plan.*

3. Confirm your entries

3.20.1.3.3 Alternative Access CLIP/COLP Number

1. According to the access type:

- Select in OMC: **External Lines** -> **List of Accesses** -> **Digital Accesses Details** for ISDN accesses (T0, T1 or T2)
  If the protocol is EDSS1, the field can be configured.
  If the protocol is QSIG, the field cannot be configured (unavailable and empty field).
- Select in OMC: **External Lines** -> **List of Accesses** -> **VOIP Details** for VoIP access

2. Review/modify the following attributes:

Alternative CLIP/COLP Number (by OMC)	Enter the alternative access CLIP/COLP number (22 digits maximum) When this parameter is empty, the alternative access feature is disabled. The alternative access number can be configured in any format: local, national or international. Example for France: 0390677700 (national format) or 003390677700 (international format). *Note:* *This number must be compatible with the company's subscription used for this access.* *Some public networks do not allow CLIP or COLP numbers outside their numbering plan.*

3. Confirm your entries

3.21 CLI Calling Party Identifier

3.21.1 Overview

3.21.1.1 DESCRIPTION

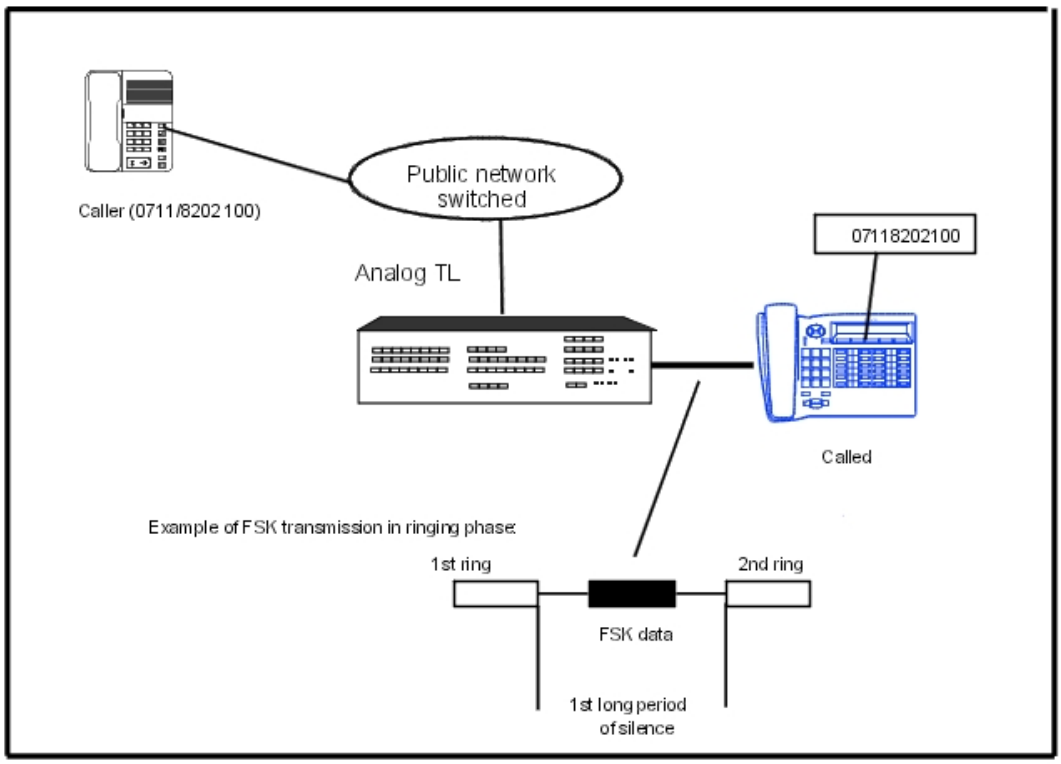
The CLI (Calling Line Identification) feature for APA (Analogue Public Access) and AMIX/AMIX-1 (Analogue Mixed Line) boards allows the caller number to be received through

the analogue switched public network.

This feature is based on the CLIP (Calling Line Identification Presentation) additional service; the CLIP information is transmitted via FSK (Frequency Shift Keying) asynchronous signals in on-hook mode (during ringing).

The FSK signal can be detected in two different ways: centrally at the CPU level or locally via the APA board (CLIDSP daughter board).

The central detection at the CPU board level is not available in the USA (local detection only via CLIDSP daughter board on APA).



3.21.1.2 HARDWARE REQUIREMENTS

Depending on the detection type, the system must be equipped with:

- local detection: the APA boards must be equipped with the CLIDSP daughter boards.

  Note:
  5 APA boards per module, with or without CLIDSP daughter boards; one CLIDSP daughter board for 8 accesses.

- central detection: no special hardware. 6 incoming calls may be handled simultaneously.

3.21.1.3 CONFIGURATION

Enable the service, line by line, through OMC (Expert View) only:

External lines -> Details -> CLIP

3.22 Busy Greeting on Voice Mailbox

3.22.1 Overview

3.22.1.1 DESCRIPTION

This feature makes it possible to immediately route an external incoming call to the called party's voice mailbox if the line is busy (Busy degree 1 or degree 2). The caller hears a specific welcome message and can, if he/she wishes, leave a message in the called party's voice mailbox.

Dynamic routing to the voice mailbox is immediate even when the dynamic routing timer is configured.

The service is activated if there is an incoming call to a busy set and:

- for all the sets if the "DynRoutBsy" flag = 1
- or if "DynRoutBsy" = 0, but only on the sets that have access to this function

3.22.1.2 ADDITIONAL INFORMATION

Summary table

	Service active (flag DynRoutBsy = 1)		Service inactive (flag DynRoutBsy = 0)
	Called party busy	Called party free	
Routing to voice mailbox	IMMEDIATE	NO	NO
Level 1 dynamic routing	Does not start	T1 timer	T1 timer
Level 2 dynamic routing	Does not start	T2 timer	T2 timer

Call forwarding

Routing to a voice mailbox is not performed if the user called has programmed the forward function on his/her set. The service becomes valid when the forward function is cancelled.

Forward on busy

If the user has programmed his/her voice mailbox as the destination of Call forwarding on busy, the internal or external caller will also hear the message.

Default value

After a cold reset, the "DynRoutBsy" flag is set to 0 (service inactive) by default and set-by-set activation is cancelled (active in France).

Caution:

The mechanism is also active if the destination of T1 dynamic routing is a set instead of the VMU. In this case, the destination of dynamic routing will be rung immediately if the set called is busy.

There is no indication of service activation on the sets.

3.22.2 Configuration procedure

3.22.2.1 CONFIGURATION

- To globally activate the service, or not:

• by OMC (Expert View): **System Miscellaneous -> Memory Read/Write -> Misc. Labels -> "DynRoutBsy"** • by MMC-Station: **Global -> Rd/Wr -> Address -> "DynRoutBsy" -> Return -> Memory**

0: service inactive
1: service active; all incoming calls to a busy user are immediately forwarded to the called party's voice mailbox

- To activate the service or not, set by set – OMC (Expert View) only:

Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Dyn. Rout.

- Configuring the VMU grouping as Level 1 called party in the case of dynamic routing

• by OMC (Expert View): **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Dyn. Rout.** • by MMC-Station: **Subscr -> DynRou**.

3.23 Completion of Calls to Busy Subscriber

3.23.1 Overview

3.23.1.1 DESCRIPTION

CCBS - Completion of Calls to Busy Subscriber - is an addition to the ETSI service provided by the system on T0/T2 public exchange connections. (The ETSI service is country-dependent.)

This feature can be considered as an extension of the "Automatic callback on busy set" service. CCBS requires a service subscription with the exchange carrier offering this feature which can be activated for incoming or outgoing calls.

3.23.1.2 ADDITIONAL INFORMATION

- CCBS cannot be activated on incoming calls to a group, or to a set with call forwarding activated
- CCBS is deactivated automatically in the following cases:
  - CCBS on outgoing call:
  - expiration of the timeout during BookRecTim; by default, 25 seconds
  - expiration of the BookBusTim timeout; by default, 30 minutes
  - expiration of the public exchange timeout T-CCBS6 (timeout during which the public exchange user must free the line; 60 minutes)
  - CCBS on incoming call:
  - expiration of the BookBusTim timeout; by default, 30 minutes
  - expiration of the public exchange timeout T-CCBS5 (timeout during which the public exchange user must free the line; 60 minutes)

- There is no second call back attempt if the line is busy when the CCBS callback is made. The CCBS request is cancelled; another request can be made.
- A CCBS can be cancelled during the CCBS initiator callback phase.
- CCBS is only available on the ISDN accesses of an Alcatel-Lucent OmniPCX Office Communication Server system; the service is not available on a "slave" system accessing the network by break-out.
- CCBS is not supported by the T0 basic accesses configured in Point-to-Multipoint mode.
- A CCBS callback cannot be intercepted.

3.23.2 Configuration procedure

3.23.2.1 CONFIGURATION

- CCBS on outgoing call: authorize the set to use the service or not:

• by OMC (Expert View):**Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Features** -> **"Callback"**

- CCBS on incoming call: check the following settings:

• by OMC (Expert View):**External Lines -> Incoming Call Handling -> Public Line -> On Busy = Release System Misc. -> Feature Design -> Call Waiting/Automatic Camp-On (not selected)** • by MMC-Station: **IncCal** -> **Public** -> **Busy** -> **ReacPu** -> **Release Global** -> **CalExt** -> **Mode (Ext Call Waiting YES / No)**

- Modify (or not) the timeout during which the CCBS is active in the system (30 minutes by default); at the end of the timeout, the CCBS is cancelled:

• by OMC (Expert View): **System Miscellaneous -> Memory Read/Write -> Timer Labels -> "BookBusTim"** • by MMC-Station: **Global -> Rd/Wr -> Timer -> "BookBusTim" -> Return -> Memory**

- Modify (or not) the timeout during which the party requesting a CCBS on an outgoing call is rung (25 seconds by default); at the end of the timeout the CCBS is cancelled:

• by OMC (Expert View): **System Miscellaneous -> Memory Read/Write -> Timer Labels -> "BookRecTim"** • by MMC-Station: **Global -> Rd/Wr -> Timer -> "BookRecTim" -> Return -> Memory**

3.23.3 Operation

3.23.3.1 CCBS ACTIVATION/CANCELLATION ON OUTGOING CALLS

When a call is made to a public network user B whose line is busy, CCBS enables a user A with an Alcatel-Lucent OmniPCX Office Communication Server system to leave a call back request at the public exchange. When the public exchange informs the Alcatel-Lucent OmniPCX Office Communication Server system that B is free, Alcatel-Lucent OmniPCX Office Communication Server calls back A, and when A answers, it makes an automatic call back to B.

Type of station / Type of service	All stations (including Z)	Without display (# Z)	With display, no soft keys	With soft keys
CCBS request	Automatic call back request code	P.K.: **Automatic callback request**	P.K.: **#Cback**	S.K.: **#Cback**
CCBS cancellation	Cancellation prefix	P.K.: **Cancel callback**	P.K.: **#Cback**	S.K.: #**Cback**, before or during callback

Caution:

Only one automatic call back request can be activated on a set: automatic call back to busy set, automatic call back to busy trunk or CCBS. Any new CCBS request cancels the previous one.

3.23.3.2 CCBS ACTIVATION/CANCELLATION ON INCOMING CALLS

When a public network user (A) calls a busy Alcatel-Lucent OmniPCX Office Communication Server system set (B), A can activate the CCBS service provided by the public exchange. When the Alcatel-Lucent OmniPCX Office Communication Server system informs the public exchange that B is free, the public exchange calls back A, and when A answers it makes an automatic call back to B.

3.24 Fax Call Routing

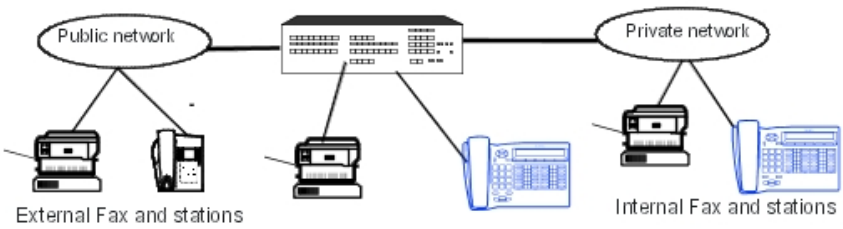
3.24.1 Overview

3.24.1.1 DESCRIPTION

This feature enables Alcatel-Lucent OmniPCX Office Communication Server users to receive voice and fax calls on the same number: their correspondents use a single number for either function. Once configured:

- all voice calls make the set ring;
- all fax calls are routed to the associated fax number. A text message advises the user that a fax has arrived.

Modem type calls are also detected ; these calls are answered by the recipient (modem connected to an analog access) or by an integrated modem if configured in the OS group. The call is refused if no modem is present.



3.24.1.2 ADDITIONAL INFORMATION

- Fax call routing cannot be used simultaneously with CCBS.
- Fax call routing can be used simultaneously with fax notification (see that section): in this case, the user receives 2 messages signaling the receipt of a fax.
- There may be a slight delay between the moment the call reaches the system and the moment it is put through to the station or fax; this is due to the workload on the DSPs in charge of fax detection.

3.24.2 Configuration procedure

3.24.2.1 ACTIVATION/DEACTIVATION

This feature requires that a destination fax number be configured for every user wanting to take advantage of this service; the number is attached to the station's DID number in the public numbering plan.

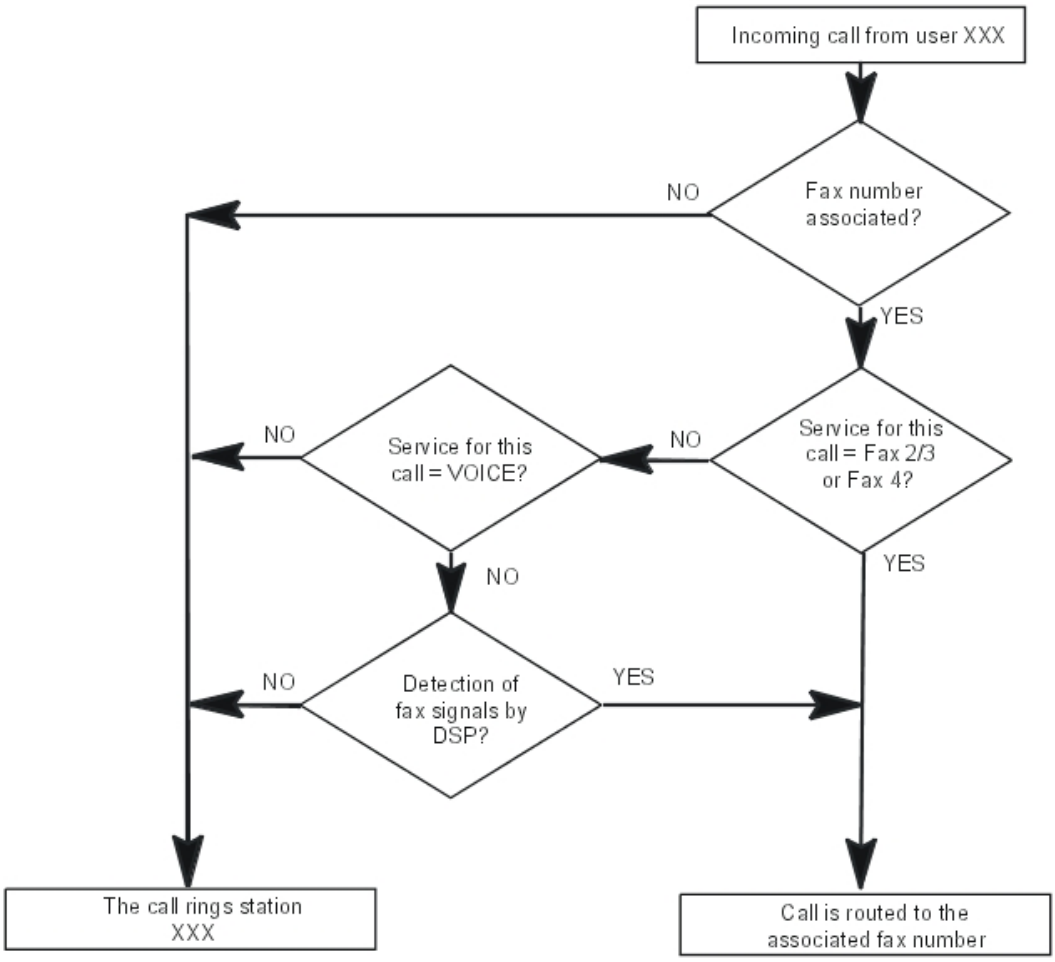
It is controlled by the noteworthy address "FaxCRActiv" (Fax Call Routing Active).

A greeting (general pre-announcement) has to be configured to keep the caller waiting during fax detection.

Handling calls to the Attendant station group

- If the general pre-announcement message is configured, every incoming call is assessed for possible routing.
- There is no need to associate a fax or modem number; fax calls are routed to the first analog interface in the system and modem calls to the integrated modem (default configuration).

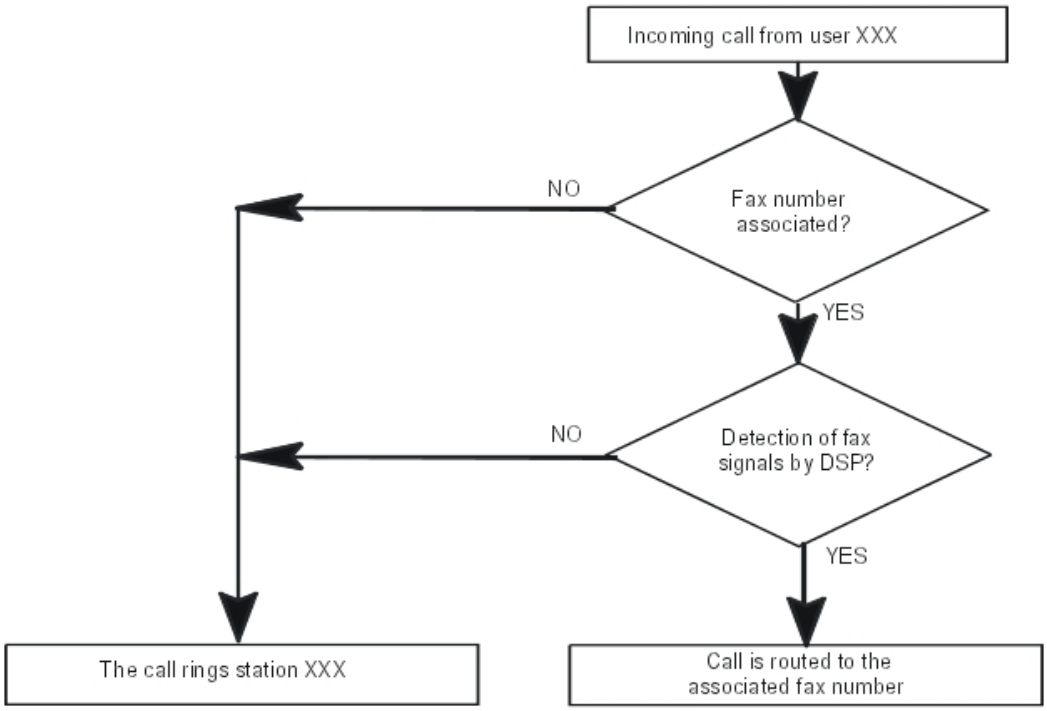
3.24.2.1.1 ISDN CONNECTION



Note:

If the service is not active (no associated fax number), any call with a service other than VOICE will be refused (service incompatibility).

3.24.2.1.2 ANALOGUE CONNECTION



Note:

If the service is not active (no associated fax number), fax calls (with VOICE service) are put through to the user station.

3.24.3 Operation

3.24.3.1 CONFIGURATION

- Enter the destination fax number:

• by OMC (Expert View): **Numbering -> Numbering Plans -> Public Numbering Plan -> Fax** • by MMC-Station: **NumPln -> PubNum** -> **FaxRou**

- Assigning welcome messages:

• by OMC (Expert View): **Users Misc. -> Preannouncement** • by MMC-Station: **PreAnn -> Add -> Msg**

- To define the pre-announcement mode (none, mode 1- before call distribution or mode 2- during call distribution) in accordance with the time range:

• by OMC (Expert View): **Users Misc. -> Preannouncement** • by MMC-Station: **PreAnn -> Add -> Mode**

Note:

It is always the general pre-announcement that is used for fax call routing, even if there is a customised pre-announcement message configured.

Whatever the pre-announcement configuration, the message will be broadcast once, always before call distribution.

The **"Busy"** flag (accessed via OMC -> Users Misc. -> Pre-announcement ->Details) does not apply to fax call routing.

The noteworthy address (Memory read/write - other labels) FaxCRActiv must be set to 01.

3.25 Busy Tone Detection

3.25.1 Overview

3.25.1.1 DESCRIPTION

Offered starting with version R2.0 of the software, the tone detection mechanism allows analogue network line connections to be released without back forwarding of releasing protocol (e.g. polarity inversion). By default, the mechanism is active in all countries.

The tone detection is made by the system's DSP (Digital Signal Processor); it may be enabled line by line (APA or ATA interfaces).

This mechanism is used to allow analogue lines to be joined (external forwarding, external dynamic routing, DISA transit, external transfer) without polarity inversion.

3.25.1.2 ADDITIONAL INFORMATION

- The number of DSPs assigned to tone detection is limited to 6 per module; these resources are shared among the various connected LR interfaces.

3.25.2 Configuration procedure

3.25.2.1 CONFIGURATION

- Enable, line by line, the tone detection mechanism through OMC (Expert View) only:

External lines -> Analogue access -> Details -> Check "? Busy Tone Detection"

- Modify the automatic release's timeout value (or security timeout) of the lines in case of analogue joining (without other release mechanism), through DHM-OMC (Expert View) only:

System Miscellaneous -> Feature Design -> Part 5 -> Automatic Release for Analogue Trunk-to-trunk joining

Values of the security timeout:

- from 1 to 127 hours
- by default: 6 hours
- 0 = no timeout

3.26 Making/Answering a Call

3.26.1 Overview

3.26.1.1 DESCRIPTION

A call can be either:

- internal, or
- external

3.26.1.1.1 MAKING A CALL

Only an internal call can have 3 types of destination:

- a station
- a station in a Hunt Group (attendant or stations)
- all the stations in a Broadcast Group, in the case of a **broadcast call**

To make a call, the user can either choose to pick up first (mandatory if the station does not have a speaker) or not pick up.

Then, depending on the user's station, an internal or external call can be made either by:

- manual dialling:
  - on the numeric keypad, or
  - on the alphabetic keypad (**Dial by name function**: concerns the programmed numbers in the internal directory or the collective speed dial)
- pre-recorded dialling:
  - direct call key
  - repetition of last number/numbers retransmission list (function **Bis**); the last number transmitted by the station is automatically memorised with its corresponding sub-address. This feature is provided for the stations without a display screen regardless of the system's software version, and for the stations with display screen for software versions prior to R2.0. Starting with R2.0, the stations with a display screen may access a list of the last 10 numbers called (internal or external) and thus select from the list, a number to be transmitted.
  - transmission of the number stored in temporary memory; the last number transmitted from a station can be transferred from the "Redial" memory to "**temporary memory**" Starting with R2.0, it is possible to save in temporary memory any incoming or outgoing number (see paragraph “Additional information” for more details)
  - transmission of a **personal speed dial** number; it is possible to save numbers in this directory (see paragraph “Additional information” for more details)
  - call back a number in the **directory of unanswered calls**: this directory contains the unanswered external calls, with or without User to User Signalling (see "ISDN Services") and the internal calls with UUS (see "ISDN Services") automatically memorised by the system
  - for external calls only, transmission of a **collective speed dial** number (including emergency numbers and collective speed dial numbers with speed dial rights = 0; see "Link Classes Of Service" file) created by MMC

- for external calls only, transmission of an **emergency number** - one of 5 factory-preset numbers which cannot be modified by MMC. These numbers are different from those programmed as system speed dial numbers.

When making a call, the user can:

- **protect the call** (in particular data communications) against the camp-on tone and third party intrusion (see "Camp-on on busy station or group" and "Intercom intrusion on free"); these protections are programmable for each station and for all the calls.
- opt not to disclose his identity. The **Calling Line Identification Restriction (CLIR)** service can be set for external calls only, by setting via OMC the "ClirExtOnly" noteworthy address to 1, and by activating the identity secrecy flag on the set.

Auto. call setup on going off hook: this service enables an authorised user to call a correspondent pre-programmed by MMC, simply by going off-hook or pressing the Hands-free key, either immediately or after a timeout. The destination can be:

- an internal user (individual)
- a Hunt Group or Assistant Group
- an external user (by system speed dial number)

Broadcast Call: this service enables a sending user belonging to a Broadcast Group to send a spoken message lasting no more than 20 seconds to the free stations in this group equipped with a speaker. The destination stations are unable to answer this message.

3.26.1.1.2 RECEIVING A CALL

An incoming call is signalled by ringing the station. The ringing rate varies according to whether the call is internal or external. When auto-answer mode is active, the called phone will ring with a specific ringing (same ringing as for auto-answer of local calls): the consequence is that it will no longer be possible to distinguish local calls from external calls when auto-answer mode is active.

A **single-line** station (see "Resource keys") can only receive one call at a time.

The answer mode of the set can be:

- manual: the user can only answer this call by going off hook
- auto-answer or **Intercom** (on a set with the Hands-Free feature): the station "answers" automatically the call after a specific ring tone and goes into hands-free mode (with or without headset). However, for a DECT Reflexes handset, auto-answer will only be active if the intercom mode is enabled (user handset customization) and a headset is plugged in on the handset.
  In case of automatic answer, a ring back tone informs the internal calling party that the answer is an automatic answer. External calling parties are not notified.
  Automatic answer works after a call has been transferred.
  According to configuration, the auto-answer (Intercom) mode applies only to internal calls or both to internal and external calls.

A **multi-line** station (see "Resource keys") can take several calls at once. The answer mode can be:

- manual: the user can select the call he wants to answer or ignore all incoming calls if he wants to make a call
- automatic: the system determines what type of call is at the station (see "Answering camped-on calls")

- auto-answer or **Intercom** (on a set with the Hands-Free feature): the station "answers" automatically the call with the highest priority after a specific ring tone, and goes into hands free mode (with or without headset). However, for a DECT Reflexes handset, auto-answer will only be active if the intercom mode is enabled (user handset customization) and a headset is plugged in on the handset.
  In case of automatic answer, a ring back tone informs the internal calling party that the answer is an automatic answer. External calling parties are not notified.
  Automatic answer works after a call has been transferred.
  According to configuration, the auto-answer (Intercom) mode applies only to internal calls or both to internal and external calls.

Non answered calls can be stored in the memory of the set. This memory is shared with text messages and can store 10 messages (text or non answered call) maximum. The 11th message is lost. The user has to delete useless messages to avoid congestion.

3.26.1.2 ADDITIONAL INFORMATION

- To use the directory of unanswered calls in a parallel group of stations (see "Hunt Groups"), the first station in the group, on creation by MMC, must be a station with a display.
- In "Answering a call: manual connection", an automatic callback or a hold reminder have priority: the user cannot answer another call.
- During group broadcasting, all the stations involved are considered to be busy.
- To stop broadcasting to his own station, a user can go pick up or press the "Release" key.
- A forwarded station receives the broadcast message.
- If all members of the called Broadcast Group are busy, the broadcast call will be unsuccessful.
- The first analog (Z) station is considered as a fax and is therefore protected by default against barge-in and the camp-on tone.
- Specific to Brazil: The **DDC Protection** flag (accessible by Subscribers and Base stations List -> Details -> Service category -> Part 2-> DDC Protection and by External Lines -> External Access Table -> Details -> DDC Protection) makes it possible to reject all incoming calls which the caller tries to charge to the called party (collect call).
- List of retransmitted numbers (R2.0): a retransmission list can include a maximum of 10 internal or external numbers; this limit may be reduced depending on the keys" and directories" key pool use.
  If a call arrives while the retransmission list is in use, the call is switched to standby.
- Temporary save of a number (R2.0): a number may be saved in the temporary memory under the following conditions:
  - when a call is in progress
  - during a call phase
  - during review of the standby calls
  - during review of the unanswered calls directory (text mail)
  - during use of the retransmitted numbers list

  A saved incoming external number in temporary memory cannot be directly retransmitted; the seizure number of the trunk group used for the call must be dialled first.
  Group call: as long as there is no answer, the group call is saved; after answering, the number of the answering Station is saved.

If an incoming call arrives while saving a number (temporary memory or individual directory), this call will be released (as during customisation).

- Saving a number in the individual directory (R2.0): a number may be saved in the individual directory under the following conditions:
  - when a call is in progress
  - during review of the unanswered calls directory (text mail)
  - during use of the retransmitted numbers list
- As of R7.1, the user can choose to display the calling party name or the calling party number. During ringing or conversation, a press on the **i** key switches between the two display modes.
  The initial display is based on the parameter: **Name Display**. If this parameter is enabled, the initial display is the calling party name.

  Note:
  This feature works only if the calling party name is available.
  This feature is available only for the following sets:
  - Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone, Alcatel-Lucent IP Touch 4068 Phone
  - Alcatel-Lucent 4029 Digital Phone, Alcatel-Lucent 4039 Digital Phone, Advanced Reflexes
  - Alcatel-Lucent 300 DECT Handset, Alcatel-Lucent 400 DECT Handset, Alcatel Mobile Reflexes 100and Alcatel Mobile Reflexes 200. On these sets, a long press on the phone book key is used to switch between name and number display.

3.26.2 Configuration procedure

3.26.2.1 CONFIGURATION

- To specify whether or not to authorize the "Automatic call setup on going off hook" feature for each station:

• by OMC (Expert View):**Users/Base stations List** -> **Users/Base stations List** -> **Details** -> **Misc.** -> **Hotline** • by MMC-Station: **User or Subscr** -> **AutoCa** -> **Active**

- To validate the "Automatic answer for external call" feature for all sets in automatic answer mode.

• by OMC (Expert View):**System Miscellaneous -> Feature Design -> Part 2-> "Automatic answer for external call"** ->

- If the "Automatic call setup on going off hook" feature is authorized, define whether the call is immediate or after a time-out and define the call destination for each station:

• by OMC (Expert View):**Users/Base stations List** -> **Users/Base stations List** -> **Details** -> **Misc.** -> **Hotline** • by MMC-Station: **User or Subscr** -> **AutoCa** -> **Temp**

- To modify the default time-out for the "delayed" automatic call setup on going off hook - OMC (Expert View) only:

System Miscellaneous -> Feature Design -> Part 3 -> "Timer for delayed off-hook Automatic Call" (hotline)"

- To create the personal speed dial numbers for each station:

- by OMC (Expert View): **Users/Base stations List -> Users/Base stations List -> Details -> Pers. SPD**.
- by MMC-Station: **User or Subscr -> Pers. SPD**.
- by customization: **Pers. SPD**

- To create the system speed dial numbers:

- by OMC (Expert View):**Common Speed Dial**
- by MMC-Station: **ComSpd**

- To create the internal directory:

- by OMC (Expert View): **Directory**
- by MMC-Station: **Global** -> **Name**

- For each station, all calls can be protected against barge-in and the camp-on tone:

- by OMC (Expert View):**Users/Base stations List** -> **Users/Base stations List** -> **Details** -> **Features** -> **"Barge-in Protection"** and **"Warn tone Protection"**

- For each station, the caller's identity can be restricted for all calls:

- by OMC (Expert View):**Users/Base stations List** -> **Users/Base stations List** -> **Details** -> **Features** -> **"Identity Secrecy"**

- To create the Broadcast Groups:

- by OMC (Expert View): **Broadcast groups**
- by MMC-Station: **Group** -> **Broadcast**

- Broadcast on external speaker:
  This feature is not controlled by a software key. To realize this feature, the system must be fitted with an AFU daughterboard on the CPU/CPUe board (the hardware can be checked via OMC menu -> Main CPU -> Details -> Daughterboards):
  - In the **Broadcast Groups** menu, select one group and press **Details**.
  - Press **Add** to add members into the group. If the system is equipped with an AFU daughterboard, then **Speaker user** will appear in the list.
  - Add **Speaker user** with attribute **Receive** or **Send/Receive** and all other users allowed to make/receive the broadcast message.
- To modify the default time-out for the delayed automatic answer in headset mode - OMC (Expert View) only:

System Miscellaneous -> Feature Design -> Part 4 -> "Time before auto. conn. in headset mode"

- To modify the default time-out for the delayed automatic answer without a headset - OMC (Expert View) only:

System Miscellaneous -> Feature Design -> Part 4 -> "Time before connection without headset"

- Define whether the Redial feature (retransmission of the last number/list of retransmitted numbers) relates to all the called numbers or only to the external numbers, via OMC (Expert View) only:

System Miscellaneous -> Feature Design -> ? External redial only

- To display the calling party name (if available) initially:

User/Base station list-> Details -> Feature right [Part 1] -> Name Display

Note:
If not validated, the calling party number is displayed.

3.26.3 Operation

3.26.3.1 ACTIVATION/USE

P.K.:: Programmed Key - defined by OMC (Expert View) or MMC-Station

F.K. : Fixed Key

S.K.:: Soft Key

Prefix:Code programmed in the internal numbering plan

3.26.3.1.1 ACTIVATING THE SERVICES

Type of station / Type of service	**Z**	**Without display (# Z) and without** Hands-Free feature	**Without display (# Z) and with Hands-Free feature**	**4011**	**With display, no soft keys, except 4011**	**With soft keys**
Intercom mode	--	--	P.K.: **AutAns**	--	F.K.: **Intercom**, or P.K.: **AutAns**	F.K.: **Auto-answer mode (intercom mode)**
Communication protection	Access	F.K.: **Data** or P.K.: **ProCom**				
Identification restriction	--	P.K.: **CLIR**				F.K.: **ISDN** + S.K.: **CLIR**
Transfer to temporary memory	--	P.K.: **Temporary number**				S.K.: **NbSave**
Storage in an individual directory	--	F.K. **i** + selection **->Rep** + index 0 to 9 + label				S.K.: **->Rep** + S.K. associated to number + label

3.26.3.1.2 ANSWERING A CALL

	**Z**	**Without display (# Z) and without Hands-Free feature**	**Without display (# Z) and with Hands-Free feature**	**4011**	**With display, no soft keys, except 4011**	**With soft keys**
In manual mode	--	Press the resource key				
In automatic mode	Go off hook	Go off hook	Off hook or press F.K.: **Handsfree**	Go off hook	Off hook or press F.K.: **Handsfree**	
In intercom mode	--		Automatic connection	--	Automatic connection	

3.26.3.1.3 MAKING A CALL

	**Z**	**Without display (# Z)**	**DECT**	**With display, no soft keys**	**With soft keys**
Auto. call setup on going off hook	**Go off hook**	**Go off-hook or press F.K. Hands-free**	**Go off hook**	**Go off-hook or press F.K. Hands-free**	
Dial by name	--	--	F.K.: **Dial by name**, then enter name, then F.K.: **Valid**	P.K.: **Dirtry**, then enter name, then F.K.: **LS** or **Mute** to confirm	Enter the name, then "Return"
Bis (only one number)	Access	F.K. or P.K.: **Redial**	F.K.: **Redial**		S.K.: **Redial**
Bis (list of numbers)	--	--	F.K. or P.K. **Bis** + selection + F.K. **Valid**		S.K.: **Bis** + selection + S.K. **Redial**
Temporary memory	--	P.K.: **Personal speed dial** + P.K.: **Temporary number**	F.K.: **Personal speed dial** + P.K.: **TmpRep**		S.K.: **NbSend**
Personal speed dial	--	P.K.: **Personal speed dial** + index 0 to 9	F.K.: **Personal speed dial** + index 0 to 9		F.K.: **Personal speed dial** + S.K. associated with number

Type of station / Type of service	Z	Without display (# Z)	DECT	With display, no soft keys	With soft keys
Non answered calls repertory	--		F.K.: **Mail** + 2 + F.K.: **Valid**	F.K.: **Mail** or P.K.: **TxtMsg** + 2 + F.K.: **LS**	F.K.: **Mail** + S.K.: **Text** + S.K.: **Read** + S.K.: **Call**
Collective speed dial numbers (including emergency numbers)	Access				
Emergency numbers not belonging to the common speed dial numbers	Dial the emergency number				
Broadcast call	Broadcast Group number	P.K.: **Direct call**			

3.27 Camp-on Busy Station or Group

3.27.1 Overview

3.27.1.1 DESCRIPTION

A user is automatically camped-on on a station he is calling when the following conditions are met:

- it is busy (in conversation with a party)
- it has at least one resource free (see "Resource keys" file)
- it is not protected against camp-on
- the caller is authorized to camp-on

A user is automatically camped-on a Hunt Group which he is calling when the following conditions are met:

- all the stations in the group are busy, i.e. in conversation with a party
- at least one of the stations in the group has a free resource (see "Resource keys" file)
- the stations in the group are not protected against camp-on
- the caller is authorized to camp-on

A camped-on caller can:

- Release the call, possibly leaving a text message (see "Text mail/Callback request")
- leave an **automatic callback request** with the called party, if the station supports
- **intrusion** into the existing conversation, if the caller is authorized and if the station is not protected against intrusion
- transfer his PARTY if on-hold (see "Conference")

3.27.1.2 ADDITIONAL INFORMATION

- When camp-on is allowed and the called party is not protected against the camp-on tone, the camped caller hears the camp-on tone and the called party hears a single beep every 20 seconds.
- If the automatic callback request is accepted, the user hears the dial tone if he is off hook and switches to the idle status in hands-free mode.
- An authorized station can only request a single automatic callback at a time.
- A station can only receive a single automatic callback request at a time.
- A callback request does not follow a call forwarding.
- The identity of the barging in station is displayed on the stations which are already in conversation.
- Barge-in is refused (the user then remains camped-on) if:
  - the called party is in a conference call
  - the called party is barging in on another conversation
  - at least one of the stations is protected against barge-in
- An attendant station always has the authority to camp on and to barge-in.
- When the user is barging in while having a party on hold, he returns to this party by canceling the barge-in and disconnecting going on hook and returning to the call on hold.
- The first analog (Z) station is considered as a fax and is therefore protected by default against barge-in and the camp-on tone.

3.27.2 Configuration procedure

3.27.2.1 CONFIGURATION

- To specify whether or not to protect a station against camp-on:

• by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Features** -> **"Camp-On Protection"**

- To specify whether or not to protect a station against the camp-on tone:

• by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Features** -> **"Warntone Protection"**

- To specify whether or not to authorize camp-on for a station:

• by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Features** -> **"Camp-On Allowed"**

- To specify whether or not to protect a station against intrusion:

• by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Features** -> **"Intrusion Protection"**

- To specify whether or not to authorize intrusion for a station:

- by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Features** -> **"Intrusion Allowed"**

- To specify whether or not to authorize a station to leave an automatic call back request:

- by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Features** -> **"Callback"**

3.27.3 Operation

3.27.3.1 ACTIVATION/USE

P.K.: Programmed Key – defined by OMC (Expert View) or MMC-Station

F.K.: Fixed Key

S.K.: Soft Key

Code: Code programmed in the "Features in Conversation" table

Type of station / Type of service	**All stations including Z**	**Without display (# Z)**	**With display, no soft keys**	**With soft keys**
Automatic call back request (*)	Function code	P.K.: **Automatic callback request**	P.K.: **#Cback**	S.K.: **#Cback**
Intrusion	Function code	P.K.: **Intrusion**	P.K.: **Intru**	S.K.: **#Intru**

(*) When the called party becomes free, the station which requested call back is rung. If it goes off hook, the called party station rings in turn.

3.27.3.2 CANCELLATION

Prefix: Code programmed in the internal numbering plan

Type of station / Type of service	**All stations including Z**	**Without display (# Z)**	**With display, no soft keys**	**With soft keys**
Automatic call back (**)	Prefix	P.K.: **Cancel callback**	P.K.: **#Cback**	S.K.: #**Cback**, before or during callback
Intrusion	Activation code	P.K.: **Intrusion**	P.K.: **Intru**	S.K.: **#Intru**

(**) The automatic call back request is also cancelled if:

- the person requesting call back does not go off hook within 15 seconds or presses the "Release" key during these 15 seconds
- the called station does not release within 30 minutes.

3.28 Answering Camped-on Calls

3.28.1 Overview

3.28.1.1 DESCRIPTION

When one or more callers (if the station has the necessary resources) are camped on a subscriber (see "Camp-on on busy station or group"), the subscriber can either:

- **consult the identity of the camped callers**, if the station has soft keys
- answer (consult) one or more camped-on calls, without releasing the current communication, or
- answer a camped-on call by releasing its current communication. In this case, the system determines which camped-on call is presented to the station according to the priority of the calls camped-on.

The level of priority depends on three criteria:

- the type of caller: internal, external or OS (for example, if a station has a caller camped on but has no resources left, an OS call "breaks" the first camp-on and is itself camped on)
- the type of called party: Operator Group, Hunting Group or station
- the type of call: simple call, recall (for example after transfer failure, see "Conference") or hold reminder

The system allocates the following descending order of priority:

- external hold recall, delayed or otherwise
- internal hold recall, delayed or otherwise
- external callback
- external call
- internal callback
- call from an operator station
- internal call
- Operator Group call
- Hunting Group call

3.28.1.2 ADDITIONAL INFORMATION

- A station which has activated paging or which is in a conference call (see "Conference") or intrusion (see "Camp-on on busy station or group"), cannot answer a camped-on call.
- When consulting the identity of the camped-on callers, a station with soft keys can also consult the User to User Signaling (UUS) of the caller (see "ISDN Services").

3.28.2 Configuration procedure

3.28.2.1 CONFIGURATION

- To specify whether or not to protect a station against camp-on:

• by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Features** -> **"Camp-On Protection"**

- To specify whether or not to protect a station against the camp-on tone:

- by OMC (Expert View):**Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Features** -> **"Warntone Protection"**

- To specify whether or not to authorize camp-on for a station:

- by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Features** -> **"Camp-On Allowed"**

3.28.3 Operation

3.28.3.1 ACTIVATION/USE

S.K.: Soft Key

Code: Code programmed in the "Features in Conversation" table

Type of station / Type of service	**All stations including Z**	**Without display (# Z)**	**With display, no soft keys**	**With soft keys**
Consultation of camped-on caller identities	--			S.K.: **Queue**
Answer after consultation of identity (*)	--			S.K.: **Answer**(**)
Answer a camped-on call (*)	Function code	Resource key		

(*) "Manual" answering of a camped-on caller entails exclusive hold (see "Three-party calls" file) of the current communication.

(**) When the identity of the caller to be consulted is displayed.

3.28.3.2 CANCELLATION

Type of station / Type of service	**All stations including Z**	**Without display (# Z)**	**With display, no soft keys**	**With soft keys**
Return to initial correspondent after consulting a camped-on caller	Enquiry or shuttle call cancellation code(*)	Resource key of correspondent on hold		

(*) In the first case, the caller is released and in the second, placed on exclusive hold.

3.29 Three Party Calls

3.29.1 Overview

The operating mode, Europe or US, cannot be configured with MMC-station or OMC. This mode is globally specified for the system when configured in the factory.

3.29.1.1 DESCRIPTION

3-party calls are:

- call consultation (enquiry), prior to the following:
- broker
- conference
- transfer

3.29.1.1.1 Consultation (Enquiry)/Hold

A station involved in an internal or external conversation can make a new internal or external call using either:

- one of the means described in "Making/Answering a call"
- or by answering a camped-on call (see "Camp-on on busy station or group")
- or by picking up a call intended for another station (see "Call PickUp" and "Call Parking/Parked Call Retrieval")

The current party is automatically placed on hold by the system. This type of **hold** is said to be "**exclusive**" because only the user who activated it can retrieve the party.

A user can place a party on exclusive hold when:

- he is in conversation with the party
- he has called the party and hears the ringing tone
- he has called the party and hears the camped-on tone

"Manual" call holding is also possible. In this case, it is said to be "**common**" because all the users supervising the resource on hold can retrieve the party (RSP resource only).

A user can only place a party with whom he is in conversation on common hold.

Hold recall: When a user goes on hook with a party on hold, the system recalls the user. This can be either immediate (overlooked hold) or time-delayed. When the hold recall is time-delayed, the user can make an outgoing call or answer an incoming call: the hold recall will take place at the end of the timeout or at the end of the new call.

3.29.1.1.2 Broker

This service enables the user to speak alternately with a party on line and a party on hold.

3.29.1.1.3 Conference

This service enables an authorized user on a consultation call to set up a call with two parties simultaneously.

3.29.1.1.4 Transfer

This service enables a call to be setup between the party on hold and the party on line. This latter was not necessarily in conversation with the user. Transfer can take place either:

- after conversation with the second party

- when the user hears the ringing tone (the second party has not answered)
- when the user is camped-on on the second party's station
- when the user has activated paging for this second party (who has not answered)
- during the routing phase of the second call, after dialing an **external** number

3.29.1.2 ADDITIONAL INFORMATION

- A party on hold hears music-on-hold if external and the hold tone if internal.
- It is impossible to place on hold:
  - a network call in the routing phase
  - a broadcast call
  - a barge-in call
  - a paging call
- At hold recall, the user's station rings and if he does not answer before the expiration of the hold recall time-out:
  - the call is returned to the general level if external
  - the call is released if internal
- A broker call is refused when the user has barged into a conversation, or is involved in a conference or paging call
- A user cannot put another caller on exclusive hold when he hears the ringing or camp-on tone, only to return to the first correspondent on hold
- If one of the stations involved in a conference goes on hook and is not the initiator of this conference, the remaining two parties stay in communication
- The system allows 3 simultaneous conferences. The DSP resources for conferences are shared with the VMU feature "recording of conversation"
- The services attributed to the stations must be of the "telephone" type, otherwise holding may be refused
- US special feature: the first time the **Transfer** or **Conference** key is pressed, this is followed by an acknowledge tone then the dial tone (stutter dial tone); the 2nd time the **Transfer** key is pressed, this is followed by an accept or reject tone (depending on the case); the second time the **Conference** key is pressed this is followed by a unique beep (1400 Hz - 1.5 seconds)

3.29.2 Configuration procedure

3.29.2.1 CONFIGURATION

- Choose between immediate or delayed hold recall:

• by OMC (Expert View): **System Miscellaneous** -> **Memory Read/Write** -> **Misc. Labels** -> **"TimedHldEn"**
• by MMC-Station: **Global -> Rd/Wr -> Address -> "TimedHldEn" -> Return -> Memory**

- To modify the implicit value of the delayed hold recall time-out:

- by OMC (Expert View): **System Miscellaneous** -> **Feature Design** -> **Part 3** -> **Duration of Hold Recall Ringing**
- by MMC-Station: **Global -> Rd/Wr -> Timeout -> " OnHoldTim" -> Return -> Memory**

- For the system, specify whether or not the conference is authorized in the system and if it is, the type of conference authorized:

- by OMC (Expert View): **System Miscellaneous** -> **Feature Design** -> **Part 2**-> **Conference (prohibited, internal only or Ext & Int)**
- by MMC-Station: **Global** -> **Confer**

- To specify whether or not each station is authorized to take conference calls (by default , all stations have this facility):

- by OMC (Expert View): **Subscribers/Base stations List** -> **Subscribers/Base stations List** -> **Details** -> **Features** -> **Conference**

- For the system as a whole, to authorize or inhibit the transfer of incoming or outgoing trunk lines to an outgoing network line (be careful with subscriber rights and trunk group link categories):

- by OMC (Expert View): **System Miscellaneous** -> **Feature Design** -> **"Transfer Ext/Ext"**
- by MMC-Station: **Global** -> **Joing.** -> **Transf**

- To authorize transfer of an incoming or outgoing network line to an outgoing network line, for each station:

- by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Features** -> **Part2** -> **"Join incoming and Outgoing"** and **"Join Outgoing and Outgoing"**

- To define the type of system reaction in the event of transfer failure (operator or initiator recall, also called "transfer master"):

- by OMC (Expert View): **System Miscellaneous** -> **Feature Design** -> **"Go to initiator if transfer fails"**
- by MMC-Station: **Global** -> **MasRec** -> **Choice**

- Modify the implicit value of the rerouting time-out at general level in the event of transfer failure:

- by OMC: **System Miscellaneous** -> **Memory Read/Write** -> **Timer Labels** -> **"TransfeTim"**
- by MMC-Station: **Global -> Rd/Wr -> Timeout -> " TransfeTim" -> Return -> Memory**

- Authorize connection of two external lines by transfer (connection matrix):

Traffic Sharing and Barring -> Joining

- To specify whether or not to authorize transfer by going on-hook with a multiline station:

- by OMC (Expert View): **System Miscellaneous** -> **Feature Design** -> **Transfer by on hook**

- To specify whether or not to authorize Ext/Ext transfer (intersite transfers) by going on-hook with a Z station:

- by OMC (Expert View): **System Miscellaneous** -> **Feature Design** -> **Transfer Ext/ext by on hook**

3.29.3 Operation

3.29.3.1 ACTIVATION/USE

Note:
*The dedicated sets with US profile (see also "Resources keys") feature fixed keys (pre-programmed) **Man. hold**, **Transfer** and **Conference**; the stations with dynamic keys provide dynamically the same keys depending on the context.*

P.K.: Programmed Key - defined by OMC (Expert View) or MMC-Station

F.K.: Fixed Key

S.K.: Soft Key

Code: Code programmed in the "Features in Conversation" table

Type of station / Type of service	**Analog (Z)**	**Single-line Analog (Z)**	**Without display and multi-line**	**With display, no soft keys**	**With soft keys**
Consultation call (enquiry) (Europe)	F.K.: **R** + call	Call			
Consultation call (enquiry) (US)	F.K. **Flash** + call	F.K. **Man. hold** + call			
Exclusive hold (Europe)	Automatic on consultation, broker or reply to a camped-on call				
Common hold (Europe)	--	--	P.K.: **Hold**		S.K.: **Hold**
Common hold (US)	F.K. **Flash**	F.K. **Man. hold**			
Broker (Europe)	Feature code		Resource key		
Broker (US)	Feature code	P.K.: **Conference**	F.K. or P.K.: **Conference**		S.K.: **Conf**
Conference (US)	F.K. **Flash** + 2nd party call + F.K. **Flash** + feature code	F.K. **Conference** + 2nd party call + F.K. **Conference**	F.K. **Conference** + 2nd party call or resource key + F.K. **Transfer**		
Transfer (Europe)	On hook		F.K.: **Transfer**		S.K.: **Transf**
Transfer (US)	On hook	F.K. **Transfer** + 2nd party call + F.K. **Transfer**	F.K. **Transfer** + Recipient resource key + F.K. **Transfer**		

3.29.3.2 CANCELLATION

P.K.: Programmed Key - defined by OMC (Expert View) or MMC-Station

F.K.: Fixed Key

S.K.: Soft Key

Code: Code programmed in the "Features in Conversation" table

Type of station / Type of service	**Analog (Z)**	**Single-line**	**Without display and multi-line**	**With display, no soft keys**	**With soft keys**
Consultation call (enquiry), Broker (Europe)	F.K.: **R** + Code **Cancel enquiry**	Code: **Cancel enquiry**	F.K.: **End** + resource key of initiator		
Common Hold Retrieval or Voice Transfer (Europe)	--	--	Resource key		
Retrieving common hold (US)	F.K. **Flash**	F.K. **Man. hold**	Resource key		
Conference, with return to conversation preceding the conference (Europe and US)	Feature code	P.K.: **Conference**	F.K. or P.K.: **Conference**		S.K.: **Conf**
Conference, with release of both parties (Europe and US)	--	On hook			

3.30 Intercom Intrusion

3.30.1 Overview

3.30.1.1 DESCRIPTION

When an internal user calls another internal user who does not answer, he can force the destination station to switch to hands free mode, if it supports this function.

The intercom call ringing tune rings the destination station for a programmed length of time and the latter switches automatically to hands free mode.

Note:

For the activation of the "Intercom" function, see "Making/Answering a Call".

3.30.1.2 ADDITIONAL INFORMATION

- The "Intercom Intrusion on Free" or "Forced" programmed key can be replaced by a macro programmed key "Macro1 = direct call of an internal number + intercom intrusion on free on the called station".
- The right to intercom intrusion is the same as that for intrusion (see "Camp-on on busy station or group").

3.30.2 Configuration procedure

3.30.2.1 CONFIGURATION

- To specify whether or not to protect a station against intercom intrusion on free:

- by OMC (Expert View): **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Features -> "Intrusion Protection"**

- To specify whether or not to authorize a station to activate intercom intrusion:

- by OMC (Expert View): **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Features -> "Intrusion Allowed"**

- To modify the duration for the intercom call ringer:

- by OMC **System Miscellaneous -> Memory Read/Write -> Timer Labels -> "AutoAnsTim"**
- by MMC-Station: **Global -> Rd/Wr -> Timer -> "AutoAnsTim" -> Return -> Memory**

3.30.3 Operation

3.30.3.1 ACTIVATION/USE

P.K.: Programmed Key – defined by OMC (Expert View) or MMC-Station

S.K.: Soft Key

Type of station	Z	Without display and multiline	With display, no soft keys	With soft keys
Activation of intercom intrusion on free when the user hears the ringing tone	--	P.K.: **Intercom intrusion on free**	P.K.: **Forced**	S.K.: **#Intru**

3.31 Call Forwarding

3.31.1 Overview

3.31.1.1 DESCRIPTION

Forwarding enables personal (individual) or group calls to be re-routed immediately. The type of calls, internal and/or external, affected by the active forwardings can be selected by configuration.

- **Follow-me**: forwarding is activated from the destination station
- **Do Not Disturb**: the user refuses all calls: internal calls are released and external calls are transferred to the attendant station
- **Immediate group call forwarding**: calls sent to all groups linked to the user are transferred to another programmed destination number (in advance or on activation of the service)
- **Immediate call forwarding**: individual calls are routed to another destination (whether set, group or VMU) programmed in advance or on activation of the service)
- **Forward to text answering**: internal calls are released after display of a text message and external calls are routed to the attendant station

- **selective forwarding**: depending on the callers' identification (call number), the calls may or may not be routed to a pre-programmed destination
- **Forward to pager**: calls are routed to the called party's pager
- **Forward on busy**: when the station is busy, calls are routed to another destination (programmed in advance or on activation of the service)
- **Withdraw from group**: the user refuses calls intended for one or more Hunting Groups or Operator Groups to which he belongs

Type of forwarding	Incoming call type	Initial destination	Personal or group forwarding	Final destination	Feature rights
Follow-me	Internal/external	Set	Personal	Internal station	-
Do Not Disturb	Internal	Set	Personal	-	-
	External			Attendant station	
Immediate	Internal	Set	Personal	Int. or ext. station or group	-
		GrpPic	Group	Internal station	
	External	Set	Personal	Int. or ext. station (*) (*) station or group	Yes for external forwarding
		GrpPic	Group	Internal station	
Text answering	Internal	Set	Personal	-	-
	External			Attendant station	
Selective	Internal	Set	Personal	Int. or ext. station (*) (*)	Yes
	External				
Paging	Internal/external	Set	Personal	Paging "Bleep"	-
Forwarding on busy	Internal/external	Set	Personal	Internal or external station or group	Yes
Unavailable (Withdraw from group)	Internal/external	GrpPic	Group	-	-

(*) External forwarding requires a particular configuration detailed in the "External Forwarding" file.

Note 1:
Alcatel-Lucent OmniPCX Office Communication Server also offers the facility to transfer a call to the voice mailbox of a third party. However, this is not an automatic transfer of an incoming call, but a manual transfer of an already answered call. For more details, see "Transferring to Voice Mail of Third Party".

Note 2:
The Alcatel-Lucent OmniPCX Office Communication Server Release 7.0 also offers the facility to activate/deactivate immediate call forwarding via the remote configuration. For more details, see module Remote configuration - Detailed description .

3.31.1.2 ADDITIONAL INFORMATION

- Only one active individual forwarding is authorised per station: (activation of an individual forwarding cancels and replaces the previous one)
- A station can simultaneously activate several forwardings: station forwarding + immediate group forwarding + selective forwarding + as many group withdraws (unavailable) as is desired
- Authorisation to forward the last station of a group can be programmed (see "Configuration")
- The "Follow-me" service can be cancelled from the destination station or the forwarded station
- The "Unavailable (Withdraw from group)" service is not available on S0 stations.
- A "Master forwarding" or "Selective forwarding" key (M. Immd", M. Busy", M. Grp") makes it possible to activate or cancel the corresponding forwarding. Furthermore, the icon or LED associated with this key, indicates when a forwarding is activated. All the preprogrammed or fixed keys are such keys
- The same station may have a "personal call forwarding" Master key and a "Group call forwarding" Master key
- A "text answering" forwarding can only be activated on a station with a display
- The "internal" type of calls to be forwarded includes internal calls as well as those coming from the private network
- Forward to text answering: when a network call from a station without UUS capability (a Z station for example) arrives at a station that has activated forwarding to text answering, the call is forwarded to the attendant station, which also receives the text message from the called station
- Prefixes for the forwarding functions in the numbering plans. The basic value may differ according to the local version of the software; the following values apply in France:
  - Forwarding: base 0 = cancel forwarding
  - Forwarding: base 1 = immediate forwarding
  - Forwarding: base 2 = forwarding on busy
  - Forwarding: base 3 = do not disturb
  - Forwarding: base 4 = forward to pager
  - Forwarding: base 5 = group call forwarding
  - Forwarding: base 6 = disconnect from group
  - Forwarding: base 7 = rejoin group
  - Forwarding: base 8 = follow-me
  - Forwarding: base 9 = cancel follow-me
  - Forwarding: base 10 = selective forwarding
- Cascade forwarding (available from version R2.0): a call may be subject to a maximum of 5 individual forwardings (default: 5; configurable by OMC):
  - In case of external forwarding (of a local call, of an incoming call by joining or by re-routing), the cascade may use public or private, analogue or digital lines
  - The cascade stops as soon as the authorised number is reached (thus avoiding loops)
  - The cascade stops when it comes to a user in forwarding:
    - Do Not Disturb
    - Text answering

  - Follow-me
  - On the person search device
  - Dynamic routing (except if routing is to an external destination)
- Screening: if the last forwarding authorised by the cascade number configuration concerns a user in the process of screening, this additional forwarding is accepted
- Group call forwarding: if the recipient of group call forwarding is himself forwarded, this forwarding will not be processed
- Forwarding on busy: the forwarding is processed even if the user is grade 2 busy (2 established calls)
- Forwarding on the person search device: this forwarding is processed even if it means exceeding the authorised number of cascades

- US special features: a “Do not disturb” forwarding is managed as an immediate forwarding on the voice server

3.31.2 Configuration procedure

3.31.2.1 CONFIGURATION

- For each station, select the type of calls (internal, external or both) to be forwarded:

• by OMC (Expert View): **Users/Base stations List -> Details -> Fwd. Rout -> Diversion Apply** • by MMC-Station: **User -> DynRou -> Ext or Inter**

- For each station, program the caller lists for selective forwarding (CLIP diversion) and the internal or external destination for each list. Lists can be unused, active (until deactivated by the station), inactive (until validated by the station), validated (programmed but not usable), negative or otherwise (a negative list is one where forwarding is activated by users other than those on the caller list):

by OMC (Expert View): **Users/Base stations List -> Details -> Fwd. Sel**

- To specify whether or not to authorize forwarding of the last member of a group:

by OMC (Expert View) only: **Common Data -> Feature Design -> Part 1 -> Disconnect last Group Member allowed**

- For each station, external forwarding can be authorized:

by OMC (Expert View) only: **Users/Base stations List -> Details -> Features -> External forwarding**

- Specify the number of cascading call forwardings (5 max., 5 by default):

by OMC (Expert View) only: **Common Data -> Feature Design -> Part 5 -> Maximum Number of Call Forwarding Cascading Levels**

- Specify whether or not to authorize a new cascade in case of external forwarding:

by OMC (Expert View) only: **Common Data -> Feature Design -> Part 2 -> Cascaded External Diversion**

In case of prohibition and if an external forwarding is detected:

- If it is the first forwarding, it is processed.

- Otherwise, forwarding is refused and the current user is warned by a ring (i.e. the user who activated the external forwarding).

3.31.3 Operation

3.31.3.1 ACTIVATION/USE

P.K.:: Programmed Key

F.K.:: Fixed Key

S.K.:: Soft Key

Prefix:Code programmed in the internal numbering plan

Type of forwarding	**All stations including Z**	**Without display (# Z)**	**With display, no soft keys**	**With soft keys**
Follow-me	Prefix + station no. to be forwarded	P.K.: **Follow Me**+ no. of station to be forwarded	P.K.: **Follo**+ n# of station to be forwarded	S.K.: **Forward** + **Follo->** + no. of station to be forwarded
Do Not Disturb	Prefix	P.K.: **Do Not Disturb**	P.K.: **DND**	S.K.: **Divert** + **DND**
Immediate forwarding of personal calls	Prefix + Destination no.	F.K.: **Divert** or (pre-)programmed **(Master) indiv. immediate forwarding** + Destination no.	F.K.: **Forward** or (pre-)programmed **M ImmD-> or Immed->** (indiv.) + Destination no.	S.K.: **Forward** + **Immed->** + Destination n#
Forward to text answering	--	--	P.K.: **Text->**	S.K.: **Forward** + **Text->**
Forward to pager	Prefix	P.K.: **Paging**	P.K.: **Page->**	S.K.: **Forward** + **Page->**
Forward on busy	Prefix + Destination no.	P.K.: **Forward on busy (master)** + Destination no.	P.K.: **M busy-> or Busy->** + Destination n#	S.K.: **Forward** + **Busy->** + Destination n#
Immediate forwarding of group callst	Prefix + Destination no.	P.K.: **(Master) Immediate call forwarding** (group) + Destination no.	P.K.: **M Grp-> or Immed->** (group) + Destination n#	
Withdraw from group	Prefix + no. of group to quit	P.K.: **Withdraw from group** + number of the group to quit	P.K.: **GrpWd** + number of the group to quit	
Selective forwarding	Prefix	P.K.: **Selective forwarding**	P.K.: **SelFwd**	

3.31.3.2 cancellation

P.K.:: Programmed Key

F.K.:: Fixed Key

S.K.:: Soft Key

Prefix:Code programmed in the internal numbering plan

Type of forwarding	**All stations including Z**	**Without display (# Z)**	**With display, no soft keys**	**With soft keys**
All, except "withdraw from group"	Prefix **Cancel all forwardings**	P.K.: **Cancel all forwardings**	P.K.: **All**	S.K.: **Forward** + **Cancl-> + type of forwarding**
Follow-me (from the destination station)	Prefix **Cancel follow-me** + no. of forwarded station	Prefix **Cancel follow-me** + no. of forwarded station	Prefix **Cancel follow-me** + no. of forwarded station	S.K.: **Forward** + **Cancl-> + Follo->** + no. of station to be forwarded
Rejoin the group	Prefix + no. of group to rejoin	P.K.: **Withdraw from group** + number of group withdrawn from	P.K.: **GrpWd** + number of group withdrawn from	

3.32 Automatic Call Back on Busy Trunk Group

3.32.1 Overview

3.32.1.1 DESCRIPTION

When a user makes a network call (public or private) by:

- using an external RSD or RSB resource key (see "Resource Keys")
- dialing a trunk group number
- using the "Dial by Name" feature
- pressing a direct call key
- using the personal and collective speed dial numbers
- using the "Redial" and "Temporary Memory" features

and hears the busy tone for the selected trunk group, he can leave an **automatic call back request** on this trunk group.

3.32.1.2 ADDITIONAL INFORMATION

- A user can leave only one type of automatic call back request at a time: on busy station or trunk group.
- If the automatic call back request is accepted, the user hears the dial tone if he is off hook and switches to the idle status in hands-free mode.
- An automatic call back request does not follow call diversion (not even a "Do Not Disturb").
- The system accepts as many automatic call back requests on a busy trunk group as it contains lines.

- Automatic call back cannot be picked up (see "Call pick-up").
- Automatic call back which the requesting party does not answer is not recorded in the directory of unanswered calls.

3.32.2 Configuration procedure

3.32.2.1 CONFIGURATION

- To specify whether or not to authorize a station to leave an automatic call back request:

• by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Features** -> **"Callback"**

3.32.3 Operation

3.32.3.1 ACTIVATION/USE

P.K.: Programmed Key – defined by OMC (Expert View) or MMC-Station

S.K.: Soft Key

Code: Code programmed in the "Features in Conversation" table

Type of station / Type of service	**All stations (including Z)**	**Without display (# Z)**	**With display, no soft keys**	**With soft keys**
Automatic call back request (*)	Function code	P.K.: **Automatic callback request**	P.K.: **#Cback**	S.K.: **#Cback**

(*) When a line in the trunk group is released, the subscriber requesting callback is rung. When he picks up the handset, he hears the dial tone. He then needs simply to dial the number without entering the trunk group number.

When the automatic callback request was left following an automatically dialed call (by personal speed dial, for example), the dialing is transmitted automatically by the system once the requester has answered the callback.

3.32.3.2 CANCELLATION

Prefix: Code programmed in the "Features in Conversation" table

Type of station / Type of service	All stations (including Z)	**Without display (# Z)**	**With display, no soft keys**	**With soft keys**
Automatic call back (**)	Prefix	P.K.: **Cancel callback**	P.K.: **#Cback**	S.K.: #**Cback**, before or during callback

(**) The automatic call back request is also cancelled if:

- the person requesting call back does not go off hook within 25 seconds or presses the "Release" key during these 25 seconds
- no line in the trunk group becomes free within 30 minutes

- all the resources of the person requesting call back are busy
- after the person requesting the callback has answered, all the lines in the trunk group return to busy.

3.33 Transmission of DTMF Codes

3.33.1 Overview

3.33.1.1 DESCRIPTION

A station can dial either:

- in rotary or pulse dialling mode, or
- in DTMF (Dual Tone Multi Frequency) mode (default for some countries)

In order to use the services of a server or a telephone answering device, a station must use DTMF dialling so that the PCX can forward the digits dialled to this server without analysing them.

A DTMF dialling station does this by default since it generates the DTMF dialling itself.

A rotary or pulse dialling station must activate **DTMF end-to-end signalling**. The digits dialled are then converted into DTMF dialling.

"DTMF end-to-end signalling" can be activated in one of the following ways:

- manually, during internal or external conversation
- automatically, via a pre-recorded number in which a "**forced DTMF end-to-end signalling**" character is programmed, possibly followed by digits to be transmitted in DTMF:
  - in the personal speed dial numbers (internal or external number)
  - in the system speed dial numbers (external number)
  - on a direct call key (internal or external number)
- automatically, during an internal or external call via DTMF end-to-end signalling programming for each station or system.

3.33.1.2 ADDITIONAL INFORMATION

- When "DTMF end-to-end signalling" is forced in a pre-recorded number, the digits to be sent in voice frequencies can be either pre-recorded or dialled by the user when he makes the call.
- The character symbolising "Forced DTMF end-to-end signalling" is the slash ("/"). This character also introduces a 5-second pause (non-modifiable) before sending the rest of the number in DTMF end-to-end signalling; to introduce a 10 second pause: xxxx // xxxx.
- When a number with "Forced DTMF end-to-end signalling" is recorded in the "Redial" or "Temporary number" store, the number is transmitted and the end-to-end signalling service activated when the content of these stores is recalled. However, the digits to be sent in voice frequencies are not retransmitted if they were dialled by the user at the time of making the call.
- The number of "Forced DTMF end-to-end signalling" characters and digits to be sent in voice frequency format depend on the total number of digits authorised in programming a

speed dial entry or call key and the number of digits forming the directory number of the called server.

- The system makes it possible to program the DTMF end-to-end signalling feature in conversation which, when it is dialled, enables the activation of the end-to-end signalling and the transmission of the character "**", frequently requested by the voice servers (see "Configuration").
- DTMF end-to-end signalling:
  - when DTMF end-to-end signalling is active for the system or station while in conversation, access to the features during a conversation are no longer offered (except for DTMF analogue stations that have access to these features via the intermediary of the "R" key).
  - to make a consultation (enquiry call) on a single-line station, DTMF end-to-end signalling must first be cancelled by pressing on a key programmed "DTMF end-to-end signalling". A multi-line station uses a resource key.
  - DTMF end-to-end signalling can be deactivated for the current call by pressing a soft key or DTMF programmed key ¦ (access to features during a conversation and to consultation (enquiry) calls is performed as it was before activating this function).

Note:

DTMF "resend" is not possible between 2 IP phone sets.

3.33.1.2.1 DTMF and IP trunking

The standard used for DTMF exchange on IP trunks is RFC2833 (RTP with specific payload type).

From Alcatel-Lucent OmniPCX Office Communication Server R6.0 on, the feature direct RTP on SIP trunking can be activated.

If direct RTP is activated, it is the IP sets which generate RTP packets containing RFC2833 towards distant IP sets or gateway.

Restrictions: IP sets not managing RFC2833 are unable to send DTMF when Alcatel-Lucent OmniPCX Office Communication Server is configured in direct RTP. IP sets managing RFC2833 include:

-
- PIMphony IP R6.0 (older PIMphony IP do not)

If direct RTP is not activated, IP sets behave like TDM sets. DTMF is sent to Alcatel-Lucent OmniPCX Office Communication Server through signalling messages and converted into RTP packets by the DSP allocated to the IP trunk

3.33.2 Configuration procedure

3.33.2.1 CONFIGURATION

- To modify the value of the time-out during which DTMF end-to-end signaling is active:

• by OMC (Expert View): **System Miscellaneous** -> **Memory Read/Write** -> **Timer Labels** -> **"IntDgMfTim"**
• by MMC-Station: **Global -> Rd/Wr -> Timers -> "IntDgMfTim" -> Return -> Memory**

- To modify the value of the time-out during which forced DTMF end-to-end signaling is active:

- by OMC (Expert view): **System Miscellaneous** -> **Memory Read/Write** -> **Timer Labels** -> **"ForceMFTim"**
- by MMC-Station: **Global -> Rd/Wr -> Timer -> "ForceMFTim" -> Return -> Memory**

- Create the Features in Conversation making it possible to activate the end-to-end signaling and to resend the * in DTMF:

- by OMC (Expert View): **Numbering** -> **FAC Numbering Plan**
- by MMC-Station: **NumPln -> Code -> Funct -> "Send MF num"**

- To specify whether or not to activate DTMF end-to-end signaling for a given station (service deactivated by default):

- by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Features** -> **MF Transparency**

3.33.3 Operation

3.33.3.1 ACTIVATION/USE

P.K.: Programmed Key – defined by OMC (Expert View) or MMC-Station

S.K.: Soft Key

Code: Code programmed in the "Features in Conversation" table

Service \ Type of station	**Z decadic**	**Without display**	**With display, no S.K.s**	**With soft keys**
Manual activation during communication	Code **DTMF end-to-end signaling**	P.K.: **DTMF end-to-end signaling**	P.K.: **#DTMF**	S.K.: **#DTMF**
Automatic activation	By collective speed dial numbers	All types of pre-recorded dialing	All types of pre-recorded dialing	All types of pre-recorded dialing

3.33.3.2 cancellation

Type of station / Service	**Z decadic**	**Without display**	**With display, no S.K.s**	**With soft keys**
When activation has been done manually	Automatic deactivation on "IntDgMfTim" time-out.	P.K.: **DTMF end-to-end signaling**	P.K.: **#DTMF**	S.K.: #**DTMF**
When activation was automatic	Automatic deactivation on "ForceMFTim" time-out when the system encounters the "/" character or manual deactivation by key.			

3.34 Call Pick-Up

3.34.1 Overview

3.34.1.1 DESCRIPTION

When a station rings, another user can answer the call in place of the destination station. This call is "picked up". There are various types of pick-up:

- a call to a station outside a pick-up group: this is an **individual pick-up**
- a call to a station within a pick-up group: this is a **group pick-up**
- a call arriving at the general level: this is a **general call answer**

3.34.1.2 ADDITIONAL INFORMATION

- A private subscriber can only pick up internal calls.
- A private call cannot be picked up.
- A call intended for a Hunting Group with cyclic or sequential management (see section "system features" file "Hunting Groups") can be picked up like an individual pick-up.
- A call intended for a group of operator stations can only be picked up by individual pick-up.
- Prefixes for pick-up functions in the numbering plans: the basic value may vary depending on the local software version. The French settings are as follows:
  - Pick-up: base 0 = individual pick-up
  - Pick-up: base 1 = group pick-up
  - Pick-up: base 2 = general call pick-up

3.34.2 Configuration procedure

3.34.2.1 CONFIGURATION

- To create the pick-up groups:

• by OMC (Expert View): **Pickup Groups** • by MMC-Station: **Groups** -> **Pick Up**

- To specify whether or not to authorize a station to pick up a call:

• by OMC (Expert View): **Subscribers/Basestations List -> Subscribers/Basestations List** -> **Details** -> **Features** -> **"Call Pickup Allowed"**

3.34.3 Operation

3.34.3.1 ACTIVATION/USE

P.K.: Programmed Key – defined by OMC (Expert View) or MMC-Station

S.K.: Soft Key

Prefix: Code programmed in the internal numbering plan

Type of station / Type of service	Multiline	All stations (including Z)	Without display (# Z)	With display, no soft keys	With soft keys
Individual pick-up (*)	--	Code + n# of station ringing	P.K.: **Individual pickup** + nº of station ringing	P.K.: **IndPic** + nº of station ringing	S.K.: **Pickup** + S.K.: **IndPic** + nº of station ringing
Group pick-up (*)	--	Prefix	P.K.: **Group pick-up**	P.K.: **GrpPic**	S.K.: **Pickup** + S.K.: **GrpPic**
General call answer (*)	--	Prefix	P.K.: **General Call Answer**	P.K.: **GenBel**	S.K.: **Pickup** + S.K.: **GenBel**

(*) If the pick-up is accepted, the user converses with the caller, if not, he hears the fast busy tone.

3.35 Call Parking/Parked Call Retrieval

3.35.1 Overview

3.35.1.1 DESCRIPTION

A user in conversation with an external correspondent can suspend this conversation and retrieve the correspondent later on from the same station or another station in the installation.

3.35.1.2 ADDITIONAL INFORMATION

- When a user is involved in a conference or an intrusion, call parking is refused.
- An internal call cannot be parked.
- When the external correspondent is parked for more than the default value of 90 seconds, the call is routed to the general level (see "Operator Station").
- The system allows as many parked calls as there are network lines.
- Prefix for the Call Parking function in the numbering plans = Pick-up prefix + base 3. (For France: the basic value may vary according to the local version of the software).

3.35.2 Configuration procedure

3.35.2.1 CONFIGURATION

- Modify, if necessary, the default timeout before rerouting of the parked call (90 seconds) – OMC (Expert View) only:

System Miscellaneous -> Feature Design -> Part 3 -> "Time before parked call is rerouted"

The rerouting of parked calls depends on the contents of **Incoming Call Handling** -> **Public Caller** -> **Go to Attendant or Release**

3.35.3 Operation

3.35.3.1 ACTIVATION/USE

P.K.: Programmed Key – defined by OMC (Expert View) or MMC-Station

S.K.: Soft Key

Code: Code programmed in the "Features in Conversation" table

Type of station / Service	**All stations including Z**	**Without display**	**With display, no soft keys**	**With soft keys**
Parking of an external correspondent	Prefix (*)	P.K.: **Call Parking** (*)	P.K.: **Park** (*)	S.K.: **Park** (*)
Parked call retrieval	Prefix **Call Parking** + nº of station from which the call was parked	P.K.: **Call Parking** + nº of station from which the call was parked	P.K.: **Park** + nº of station from which the call was parked	S.K.: **Pickup** + S.K.: **Park** + nº of station from which the call was parked

(*) If the request is accepted, the external correspondent is placed on hold and hears the please-wait music.

3.36 Paging

3.36.1 Overview

3.36.1.1 DESCRIPTION

An authorized user can inform another internal user with a portable receiver (or "bleep") that he is trying to contact him on the telephone.

Paging is carried out depending on the paging device connected to the PCX, either:

- by suffix, i.e. after calling the user to be paged, with the latter not answering the telephone
- par "mode 4" prefix: the caller dials the paging prefix then, depending on the device, makes a voice announcement or dials a pager number. The called party dials the paging answer number
- by "mode 2" prefix (using the ESPA protocol): the caller dials the paging number followed by the number for the device (it is a good idea to make pager numbers match station numbers). The called party dials the answer number followed by his station number.

3.36.1.2 ADDITIONAL INFORMATION

- A user can only activate a single paging operation at a time.
- For the "by suffix" type of paging, the system allows 4 simultaneous answer attempts by default.
- Paging must be answered before the "Maximum Waiting Time for Paging" time-out expires.

3.36.2 Configuration procedure

3.36.2.1 CONFIGURATION

- To specify whether or not to authorize a station to carry out paging by suffix:

• by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Features** -> **"Paging"**

- To program the "bleep" numbers for users with pagers:

• by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Misc.** -> **"Paging Code/Phone Card Password"** • by MMC-Station: **Subscr** -> **Paging**

- To configure the type of paging device connected to the PCX – OMC (Expert View) only:

System Miscellaneous -> Feature Design -> "Paging Type"

- To modify the paging no-answer time-out value if required out – OMC (Expert View) only:

System Miscellaneous -> Feature Design -> Part 2 -> "Maximum Waiting Time for Paging"

- If necessary modify the value of the paging device busy time-out – OMC (Expert View) only:

System Miscellaneous -> Feature Design -> Part 3 -> "Maximum Connection Time for Paging"

- To define the paging activation code:

• by OMC (Expert View): **Numbering** -> **Internal Numbering Plan** -> **Paging Activation**

- To define the answer code:

• by OMC (Expert View): **Numbering** -> **Internal Numbering Plan** -> **Paging Answ. (Gen.)**

- For "by suffix" paging, configure the analog line to which the paging device is connected:

• by OMC (Expert View): **External Lines** -> **Trunk List** -> **Details** -> "Paging" • by MMC-Station: **Access** -> **Paging**

- For "by prefix, mode 4" or mode 2" paging, configure the SLI interface to which the paging device is connected:

• by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Misc.** -> **"Special Function"** • by MMC-Station: **Subscr** -> **SpeDev**

3.36.3 Operation

3.36.3.1 ACTIVATION/USE

P.K.: Programmed Key – defined by OMC (Expert View) or MMC-Station

Prefix: Code programmed in the internal numbering plan or the "Features in Conversation" table

Type of station / Service	All stations including Z	Without display	With display, no soft keys	With soft keys
Paging by suffix, in ringing phase, the correspondent called does not answer	Prefix **Paging by suffix** (*)	P.K.: **Paging by suffix** (*)	P.K.: **Page** (*)	
Paging by prefix, mode 4	Prefix **Paging by prefix** + nº of pager(**)	P.K.: **Paging by prefix** + nº of pager(**)	P.K.: **PgPfx** + nº of pager(**)	
Paging by prefix, mode 2	Prefix **Paging by prefix** + nº of station paged (*)	P.K.: **Paging by prefix** + nº of station paged (*)	P.K.: **PgPfx** + nº of station paged (*)	
Answering paging by suffix	Prefix **Selective paging answer** + nº of station paged	P.K.: **Selective paging answer** + nº of station paged	P.K.: **PgaSel** + nº of station paged	
Answering paging by prefix, mode 4	Prefix **General Paging Answer**	P.K.: **General Paging Answer**	P.K.: **PgaGen**	
Answering paging by prefix, mode 2	Prefix **Selective paging answer** + nº of station paged	P.K.: **Selective paging answer** + nº of station paged	P.K.: **PgaSel** + nº of station paged	

(*) The requesting party stays on line and waits for the paged party to answer. Conversion of the set number into paging receiver number is carried out by the system, which informs the paging device.

(**) The requesting party stays on line and waits for the paged party to answer.

3.37 Main PCX Recall

3.37.1 Overview

3.37.1.1 DESCRIPTION

If a user wishes to use the services offered by the analog network operator, he must transmit a calibrated loopbreak over the line.

This procedure must also be followed when the system is connected to a PCX of larger capacity via analog network lines.

3.37.1.2 ADDITIONAL INFORMATION

The "Main PCX Recall" programmed key or "#PBX" key can be replaced by a macro command programmed key "Macro3 = Main PCX recall + transmission of a number or code".

3.37.2 Configuration procedure

3.37.2.1 CONFIGURATION

- For each analog network line, configure the value of the calibrated loopbreak using OMC

Expert View (only):

External Lines -> **List of Accesses** -> **Details** -> **"Cut off Type"**

- To modify the default value for the activation of the time-out for the calibrated loopbreak if no figure has been transmitted:

• by OMC **System Miscellaneous -> Memory Read/Write -> Misc. Labels -> "IntClLpTim"** • by MMC-Station: **Global -> Rd/Wr -> Address -> "IntClLpTim" -> Return -> Memory**

3.37.3 Operation

3.37.3.1 ACTIVATION/USE

P.K.: Programmed Key – defined by OMC (Expert View) or MMC-Station

F.K.: Fixed Key

S.K.: Soft Key

Code: Code programmed in the "Features in Conversation" table

Type of station	**Z**	**Without display**	**With display, no soft keys**	**With soft keys**
Main PCX recall	F.K.: **R**. **+** Code (*)	P.K.: **Main PCX recall** (*)	P.K.: **#PBX.** (*)	S.K.: **#PBX.** (*)

(*) the system then transmits a main PCX recall to the local PCX and the following digits.

3.37.3.2 CANCELLATION

Type of station	**Z**	**Without display**	**With display, no soft keys**	**With soft keys**
Cancel main PCX recall	Automatic (*)	P.K.: **Main PCX recall**	P.K.: **#PBX.**	S.K.: #**PBX.**

(*) after the expiry of a time-out of:

- 5 seconds, programmable, if no figure has been entered
- 10 seconds if a figure has been entered (normal time-out for figures)

3.38 Text Mail/Delayed Callback Request

3.38.1 Overview

3.38.1.1 Text Mail

A user who has a station with a display can send a text message to another internal user who has a display and Message LED, either:

- while not on a call
- during call setup, whatever the called party's status

The system offers 27 pre-programmed messages. Some of these include a variable part (for example, a date or room number, etc.) that has to be filled in. A user who has a station with soft keys can also create a complete message using the alphabetic keypad.

When the recipient has a station without a display (but with a Message LED), the text message becomes a "delayed callback request".

Starting with version R2.0 of the software, the number of the text message sender may be saved (temporary memory (storage) or personal directory) (see also module Making/Answering a Call - Overview).

Starting with version R7.0, pre-programmed messages can be recorded in non-Latin characters. Users with compatible sets can edit and display messages in non-Latin characters.

Alcatel-Lucent IP Touch 4028/4038/4068 and Alcatel-Lucent 4029/4039 Digital Phone sets support Latin, Cyrillic and Chinese/Taiwanese/Cantonese characters.

Alcatel-Lucent IP Touch 4008/4018 and Alcatel-Lucent 4019 Digital Phone sets can display Latin and Cyrillic characters.

Other sets only support Latin characters.

3.38.1.1.1 User-Defined Messages

Sending a User-Defined Message

On Alcatel-Lucent IP Touch 4028/4038/4068 and Alcatel-Lucent 4029/4039 Digital Phone sets, a user can edit a user-defined message with:

- Latin characters, and
- Non-Latin characters corresponding to the set language (for example Cyrillic characters if the set language is Russian, or Chinese characters if the set language is Chinese)

On other sets, users can edit user-defined messages with Latin characters only.

Displaying a Received User-Defined Message

The display of messages depends on the set capabilities and on the set language.

Alcatel-Lucent IP Touch 4028/4038/4068 and Alcatel-Lucent 4029/4039 Digital Phone sets can display:

- Latin characters
- Cyrillic characters
- Chinese/Cantonese/Taiwanese characters if the set language is Chinese/Cantonese/Taiwanese

Alcatel-Lucent IP Touch 4008/4018 and Alcatel-Lucent 4019 Digital Phone sets can display:

- Latin characters
- Cyrillic characters

Other sets only display Latin characters.

Characters which cannot be displayed on a set are replaced by question marks ("?").

3.38.1.1.2 Pre-Programmed Messages

Sending a pre-programmed message

On Alcatel-Lucent IP Touch 4028/4038/4068, Alcatel-Lucent 4029/4039 Digital Phone and MIPT sets, users can select one of the four system languages to send a pre-programmed message.

On Alcatel-Lucent IP Touch 4008/4018 and Alcatel-Lucent 4019 Digital Phone sets, users can only select one of the languages that can be displayed on their sets, i.e. languages written in Latin or Cyrillic characters.

On other sets, users can only select languages written in Latin characters.

Editing a Pre-Programmed Message

On Alcatel-Lucent IP Touch 4028/4038/4068 and Alcatel-Lucent 4029/4039 Digital Phone and MIPTsets, a user can edit a pre-programmed message with:

- Latin characters, and
- Non-Latin characters corresponding to the set language (for example Cyrillic characters, if the set language is Russian)

On Alcatel-Lucent IP Touch 4028/4038/4068 and Alcatel-Lucent 4029/4039 Digital Phone and MIPT sets, users may select predefined messages in languages not available on their own set. A set whose language is English can send predefined messages in Chinese for instance. During selection of the message, the message list is displayed in Latin characters, but the set receiving the message will display its Chinese equivalent.

On other sets, users can edit pre-programmed messages with Latin characters only.

Displaying a Pre-Programmed Message on the Receiving Set

On Alcatel-Lucent IP Touch 4028/4038/4068 and Alcatel-Lucent 4029/4039 Digital Phone sets where the set language is Chinese/Cantonese/Taiwanese, a pre-programmed message is displayed normally (exactly as it was sent).

On Alcatel-Lucent IP Touch 4028/4038/4068 and Alcatel-Lucent 4029/4039 Digital Phone sets where the set language is not Chinese/Cantonese/Taiwanese and on Alcatel-Lucent IP Touch 4008/4018 and Alcatel-Lucent 4019 Digital Phone sets:

- A pre-defined message sent in Chinese/Cantonese/Taiwanese language is replaced by its translation in the default Latin language (English or the first Latin language, if English is not a system language) and unsupported characters edited by the sender are replaced by question marks ("?")
- A pre-defined message containing only Latin and Cyrillic characters is displayed normally (exactly as it was sent)

On other sets, a pre-defined message sent in non-Latin characters is replaced by its translation in the default Latin language (English or the first Latin language if English is not a system language) and unsupported characters edited by the sender are replaced by question marks ("?").

3.38.1.2 Delayed Call-Back Request

A user whose set does not have a display but has a "Delayed callback request key" can leave a delayed callback request for another user whose set has a Message LED. The callback request can only be left during call setup as long as the called party has still not answered.

3.38.1.3 Additional Information

- On a analog (Z) station intended to receive a delayed callback request, a "virtual" "Master

Mailing" key must be configured with OMC (Expert View), or an "MsgLed" with MMC-Station.

- Calls from external Z users to stations in redirected text answering are forwarded to the Attendant Station; the text message is shown on the Attendant Station display.

3.38.2 Configuration procedure

3.38.2.1 CONFIGURATION

- To modify the pre-defined messages - OMC (Expert View) only:

System Miscellaneous -> Messages and Music -> Mailing Messages

3.38.3 Operation

3.38.3.1 ACTIVATION/USE

P.K.:: Programmed Key - defined by OMC (Expert View) or MMC-Station

F.K. : Fixed Key

S.K.:: Soft Key

Prefix:Code programmed in the internal numbering plan

Station / Service or Function	**Z**	**Without display (# Z)**	**With display, no S.K.s**	**With soft keys**
Choice of text message (*)	--	--	F.K.: **Mail** or P.K.: **MsgLED** + 3 + Destination no. if requested + F.K. **i** + 3 + Message no.	F.K.: **Mail** + S.K.: **Text** + no. of destination if requested + S.K.: **MsgNo** +Message no.
Modify language for the message	--	--	F.K. **i** + 4	S.K.: **Lang**
To validate the chosen message	--	--	F.K.: **LS**	S.K.: **OK**
To validate the variable part	--	--	F.K.: **LS**	S.K.: **OK**
Read text messages received (*)	--	--	F.K.: **Mail** +3	F.K.: **Mail** + S.K.: **Text** + S.K.: **Read**

Station / Service or Function	Z	Without display (# Z)	With display, no S.K.s	With soft keys
Send a delayed call-back request	Code +1	P.K.: **Delayed callback request** + 1	--	
Presence of a text message or delayed call-back request	Flashing LED **Message**		Flashing 2-colour LED and **Message**	
Answer a delayed call-back request	Prefix	P.K.: **Delayed call-back request**	--	

(*) When the set is idle, the system gives priority to "reading" the messages received (voice messages first, then text).

3.39 ISDN Services

3.39.1 Overview

3.39.1.1 Description

The default dialling mode on ISDN lines is digit by digit. At the press of a key, users can employ block dialling to access a range of services:

- addition of a **sub-address** to the number dialled
- activation of **calling line identification restriction**, i.e. the caller's identity is not transmitted to the called party
- for a station with soft keys only, transmission of **user-to-user signalling (UUS)**, i.e. a text message on a station with a display.
  Starting with R7.0, provided their sets allow it, users can send UUS messages containing non-Latin characters (see module Text Mail/Delayed Callback Request - Overview)
  - If the receiver belongs to the same PCX as the sender, the treatment applied before displaying the UUS message is the same as for displaying a text message. For more information, see: module Text Mail/Delayed Callback Request - Overview § Displaying a Pre-Programmed Message on the Receiving Set .
  - If the receiver is an ISDN destination, as the ISDN UUS service is restricted to Latin characters, the message is changed into IA5 format: a pre-defined message sent in non-Latin language is replaced by its translation in the default Latin language and non-Latin characters edited by the sender are replaced by question marks ("?").

The "**Calling Line Identification Restriction**" function can also be activated in digit-by-digit dialling mode for all stations (see "Making/Answering a call").

When a call is received, the **"malicious call identification" service is available** This service, available by subscription to the network, involves the network operator recording certain call details either during the communication or during the release phase after the caller has hung up, (numbers of both parties; date and time of call; sub-address of caller if applicable).

The **keypad dialling features** offer access (transparently) to the services provided by the public network exchange carrier (the functional services of the particular operator).

3.39.1.2 Additional Information

- When the user has activated the block dialling, he cannot select a specific access via an RSP (see "Resource Keys").
- In block dialling, if the dialling transmitted is incomplete, the line used is released as no digit can be added to the dialling.
- Only a station with soft keys can receive UUS during an answered call. It can be reviewed during the conversation by pressing the "Msg" soft key.
- Malicious call identification is not available to stations behind a private network
- Malicious call identification cannot be requested after a call transfer or suspension.

3.39.2 Configuration procedure

3.39.2.1 CONFIGURATION

- For each station, to specify whether or not to permanently activate "calling line identification restriction":

• by OMC (Expert View):**Subscribers/Base stations List** -> **Subscribers/Base stations List** -> **Details** -> **Features** -> **"Identity Secrecy"**

- For each station, to specify whether or not to authorize reception of User to User Signaling:

• by OMC (Expert View): **Subscribers/Base stations List** -> **Subscribers/Base stations List** -> **Details** -> **Features** -> **"UUS Allowed"**

- To modify the maximum time-out, after going on hook, for requesting recording of the caller's identity - OMC (Expert View) only:

External Lines -> Protocols -> ISDN Trunk -> Layer 3 -> "T305 Disconnect Supervision"

3.39.3 Operation

3.39.3.1 ACTIVATION/USE

P.K.:: Programmed Key - defined by OMC (Expert View) or MMC-Station

F.K. : Fixed Key

S.K.:: Soft Key

Type of station / Service	Z	Without display	With display, no soft keys	With soft keys
Activate calling line identification restriction before dialing, in sequential or block dialing modes	--	P.K. **CLIR**	P.K.: **CLIR**	P.K.: **CLIR**
Switch to block dialing mode	--	--	F.K.: **ISDN** or P.K. **BMdial**	F.K.: **ISDN**
Delete digit preceding the cursor in block mode dialing (number and sub-address)			F.K.: **CLIR**	S.K.: **Rubout**
Add a sub-address in block dialing mode	--	--	P.K.: **SubAdd**	S.K.: **SubAdd**
To validate the sub-address, in block dialing mode	--	--	P.K.: **SubAdd**	S.K.: **OK**
Add UUS, in block dialing mode	--	--	--	S.K.: **Text** + n# of message (from 0 to 27) (*)
Activation of calling line identification restriction, in block dialing mode	--	--	--	S.K.: **CLIR**
To set up the call in block dialing mode (with or without sub-address, with or without UUS).	--	--	F.K.: **ISDN** or P.K. **BMdial**	S.K.: **Send**
Activate malicious call identification	Function code			S.K.: **MCID**

(*) Messages 1 to 27 are pre-defined in the system. Some of them have a variable part which must be completed (return time, room number, etc.). Message n# "0" can be made up completely from the alphabetic keypad (up to 32 characters).

3.40 ISDN Services With Keypad Facility

3.40.1 Overview

3.40.1.1 KEYBOARD FACILITIES (KEYPAD DIALLING)

In certain countries, the public ISDN operator provides services that can be activated using the ETSI ETS 300 122 protocol (in addition to these generic services, each public operator defines how these services are handled in their national specifications).

To access these services, the system establishes transparent communications between the public exchange and the internal users, who can then key in codes and receive a response from the public exchange.

This service is available with all station types on an Alcatel-Lucent OmniPCX Office Communication Server system directly connected to the public exchange (not through a private network).

Up to the version R2.0, the operator services can only be activated from the rest state of the set. From the version R2.01, in addition to activation from the rest state, it is possible to activate the services of the operator during the call (for instance using the "conference operator" service to set up a conference with 2 outside parties while only using a single B channel)

3.40.2 Configuration procedure

3.40.2.1 Configuration

- To activate the service at system level:

• by DHM-OMC (Expert View) : **System features -> Features -> Access transparent to system functions in idle state** • by DHM-OMC (Expert View) : **System features -> Features -> Access transparent to system functions in conversation**

- For each set concerned, create a service implementation key during call:

• by DHM-OMC (Expert View): **Subscribers/Base stations List -> Subscribers/Base stations List -> Details -> Key -> Function = System simultaneous call function**.

- Define the feature access code "Simultaneous call system function":

• by DHM-OMC (Expert View) : **Dialling plan -> Feature access code (service codes) -> Simultaneous call system function**

3.40.3 Operation

3.40.3.1 Activation/Deactivation

3.40.3.1.1 From the rest state (to R2.0)

Operator services can be activated if the "Transparent access to system functions in idle state" flag is active and if the user DID number is configured in the public dialling plan.

Note:
The placing of the flag is only necessary if the service codes are carried in the "Keypad Facility" information element; in some countries (Finland for instance), codes are contained in the "Called party number" element and the placing of the flag is then ignored (codes are issued without special processing).

To activate the service:

- **by manual dialling:** dial the ISDN trunk group seizure code, then press * or # followed by the operator service code (22 figures maximum).
- **by using a "Dialling" programmed key:** this key is programmed with the trunk group seizure code and all or part of the service code.
- **by using a "Block dialling" programmed key.**

3.40.3.1.2 During a call (from R2.01

Operator services can be activated during an outside party call (incoming or outgoing call on digital line) if the "Access transparent to system functions in conversation" flag is active.

To activate the service:

- **by using a programmed key "Simultaneous call system function":** after pressing this key (the icon or the led of the key indicates activation), dial the number of the 2nd

correspondent (simultaneous call, the 1st correspondent is put on hold) or dial the feature access code (conference, alternation on inquiry, cancellation of the simultaneous call) of the internal dialling plan desired; this code will be converted into corresponding operator service code.

- **by dialling the feature access code "Simultaneous call system function":** this option is offered to sets without programmed key (analogue sets).

3.41 Station Comfort Features

3.41.1 Overview

3.41.1.1 DESCRIPTION

User convenience involves:

- the ability to cut oneself off from the other party, i.e. to deactivate the microphone (in the handset or the handsfree feature) by activating "**mute**".
- for a station with display, the option of reading the number assigned to the station (and, if it exists, the number assigned to the V24, S0, or Z option) and the associated name programmed into the internal directory using the "**Station Identity**" feature
- the option of preventing use of one's own station (programming, making external calls, access to text messages and non-answered calls directory, activation and cancellation of call forwarding) by activating **locking** of the station of the latter.
- the ability to use the station's loudspeaker with **amplified reception** and to adjust the volume.
- for dedicated sets, the option of adjusting the conversation volume at the handset.
- the option to choose the time display format: European or US format.

3.41.2 Configuration procedure

3.41.2.1 CONFIGURATION

- On each station, the personal code can be modified by customization only.
- For dedicated sets, to specify whether or not to authorize adjustment of the handset volume:

- by OMC: **System Miscellaneous** -> **Memory Read/Write** -> **Timer Labels** -> **" GainCtrlON"**
- by MMC-Station: **Global -> Rd/Wr -> Address -> " GainCtrlON" -> Return -> Memory**

- For stations with display, choose the time display format: Europe or US

- by OMC **System Miscellaneous** -> **Memory Read/Write** -> **Timer Labels** -> **"TimeAmPm" with 00 = European format, 01 = US format**
- by MMC-Station: **Global -> Rd/Wr -> Address -> "TimeAmPm" with 00 = European format, 01 = US format -> Return -> Memory**

3.41.3 Operation

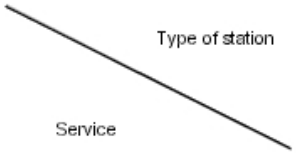
3.41.3.1 ACTIVATION/USE

P.K.:: Programmed Key - defined by OMC (Expert View) or MMC-Station

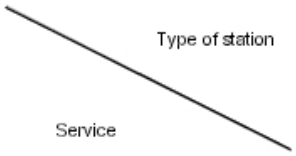
F.K. : Fixed Key

S.K.:: Soft Key

Prefix:Code programmed in the internal numbering plan

	**Z**	**Without display, without "mute" F.K.: and/or without LS**	**Without display, with "mute" F.K.: and/or with LS**	**With display, no S.K.s**	**With soft keys**
Communication mute	--	--	F.K.: **CLIR**	F.K.: **CLIR**	
Station identity (and option)	--	--	--	2 presses on key **i**	
Lock	Prefix + personal code	P.K.: **Lock/Unlock** + personal code		P.K.: **Lock** + personal code	S.K.: **Lock** + personal code
Amplified reception	--	--	F.K.: **LS** or F.K.: **LS+**	F.K.: **LS**	
Adjust the handset volume	--	--	F.K.: **LS-** and **LS+**		

3.41.3.2 cancellation

	**Z**	**Without display, without "mute" F.K.: and/or without LS**	**Without display, with "mute" F.K.: and/or with LS**	**With display, no S.K.s**	**With soft keys**
Communication mute	--	--	F.K.: **CLIR**	F.K.: **CLIR**	
Unlock	Prefix + personal code	P.K.: **Lock/Unlock** + personal code		P.K.: **Lock** + personal code	S.K.: **Lock** + personal code
Amplified reception	--	--	F.K.: **LS** or F.K.: **LS-**	F.K.: **LS**	

(*) Mute is also deactivated at the end of the communication.

3.41.3.3 DATE AND TIME DISPLAY

The date and time display format can be defined using the "TimeAmPm" flag: European format (flag = 00) or US format (flag = 01).

3.41.3.3.1 Date display

European format: **Wed 22 May**.

US format: **05/22/02**

3.41.3.3.2 Time display

European format	Format
00:00 to 00:59	12:00 am to 12:59 am
01:00:00 to 11:59:00	01:00:00 am to 11:59:00 am
12:00:00 to 12:59:00	12:00 pm to 12:59 pm
13:00:00 to 23:59:00	01:00:00 pm to 11:59:00 pm

3.42 Specific Operator Station Services

3.42.1 Overview

3.42.1.1 DESCRIPTION

An Operator Station can:

- switch the entire installation to normal or restricted mode, independently of the time range (see "Normal/Restricted service (system level)")
- reserve a trunk group (the last) for exclusive use of the Operator Stations. Each O.S. in the active group can use this trunk group for communications with the network.
- activate the background music, coming from a tuner on an external loudspeaker connected to the system.
- activate forwarding of all internal and external calls intended for the O.S. group to a network destination, defined by a common speed dial number or an internal destination, either:
  - by switching the installation into restricted mode (using a programmed key)
  - or using a programmed Attendant diversion key

This forwarding can also be automatically activated according to the time range.

The system can be used to program 3 different forwarding destinations:

- the first, for automatic activation by scheduling: this is valid for all time ranges
- the second, for manual activation, by switching the installation to restricted mode on one of the O.S. in the active group
- the third, by using the operator calls forwarding key pre-programmed with the local or collective speed dial number for which the calls are intended

Operator call diversion is activated and deactivated in accordance with the following descending order of priority:

- by forwarding key
- by normal/restricted mode key
- by scheduling.

3.42.1.2 ADDITIONAL INFORMATION

- There is no particular signal to indicate attendant diversion when it is activated by scheduling.
- The icon or the LED associated with the NRmode programmed key is lit when one of the O.S. has used this key.
- The icon or LED associated with all of the "Attendant diversion" programmed keys signals activation of forwarding by this key.
- No checks are run on the collective speed dial rights, the barring or the traffic sharing on forwarding to an external number.
- When the O.S. call is the result of the dynamic routing mechanism (see "Incoming call distribution"), the call is forwarded and the initial call destination and level 1 destination are released.
- When calls to the O.S. are forwarded:
  - there is no overflow to the default O.S. group
  - pre-announcement is not used.

3.42.2 Configuration procedure

3.42.2.1 CONFIGURATION

- For each time-range, define whether attendant diversion is activated when the OS switches manually to restricted mode – OMC (Expert View) only:

Time Ranges -> "All Days"

- To define the type of mechanism used to forward external incoming calls to a network number: rerouting or joining (see "External Forwarding" for more details on the 2 types of forwarding):

- by OMC (Expert View): **System Miscellaneous** -> **Feature Design** -> **Part 2** -> **"External Diversion Mode"**
- by MMC-Station: **Global** -> **Joing** -> **Forwd**

- When the selected mechanism for forwarding external incoming calls to a network number is "joining", fill out the connectivity matrix by OMC (Expert View) only:

Traffic Sharing and Barring -> Joining

- Program the number (internal or collective speed dial) to which the operator calls are forwarded following automatic activation by scheduling – OMC (Expert View) only:

Time Ranges -> "Destination for time ranges"

- Program the number (internal or collective speed dial) to which the operator calls are forwarded following manual activation with the "NRmode" programmed key – OMC (Expert View) only:

Time Ranges -> "Destination if restr. mode manually activated"

- On the OSs, program one or more "Attendant diversion" keys with a number (internal or collective speed dial) to which the operator calls are to be forwarded:

• By OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Keys** -> **"Attendant Diversion"** • by MMC-Station: **Subscr** -> **Key** -> **Option** -> **ExtFwd**

3.42.3 Operation

3.42.3.1 ACTIVATION/USE

P.K.: Programmed Key – defined using OMC (expert View) or MMC-Station

Switch to restricted mode	When the system operates in normal mode, P.K.: **NRMode** + operator code
Reservation of last trunk group	P.K.: **Reserv** + operator code
Broadcasting music on an external loud speaker	P.K.: **BkgMus**+ operator code
Attendant diversion	Automatic, by scheduling or P.K.: **NRMode** when installation is in "Normal" mode + operator code or P.K.: **Attendant diversion** + destination if necessary + operator code

3.42.3.2 CANCELLATION

By switching to normal mode	When the system is in restricted mode, P.K.: **NRMode** + operator code
Reservation of last trunk group	P.K.: **Reserv** + operator code
Broadcasting music on an external loud speaker	P.K.: **BkgMus**+ operator code
Attendant diversion	Depending on activation mode: Automatic, by scheduling or P.K.: **NRMode** when installation is in "Restricted" mode + operator code or P.K.: **Attendant diversion** + operator code

3.43 Specific Features of SO Stations

3.43.1 Overview

3.43.1.1 DESCRIPTION

The PCX provides the following services for S0 stations:

- suspension, which consists in suspending an internal or external call in progress on a

basic access and picking it up later from the same S0 station relocated on the basic access or another S0 station connected to the same basic access. The call can be identified by a code before being suspended. This code is used to locate the call.

- call waiting, which enables an S0 station to be informed that an external call is intended for it even if no B channel is available on its basic access. The S0 station can ignore, reject or accept the call.
- malicious call identification subscription so that the network carrier can be asked to record the caller's identity during the call or for a programmed time after hanging up.
- forwarding of calls on no answer, enables the internal and/or external calls to be routed to the programmed destination.

Note:

The SO supplementary services are not supported.

3.43.1.2 ADDITIONAL INFORMATION

- A call which is suspended and not retrieved after expiration of the suspension time-out is released if internal and re-routed to the general level (see "Attendant Stations") if external.
- A user cannot suspend a call if he or she already has a party on hold.
- The user who suspended a call is charged for the entire call, before suspension and after retrieval.
- The number of calls suspended simultaneously is limited and depends on the size of the cabinet.
- Call waiting on an S0 station is limited by a non-modifiable time-out.
- The number of calls waiting on the same access is limited to 2.
- Malicious call identification cannot be requested after a call transfer or suspension.
- The user is informed by the network of the reason for the rejection of a malicious call identification request.
- Apart from the caller's identity, the network records the time of identification request activation and the number dialled by the caller.
- Multiple directory numbers: when an S0 option (digital stations) is initialized, the system assigns 1, 2 or 3 directory numbers, depending on the country. With OMC, you can:
  - add users for the S0 option (individually or in groups), up to the system capacity. There is no automatic renumbering after adding users, so the installer should be careful to preserve the coherence of the numbering plan.
  - delete individual users (Note: the primary user of an option cannot be deleted separately; deleting the first user deletes all the other users of the same option).

3.43.2 Configuration procedure

3.43.2.1 CONFIGURATION

- To modify the default maximum suspension time-out – OMC (Expert View) only:

System Miscellaneous -> Feature Design -> Part 3 -> "Suspension"

- To authorize or inhibit camp-on on S0 stations – OMC (Expert View) only:

System Miscellaneous -> Feature Design -> "Call Waiting/Automatic camp-on"

- To modify the maximum time-out, after going on hook, for requesting recording of the caller's identity – OMC (Expert View) only:

External Lines -> Protocols -> ISDN Trunk -> Layer 3 -> "T305 Disconnect Supervision"

3.43.3 Operation

3.43.3.1 ACTIVATION/USE

Activation of the various services depends on the S0 station ; refer to the station user guide.

3.43.3.2 cancellation

Cancellation of the various services depends on the S0 station; refer to the station user guide.

3.44 Priority Calls

3.44.1 Overview

3.44.1.1 DESCRIPTION

2 types of priority call can be made:

- a call from a bank alarm system
- a voice call (or a call through a preprogrammed key)

Call from a bank alarm system (automatic call)

The bank alarm device is connected to the PCX by means of an SLI-board Z interface.

The call is triggered by the analog (Z) user going off-hook.

The external destination is called using a system speed dial number. The call is subject to checks on restriction and traffic sharing link COS as well as system speed dial rights (see "Link Classes Of Service").

The call takes priority over ordinary calls in progress. If all lines are busy, the system releases an ordinary call in order to set up a priority call.

Call from a programmed key (manual call)

The call destination (collective speed dial number or external number) is associated with a programmed key on a terminal.

Priority levels are defined to ensure that an automatic or manual call cannot cut off a higher-level call.

3.44.1.2 ADDITIONAL INFORMATION

- The bank alarm device cannot be connected to a Z interface behind a digital station.
- Several priority calls can be set up simultaneously
- A priority call may fail if the public exchange is saturated, if the destination is busy or if it

collides with an incoming call during the "setup" phase.

- The event "R_PRIORITY_CALL" – specifying the number of the station on which the call was released – is generated in the PCX history table whenever a call is released to make way for a priority call.
- The bank alarm device's directory number cannot be a private one.
- To avoid the system releasing a basic call on a B channel belonging to the trunk group assigned to the bank alarm device, when a B channel is free in another trunk group, it is advisable to configure all the accesses on a single trunk group.
- All calls made from an S0 terminal are considered as priority calls if a priority level >0 is defined

3.44.2 Configuration procedure

3.44.2.1 CONFIGURATION

- To declare the bank alarm system:

• by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Misc.** -> **"Special Function = Bank Alarm"** • by MMC-Station: **Subscr** -> **SpeDev** -> **Choice** -> **Bank Alarm**

- Define whether the call is a hotline call or normal:

• by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Misc.** -> **"Hotline"** • by MMC-Station: **Subscr** -> **AutoCa** -> **Active**

- Define the destination for the automatic call:

• by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Misc.** -> **"Hotline"** -> **"Destination n#"** • by MMC-Station: **Subscr** -> **AutoCa** -> **Desti**

- To activate or inhibit metering:

• by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Metering**

- Modify the bank alarm device's default speed dial rights, if necessary:

• by OMC (Expert View): **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Collective Speed Dial**

- Modify the default barring link categories, if necessary:

- by OMC (Expert View):
  - for the bank alarm device: **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Barring**
  - for the trunk groups: **External Lines -> Trunk groups -> Details -> Link-Cat**
- by MMC-Station:
  - for the bank alarm device: **Subscr -> BarTyp**
  - for the trunk groups: **TrGp ->** Catego

- Modify the default traffic sharing link categories, if necessary:

- by OMC (Expert View):
  - for the users: **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Barring**
  - for the trunk groups: **External Lines -> Trunk groups -> Details -> Link-Cat.**
- by MMC-Station:
  - for the users: **Subscr -> BarTyp (last 2 values)**
  - for the trunk groups: **TrGp ->** Catego (last 2 values)

- To create a priority call key:

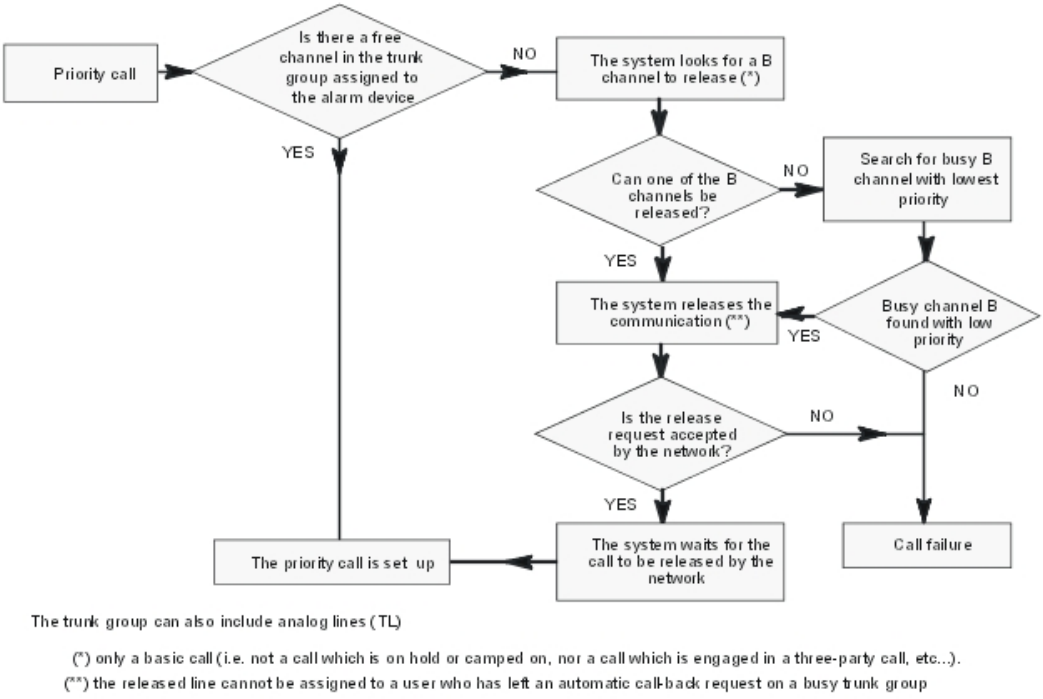
- by OMC (Expert View): **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Keys = Priority Call**
- by MMC-Station: **Subscr -> Keys**

- Define the priority level (0 to 7 with 7 = highest priority):

- by OMC (Expert View): **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Misc.**
- by MMC-Station: **Subscr -> Prio**

3.44.3 Operation

3.44.3.1 PRIORITY CALL MADE BY A USER



3.45 Multi-sets

3.45.1 Overview

3.45.1.1 Description

Multi-set is a powerful and useful feature that allows up to three telephones to share a common directory number and the same user services within Alcatel-Lucent OmniPCX Office Communication Server. A multi-set can include fixed and/or mobile phones.

A multi-set comprises a primary phone and either one or two secondary phones:

- The multi-set adopts the directory number and configured features of the primary phone.
- The secondary phones are known through the multi-set directory number, but can still be reached individually through their own directory numbers.

Therefore, a call to the multi-set number causes the primary and secondary phones to ring (but a call to a secondary's own directory number only causes the relevant secondary phone to ring).

More specifically, a multi-set is characterised by the following properties:

- All phones in the multi-set share the same directory number (that of the primary).
- All phones in the multi-set share the same voice-mail box and voice-mail functions.
- The user has access to the same phone services from all phones in the multi-set.
- The management of the engaged status is common to all phones in the multi-set (when

one phone is engaged, the others are also considered engaged, when contacted through the multi-set number).

The basic concept of a multi-set is illustrated in the figure below.

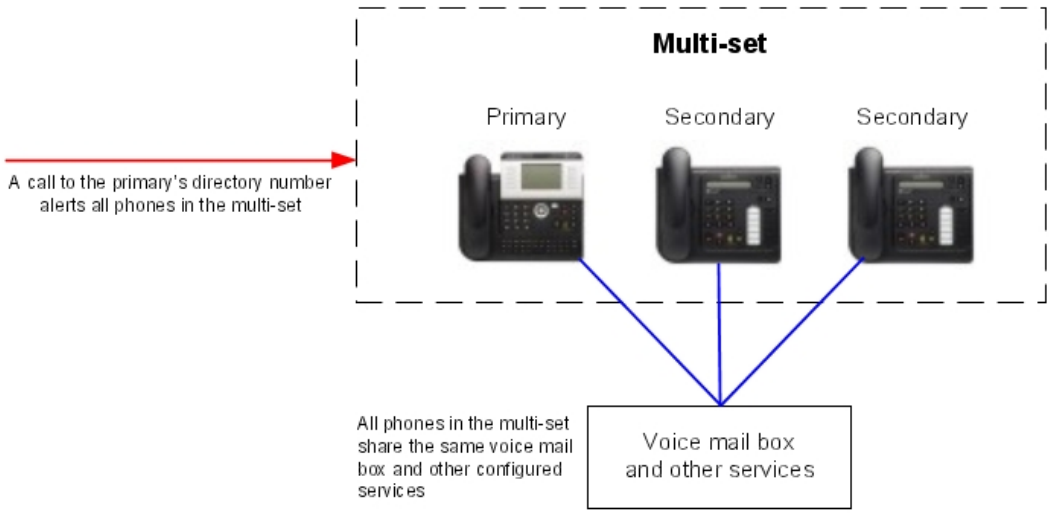


Figure 3.28 : Concept of a multi-set

3.45.2 Configuration procedure

3.45.2.1 Multi-set creation

A multi-set can be configured from the OMC tool of Alcatel-Lucent OmniPCX Office Communication Server. This procedure requires you to:

- choose the primary phone of the multi-set by its directory number
- add one or two secondary phones into the multi-set, specified by their own directory numbers.

Once you have configured the multi-set in this way:

- The secondary set(s) will adopt the directory number, mailboxes and characteristics (features, barring, dynamic routing, password, diversions, etc) of the primary phone.
- The voice and text mailboxes of each secondary set will be deleted.

The properties of the primary phone are not affected.

Note:

Secondary phones can also be removed from a multi-set during this configuration. The secondary phone is then reset and returns to its default configuration.

3.45.2.2 Multi-set restrictions

Note the following restrictions in configuring a multi-set:

- A maximum of 2 secondary phones can be used (giving a maximum of 3 phones in a multi-set).

- An individual phone (primary or secondary) can be included in only one multi-set.
- A multi-set cannot be included in a hotel PCX.
- A multi-set cannot be used as an ACD (Automated Call Distribution) agent or supervisor.
- A multi-set cannot be a member of an attendant group.

3.45.2.3 Busy ring configuration

When at least one of the phones of a multi-set is busy, the arrival of a new call may be indicated on an idle phone of the multi-set by a specific ringing signal. There are three ringing possibilities which can be configured by setting the parameter MLTSETRING in the OMC tool of Alcatel-Lucent OmniPCX Office Communication Server (within **Other labels** under **Menu Memory Read/Write**):

- MLTSETRING=01: no ring
- MLTSETRING=02 (default value): short ringing (two beeps followed by a long silence)
- MLTSETRING=03: normal ringing (as appropriate for an external or internal call)

Note:

If the secondary set of a multi-set is a GAP handset, the following restrictions must be taken into account:

- ***When the GAP handset is registered in BASIC mode:***
  The flag MLTSETRING has no effect on this set. In this case, if the primary set is busy when a call to the multi-set is received, the GAP handset rings and the call is presented on its display.
- ***When the GAP handset is registered in ENHANCED mode:***
  - *If the flag MLTSETRING is set to 01 and the primary set is busy when a call to the multi-set is received, the GAP handset does not ring and the call is not presented on its display.*
  - *If the flag MLTSETRING is set to 00 or 02 and the primary set is busy when a call to the multi-set is received, the GAP handset rings and the call is presented on its display.*

3.45.3 Operation

3.45.3.1 Introduction

The operation of a multi-set is described below in terms of:

- multi-set functions
- multi-set busy states
- multi-set call presentation (alerting)

3.45.3.2 Multi-set functions

The multi-set functions and their configuration are divided into three groups, as described in the table below.

table 3.236 : Multi-set functions

Group	Functions	Comments
1. Functions common to all sets (see § below)	Password Language Feature rights Dynamic routing Personal assistant Barring, traffic sharing Collective speed dial rights	The multi-set inherits these function settings from the primary phone. They are then shared by all phones in the multi-set. Those functions that can be modified at phone level can be configured from the primary or secondary phones. Those functions that can be modified from the OMC tool can also be modified from the primary phone but not from a secondary phone.
2. Feature activation functions (see § below)	Voice mailbox Text mailbox Diversion Selective diversion Appointment Callback Hunting group Pick-up group Broadcast group	These functions can mostly be enabled/disabled from any of the multi-set phones. Note that a multi-set cannot be a member of an attendant group.
3. Specific multi-set functions (see § below)	Multi-set alerting multi-set busy status	

These function groups are described in detail in the tables below.

table 3.237 : Functions common to all sets

Function	Description	Comments/Restrictions
Password	All phones in the multi-set share the same password, which is the password of the primary phone when the multi-set was created.	The password can be changed from any phone (primary or secondary) in the multi-set.
Language	The language is common to all phones in the multi-set and corresponds to the language of the voice mail box. Cyrillic font display is only supported if the phone supports Cyrillic, otherwise the phone displays in its default language.	The language can be changed from any phone (primary or secondary) in the multi-set.
Feature rights	All phones in the multi-set share the same feature rights, which are the feature rights of the primary phone when the multi-set was created.	Feature rights can only be modified by the OMC tool.

Dynamic routing	The dynamic routing of a multi-set is defined by the primary phone's dynamic routing configuration.	When a call to a multi-set is diverted to a phone outside the multi-set, the multi-set directory number is displayed on the destination phone along with the caller's number. A call to a secondary's own directory number is also diverted according to the dynamic routing of the primary, but the secondary's number is displayed on the destination phone along with the caller's number.
Personal assistant	All phones in the multi-set share the same personal assistant, which is the personal assistant of the primary phone.	The personal assistant can be configured and activated/deactivated from any phone (primary or secondary) in the multi-set.
Barring, traffic sharing and collective speed dial rights	All phones in the multi-set share the same settings for barring, traffic sharing and collective speed dial rights. These are the settings of the primary phone.	These settings can only be modified by the OMC tool.

table 3.238 : Feature activation functions

Function	**Description**	**Comments/Restrictions**
Voice mailbox	All phones in the multi-set share the same voice mailbox, which is the mailbox of the primary phone. Therefore, all phones are notified of a change of status of the voice mailbox (message waiting indicator). The language of the voice mailbox is that of the primary phone. The voice mailbox of a secondary phone is removed when it is associated with a multi-set. When a secondary phone's own directory number is called, it is the voice mailbox of the multi-set that is reached.	All operations on the voice mailbox can be performed from any phone of the multi-set, except voice mail screening which can only be done from the primary.
Text mailbox	All phones in the multi-set share the same text mailbox. Therefore, all phones (with a display) are notified of a change of status in the text mailbox (message waiting indicator). When a secondary phone sends a text message, the called party notes the message as arriving from the multi-set directory number (rather than the secondary's own number).	When a text message is received by a multi-set, only phones with a display will be notified. In addition, when a text message is sent to a secondary phone's own directory number, if the secondary has no display the message notification will appear on the other multi-set phones.

Diversion	Call diversion for a multi-set operates in the same way as for a standalone phone. A call to the multi-set directory number or to a secondary's own directory number is diverted to another destination. Note that a call to the multi-set directory number can be diverted to a multi-set secondary phone. Also, a call to a secondary phone's own directory number can be diverted to the multi-set directory number.	Activation and deactivation of call diversion can be performed on any multi-set phone. However, a configuration change can only be performed by the OMC tool or the primary phone.
Appointment	An appointment reminder is notified to every phone in a multi-set.	Appointment activation and deactivation can be performed from any phone in a multi-set.
Callback	This is the "Booking on Engaged" feature which, if activated, allows a caller reaching an engaged multi-set to request an automatic callback when the multi-set becomes idle again (all phones free). That is, the caller is automatically called back by the system.	The "Booking on Engaged" feature can be activated for the multi-set as a whole. In this case, only one callback request can be stored. Alternatively, the feature can be activated for each individual phone in a multi-set. This allows up to three callback requests to be stored (one on each phone). A callback can then be performed as soon as the relevant phone becomes free (rather than when the whole multi-set becomes free).
Hunting group	A multi-set can be included as a single member of a hunting group. This can be a parallel, sequential or cyclic group.	When a hunting group call reaches a multi-set, the call is managed within the multi-set according to the multi-set call presentation rules.
Pick-up group	A multi-set can be a member of a pick-up group, with the following rules: - The primary or a secondary in the multi-set can answer a call to any other set in the pick-up group. - Any set in the pick-up group can answer a call to the multi-set (primary's directory number). - When a secondary is called on its own directory number, no other member of the pick-up group can answer the call.	If only a secondary of a multi-set is registered in a pick-up group, any other phone in the pick-up group can answer a call to the secondary's own number or to the multi-set (primary's directory number).
Broadcast group	A multi-set's directory number can be included in a broadcast group, but only the primary phone will ring.	If a secondary phone is to be a member of a broadcast group, its own directory number must be specifically included.

Redial	The same list of redial numbers is shared by all phones in a multi-set (according to the type of phone).	Some phones only support the last number dialled.
Manager/secretary	Manager and secretary phones can be included in a multi-set. A call to the manager or secretary through filtering is distributed to all phones in the multi-set.	Activation, deactivation and monitoring can only be performed by the primary in the multi-set.
Call park	This feature operates as for a standalone phone.	A call parked by a secondary phone can be retrieved from any phone with either the directory number of the primary or the directory number of the same secondary phone.

table 3.239 : Specific multi-set functions

Function	Description	Comments/Restrictions
multi-set busy status	A phone in a multi-set can be idle or in one of two busy statuses. The combination of statuses of the primary and secondary phones determines the overall status of the multi-set and whether a call can get through.	Details of the multi-set busy statuses are provided in § Multi-set engaged status .
Multi-set alerting	Phones in a multi-set are alerted to an incoming call according to the engaged status of the phones in the multi-set.	Details of multi-set alerting are provided in § Multi-set display of incoming calls .

3.45.3.3 *Multi-set engaged status*

When a call arrives for a multi-set, the status of the multi-set must first be determined in order to establish whether the call can be taken and how the call will be displayed (see § Multi-set display of incoming calls).

The status of each phone can be either:

- **IDLE:** Not in use.
- **ENGAGED 1:** In use, but can still receive an incoming call.
- **ENGAGED 2:** In use and cannot receive an incoming call.

The multi-set also adopts one of these statuses according to the statuses of the constituent primary and secondary phones. This dependency is summarised in the table below which shows the multi-set status for the different combinations of primary and secondary statuses.

Secondary statuses	Primary statuses		
	IDLE:	ENGAGED 1	ENGAGED 2
IDLE:	IDLE:	ENGAGED 1	ENGAGED 2
ENGAGED 1	ENGAGED 1	ENGAGED 1	ENGAGED 2
ENGAGED 2	ENGAGED 2	ENGAGED 1	ENGAGED 2

3.45.3.4 Multi-set display of incoming calls

When all phones in a multi-set are idle, an incoming call will be indicated on all phones with the normal ring tone for the call type (external or internal). However, when at least one of the phones is engaged, an idle phone may be alerted with a specific ring tone; this helps to notify users that one phone of the multi-set is already in use. The possible ring tones that can be configured for the engaged status are:

- normal ring (as appropriate for an external or internal call)
- short ring (two beeps followed by a long silence)
- no ring

Note:
If an external call is not answered, a call waiting notification is received in the text mailbox of the multi-set.

The display of incoming calls on the phones in a multi-set are summarised in the table below.

Secondary statuses	**Primary statuses**		
	IDLE:	**ENGAGED 1**	**ENGAGED 2**
IDLE:	PRIMARY: normal ring SECONDARY: normal ring	PRIMARY: call waiting notification SECONDARY: normal/short/no ring	PRIMARY: no ring SECONDARY: no ring
ENGAGED 1	PRIMARY: normal/short/no ring SECONDARY: call waiting notification	PRIMARY: call waiting notification SECONDARY: call waiting notification	PRIMARY: no ring SECONDARY: no ring
ENGAGED 2	PRIMARY: no ring SECONDARY: no ring	PRIMARY: call waiting notification SECONDARY: no ring	PRIMARY: no ring SECONDARY: no ring

In addition, the following alerting behaviours should be noted:

- If an engaged phone returns to the idle status and there is a call waiting on the multi-set, this phone is alerted with the normal ring.
- When the primary phone is out-of-service or in the customisation mode, the secondary phones ring as normal.
- When the primary phone calls the multi-set directory number, only the secondary phones are alerted.
- When a secondary phone calls the multi-set directory number, all phones in the multi-set are alerted except the initiating phone.
- When call diversion is configured within a multi-set (secondary to primary, primary to secondary, or secondary to secondary), only the destination phone is alerted when the multi-set is called.

3.46 Manager/Secretary Screening

3.46.1 Overview

3.46.1.1 DESCRIPTION

The system can be used to create relations between manager-secretary stations so that the "secretary" station can screen calls intended for the "manager" station, in other words, answer calls intended for the manager station and then put the correspondents through if necessary.

In a manager-secretary relation, the "secretary station" can be a Hunting Group (see "Hunting Groups").

All the stations in a manager-secretary relation must be multiline.

3.46.1.2 ADDITIONAL INFORMATION

- In order to differentiate between screened calls and direct calls to the secretary station:
  - create a second directory number for the secretary
  - program the screening with this second directory number
  - create, on the secretary station, an RSD resource key programmed with this second number in order to receive the screened calls there
- A secretary station can belong to several manager-secretary relations: the secretary station then has a filter key (also on the corresponding manager's station) and an RSL key for each manager station.
- A manager station can belong to several manager-secretary relations: the manager station then has, for each secretary station, a filter key (also on each secretary station) and an RSL key.
- When the secretary station in a manager-secretary relation is a Hunting Group, the manager station has a single filter key but as many RSL keys as there are members in the group.
- Any activation of individual forwarding on the secretary station or the manager station cancels and replaces the previously active screening.
- Any request for activation of screening is rejected on a secretary station which has already activated individual call forwarding.

3.46.2 Configuration procedure

3.46.2.1 CONFIGURATION

- To create the manager-secretary relations:

• by OMC (Expert View): **Manager-secretary Relations** • by MMC-Station: **TerPro -> MgrSec**

- For each station, authorize the type of calls (local, external, or both) to be screened:

- by OMC: **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Dyn. Rout. -> "Diversion Apply"**
- by MMC-Station: **Subscr -> DynRou**.

3.46.3 Operation

3.46.3.1 ACTIVATION/USE

P.K.: Programmed Key – defined using OMC (Expert View) or MMC-Station

Type of station / Service	**Monoline**	**Multiline without soft keys**	**With soft keys**
By the manager or secretary station	--	P.K.: **Screening**	P.K.: **Filter**

3.46.3.2 cancellation

Type of station / Service	**Monoline**	**Multiline without soft keys**	**With soft keys**
By the manager or secretary station	--	P.K.: **Screening**	S.K.: **Filter**

3.47 Forwarding to Voice Mail Unit

3.47.1 Overview

3.47.1.1 DESCRIPTION

Users can activate unconditional call forwarding or forwarding on busy for their own calls (see "Forwarding"), diverting them to the integrated Voice Mail Unit.

If the Voice Mail Unit is configured as an answering device, the callers can leave a spoken message.

3.47.1.2 ADDITIONAL INFORMATION

For more details on the Alcatel-Lucent OmniPCX Office Communication Server integrated Voice Mail Unit, see "Integrated Voice Mail Unit".

Alcatel-Lucent OmniPCX Office Communication Server also provides the facility to manually transfer an answered call to the voice mailbox of a third party. For more information on this, see "Transferring to Voice Mail of Third Party".

3.47.2 Configuration procedure

3.47.2.1 CONFIGURATION

- Select the type of calls (internal, external, or both) to be forwarded:

- by OMC (Expert View): **Users/Base stations List -> Users/Base stations List -> Details -> Dyn. Rout. -> "Diversion Apply"**
- by MMC-Station: **User or Subscr -> DynRou -> "Div"**

- For each station, program the forwarding keys:

- by OMC (Expert View): **Users/Base stations List -> Users/Base stations List -> Details -> Keys**
- by MMC-Station: **User or Subscr -> Keys**

3.47.3 Operation

3.47.3.1 ACTIVATION/USE

P.K.: Programmed Key

F.K.: Fixed Key

S.K.: Soft Key

Prefix: Code programmed in the internal dialling plan

Type of station / Service	**Analogue (Z)**	**Without display**	**With display, no S.K.s**	**With soft keys**
Immediate forwarding of personal calls to voice mail unit (VMU)	Prefix **Immediate call forwarding of personal calls** + function code **Voice Mail**	F.K.: **Divert** or (pre-)programmed **(Master) indiv. immediate forwarding** + P.K.: **Voice mail unit**	F.K.: **Divert** or (pre-)programmed **M ImmD? or Immed?** (indiv.) + P.K.: **Voice mail unit**	S.K.: **Divert** + **Immed?** + P.K.: **Voice mail unit**
Forwarding on busy to voice mail unit (VMU)	Prefix **Forward on busy** + function code **Voice Mail**	P.K.: **Forward on busy (master)** + P.K.: **Voice mail unit**	P.K.: **Mbusy? or Busy?** + P.K.: **Voice mail unit**	S.K.: **Divert** + **Busy?** + P.K.: **Voice mail unit**
Message present	Specific voice prompt + Specific dailtone + LED on Reflexes without display		Flashing of 3-colour LED and icon corresponding to F.K.: **Mail**	
Access voice mail	Prefix **access voice mail**	P.K.: **Access voice mail**	F.K.: **Message** + 1	F.K.: **Mail** + S.K.: **Voice**

3.47.3.2 CANCELLATION

P.K.: Programmed Key

F.K.: Fixed Key

S.K.: Soft Key

Prefix: Code programmed in the internal dialling plan

Type of station / Type of forwarding	**All stations including analogue (Z)**	**Without display ? Analogue (Z)**	**With display, no soft keys**	**With soft keys**
"Immediate" or "On busy"	Prefix **Cancel all forwardings**	P.K.: **Cancel all forwardings**	P.K.: **All**	S.K.: **Divert** + **Cancl?**

3.48 Transferring to Voice Mail of Third Party

3.48.1 Overview

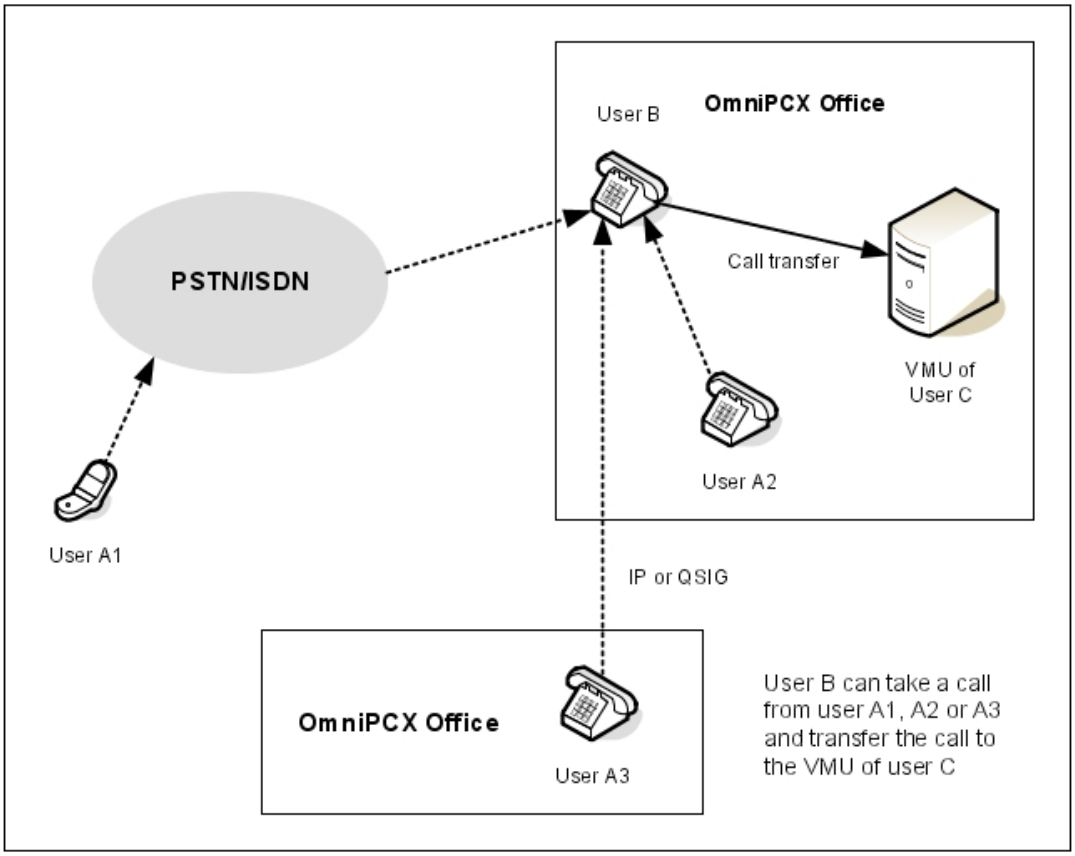
3.48.1.1 Introduction

This feature (Transfer to VMU) allows an incoming call to a subscriber's phone set to be transferred to another subscriber's Voice Mail Unit (VMU). The process is not automatic - the call must first be answered and then manually transferred to the third party VMU.

The third party must be an internal subscriber (in the same OmniPCX Office system as the phone set performing the transfer), but the caller can be any one of:

- an internal subscriber
- a subscriber on another OmniPCX Office system connected via IP or QSIG
- an external caller on PSTN or ISDN

This is illustrated in the figure below.



The transfer can be performed on the answering party's phone set using a special feature code, or using a user-programmable key or softkey (if either is supported by the phone set). For the transfer to be implemented on an individual phone set, the feature must first be enabled in the OMC tool.

3.48.2 Operation

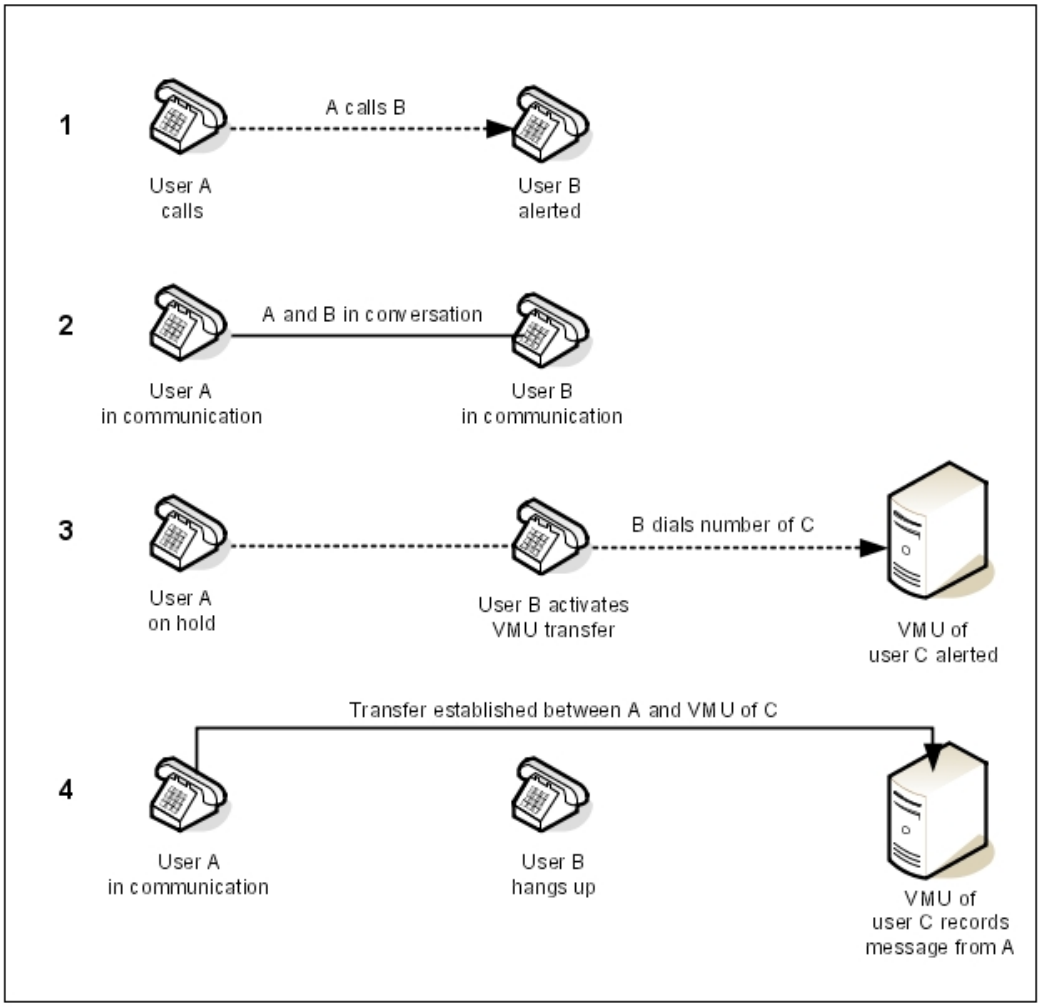
The operation of the "Transfer to VMU" feature is described below for two cases: basic "single call" and "multi-call".

3.48.2.1 Basic operation (single call)

This section describes the basic operation of the "Transfer to VMU" function, first providing an overview of the transfer process and then the required key sequence. It assumes that the incoming call (which requires the transfer) is the only active call being handled by the receiving phone set.

3.48.2.1.1 Transfer process

The figure below illustrates the basic transfer process starting with an idle phone receiving an incoming call that must be transferred to to the VMU of another subscriber in the system.



3.48.2.1.2 Key sequence

The "Transfer to VMU" function can be performed on a phone set using any of the following methods:

- **Feature code**: Defined in the OMC tool (see "Configuration Procedure") and can be used on all phones in the system
- **User Programmable Key (UPK)**: Can be used on those phones that support UPKs and for which the "Transfer to VMU" function has been enabled in the OMC tool (see "Configuration Procedure").
- **Softkey**: Can be used on phones that provide softkeys.

The required key sequences for these cases are described in the procedure below.

1. Once the incoming call (that requires the transfer) has been answered, activate the transfer function by:

- entering the required feature code on the phone's keypad, or

- pressing the UPK corresponding to the transfer function (for phones that support UPKs), or
- pressing the softkey for the transfer function (accessed by scrolling in the conversation menu on phones that provide softkeys).

2. When asked to dial, enter the extension number of the subscriber whose VMU you want to reach.

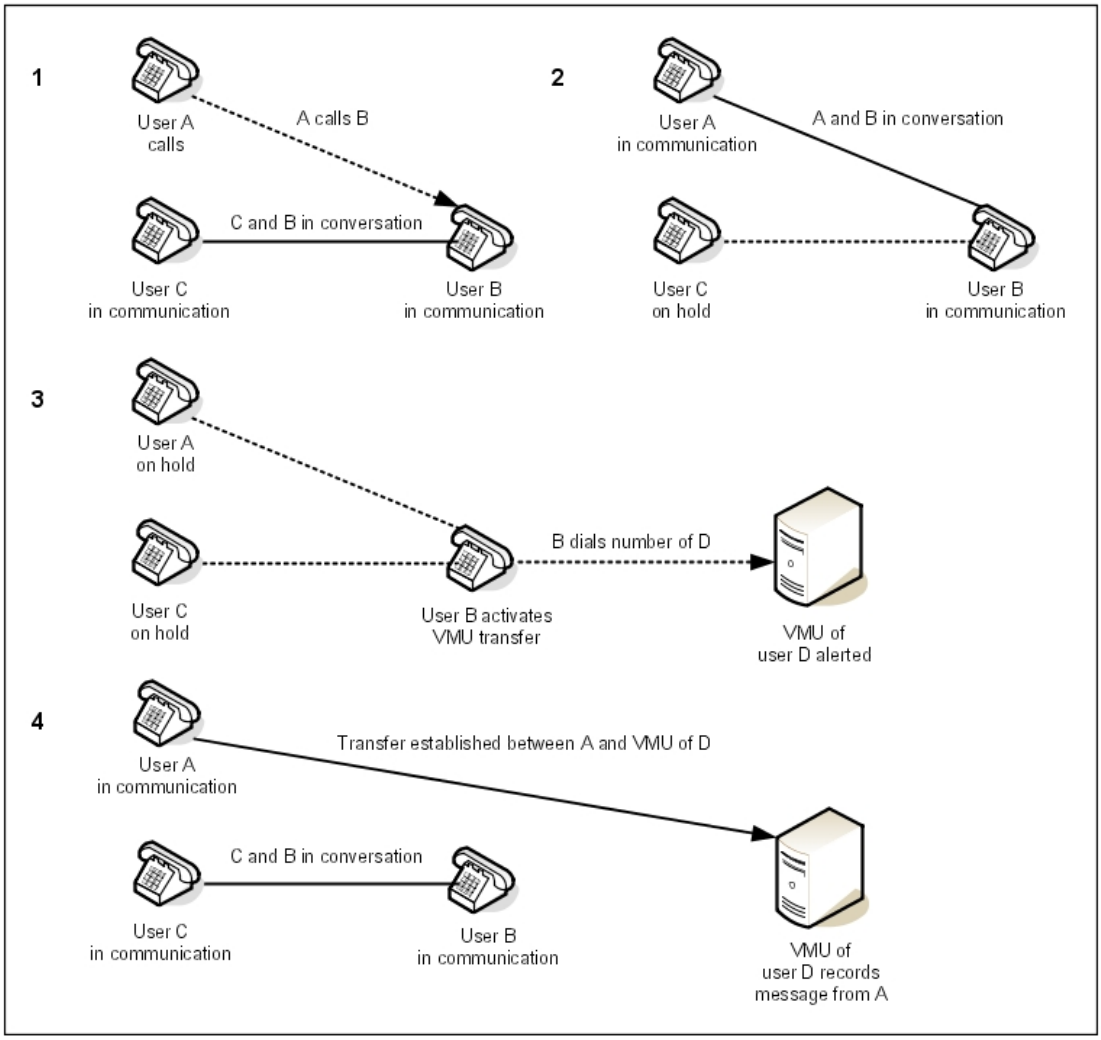
3. This step depends on the success of the connection to the required VMU:

- If the extension number is recognised and the corresponding VMU is accessible, the name of the relevant voice mail hunting group is displayed, along with a message to say that the VMU has been alerted. When the system displays a message confirming that the transfer has been accepted, you are returned to idle and can hang up.
- If the extension number is an external number or a number on another system, the transfer is rejected and you are returned to the caller.
- If the extension number does not exist or is not available, the default mailbox function of the automated attendant is called. In this case, you are returned to idle and can hang up.

3.48.2.2 Multi-call operation

This section provides an overview of the "Transfer to VMU" function in the multi-call case. It is assumed that the phone set receiving the incoming call (which requires the transfer) is already handling a conversation with another caller.

The figure below illustrates the transfer process in the multi-call case, where B is in conversation with C when a call arrives from A requiring B to transfer the call to the VMU of D.



3.48.3 Configuration procedure

3.48.3.1 Configuration

There are three ways in which the "Transfer to VMU" feature can be implemented, depending on the type of phone set used:

- by feature code (all phone sets)
- by User Programmable Key [UPK] (if supported by the phone set)
- by a softkey (if supported by the phone set)

The feature code and UPK methods require some initial configuration in the OMC tool to enable them (while the softkey method is available without configuration on phones that support it). The required configuration procedures are provided in the sections below.

3.48.3.1.1 Feature code

On all phones, the "Transfer to VMU" function can be performed for an incoming call using a numeric feature code. To use this feature, it must first be enabled (for all phones in the system) in the OMC tool, as follows:

1. In OMC, navigate down the path **Numbering > Features in Conversation**.
2. In the **Features in Conversation** screen, select the "Transfer to VMU" option in the **Function** field.
3. In both the **Start** and **End** fields, enter the numeric feature code that you wish to use for this function.
4. Click on the **Add** button and then on the **OK** button.

3.48.3.1.2 User Programmable Key (UPK):

On phone sets that support User Programmable Keys (UPKs), a dedicated key can be programmed to implement the "Transfer to VMU" function. To use the feature in this way (on a suitable phone), it must first be enabled (for the phone) in the OMC tool, as follows:

1. In OMC, navigate to the **Subscribers/Base stations List** screen.
2. In the list, identify the subscriber/base station (of a suitable type) for which the feature is to be enabled and double-click on it. This displays the **Subscriber** screen for the selected subscriber/base station.
3. Click on the **Keys** button. This displays the **Subscriber** screen for the selected subscriber/base station.
4. In the on-screen plan of the set's keypad, click on the key that you wish to programme with this function. This displays the **Individual Key Programming** screen for the selected key.
5. In the **Key Function** field, select the "Transfer to VMU" option.
6. If the phone set has a graphic display, enter a name for the key (such as "VMU transfer") in the **Key Label** field.
7. Click on the **OK** button.

3.49 SMS Transparency

3.49.1 Overview

3.49.1.1 Introduction

The SMS transparency feature of Alcatel-Lucent OmniPCX Office Communication Server allows suitable telephone sets within the system to send and receive SMS messages via the public telephone network. The basic requirements to be able to send and receive SMS messages are as follows:

- The Alcatel-Lucent OmniPCX Office Communication Server system must be connected to an SM-SC (Short Message Service Centre) on the public network.
- The telephone must be an SMS-enabled terminal.
- The subscriber must be authorised within the Alcatel-Lucent OmniPCX Office Communication Server system to send and receive SMS messages.

When enabled, the SMS transparency feature handles SMS messages in a way which

guarantees the transmission and reception of messages, and ensures compatibility with other system features.

3.49.1.2 Architecture

Normally, an SMS-enabled telephone connects to an SM-SC on the public telephone network in order to exchange an SMS message with another phone on the public network. For a telephone within the Alcatel-Lucent OmniPCX Office Communication Server system, a direct connection between the telephone and the SM-SC is not possible, since connections to the public network are made through the system PABX. Therefore, the PABX provides an interface to the SM-SC, and this connection to the SM-SC must be configured in the Alcatel-Lucent OmniPCX Office Communication Server system.

Note:

SMS messages are always sent via the public network, even messages exchanged between phones within the same Alcatel-Lucent OmniPCX Office Communication Server system.

SMS messages are transmitted in the normal voice band using in-band signalling. Alcatel-Lucent OmniPCX Office Communication Server can connect to an SM-SC using either of the ISDN and QSIG protocols (this is transparent - there is no need for any specific configuration or software variant). The exchange of SMS messages on analogue or IP trunks is not supported.

3.49.1.3 Hardware

The main hardware requirement is that a telephone authorised to send and receive SMS messages must be a suitable SMS-enabled terminal; that is, an analog terminal (Z terminal) or S0 ISDN terminal (or PC card) with SMS capability. More specifically:

- It must support the sending and receiving of SMS messages by means of a suitable man-machine interface (keyboard and display).
- It must have the CLI feature which enables the phone to detect, decode and process (for example, display) the Calling Line Identifier (CLI)

There is no restriction on the number of SMS-enabled analogue terminals or SMS-enabled S0 ISDN terminals amongst the terminals managed by the system.

An SM-SC number must be configured in each SMS-enabled telephone terminal and this number must contain the trunk prefix.

3.49.1.4 Operation

The roles of the Alcatel-Lucent OmniPCX Office Communication Server system in the transmission and reception of SMS messages are as follows:

- It provides a connection to one or more SM-SCs on the public network.
- It provides authorisations (through a barring table) for individual subscribers to send SMS messages.
- It identifies an outgoing SMS call, authorises its transmission and then protects the call.
- It identifies an incoming SMS call and then protects the call (if the destination terminal can be reached through a DDI number).

Protecting a call involves guaranteeing the bi-directional transparency of the channel for the duration of the call.

Note:

When the SMS transparency feature is disabled, the system does not disable the sending and receiving of SMS messages, but simply does not provide protection of SMS communications. SMS-enabled terminals can still send and receive SMS calls, but without a guarantee that the messages will get through.

For SMS call detection, the Alcatel-Lucent OmniPCX Office Communication Server system must be provided with a list of the available SM-SC numbers to allow it to identify that a call is coming from or going to an SM-SC. These numbers are provided inside a Noteworthy Address (SMSCNum) that can be set or changed using the OMC tool; two SM-SC outgoing numbers and two SM-SC incoming numbers can be defined.

The Alcatel-Lucent OmniPCX Office Communication Server system also performs other more specific call management roles, described in the next section.

3.49.1.5 Call management

The Alcatel-Lucent OmniPCX Office Communication Server system manages incoming and outgoing SMS messages in a way that ensures operational compatibility with other features of system. The main rules for the different features and terminal types are summarised in the table below.

<table>
<tr><td></td><td>Analogue Terminals</td><td>S0 ISDN Terminals</td></tr>
<tr><td>Call Waiting</td><td colspan="2">Call waiting is not implemented on an incoming call for a telephone terminal that is currently involved in an SMS call. The incoming call follows the normal call management rules that are applied when the telephone is busy (release, directed to attendant, etc). Since the average SMS communication takes only 8 seconds, this has little impact on the telephone service.</td></tr>
<tr><td>Call Diversion</td><td colspan="2">All types of diversion are bypassed for incoming SMS calls in order to avoid forwarding an SMS message to a terminal that is not SMS-enabled or not owned by the intended recipient of the message. The exception is that SMS call diversions configured locally on an S0 ISDN terminal are maintained.
More specifically:
- If call diversion is active for an SMS-enabled phone set (immediate diversion) and the set is free, an incoming SMS call does not follow the diversion but is delivered to the set as normal.
- If an SMS-enabled set is busy, with "diversion on busy" active, an incoming SMS call does not follow the diversion but is handled as described below for "Simultaneous Calls".</td></tr>
<tr><td rowspan="2">Simultaneous Calls</td><td>Although a telephone engaged in an audio communication cannot receive an incoming SMS message, it can still receive a notification of the SMS call (if configured).</td><td>An S0 ISDN terminal engaged in an audio communication can receive an incoming SMS message, since the two types of call can be handled on separate B-channels.</td></tr>
<tr><td colspan="2">For both types of terminal, an SMS call notification cannot be received if the telephone is engaged in another SMS call. In the case of an undelivered SMS message, once the telephone terminal has returned to idle, the message can be received if the terminal automatically calls back the SM-SC to retrieve the pending message or if the SM-SC attempts to redeliver the message (after a delay).</td></tr>
</table>

The table below describes how the management of SMS calls modifies the behaviour of other

features of the Alcatel-Lucent OmniPCX Office Communication Server system.

table 3.251 : Behaviour of Alcatel-Lucent OmniPCX Office Communication Server features for SMS calls

Feature	Behaviour
Group	If the destination number of an SMS call is a member of a group, the group rules no longer apply. The SMS message is delivered as for an incoming SMS call to an individual telephone terminal.
Pick-up	No pick-up is possible for an incoming SMS call.
Pre-announcements	Pre-announcement messages are not applicable to incoming SMS calls.
Selective monitoring	If a telephone terminal supports selective monitoring, incoming SMS calls are not presented on the supervisor set.
Subscriber monitoring	If a telephone terminal is subject to subscriber monitoring, incoming SMS calls are not reported to the monitoring set.
Voice mail/automated attendant	When a telephone terminal is busy, in the case of an incoming SMS call there is no immediate or dynamic forwarding to voice mail or to the automated attendant.

3.49.2 Configuration procedure

3.49.2.1 Overview

In order to use the SMS transparency feature of Alcatel-Lucent OmniPCX Office Communication Server, the following configuration steps must be performed.

On the telephone terminal

- The SMS feature must be activated on the phone.
- The phone terminal must be programmed with the directory number of the SM-SC (Short Message Service Centre) used for incoming SMS calls; this number is added after the main bundle number (e.g. 0).
- The phone terminal must be programmed with the CLI (Calling Line Identifier) of the SM-SC used for outgoing SMS calls; this number is added after the main bundle number (e.g. 0).

This configuration depends on the model of telephone terminal used. Consult your telephone's user documentation.

In the Alcatel-Lucent OmniPCX Office Communication Server system

- The directory numbers of the SM-SCs used for outgoing and incoming SMS calls must be specified (SMSCNum label; see next section).
- The authorised SMS-enabled telephones must be defined in the DDI numbering plan.
- The SMS-enabled telephones must be defined as CLASS terminals.
- The SMS transparency feature must be enabled at system level (SMSenabled label set to 01).

This configuration is performed using the OMC tool.

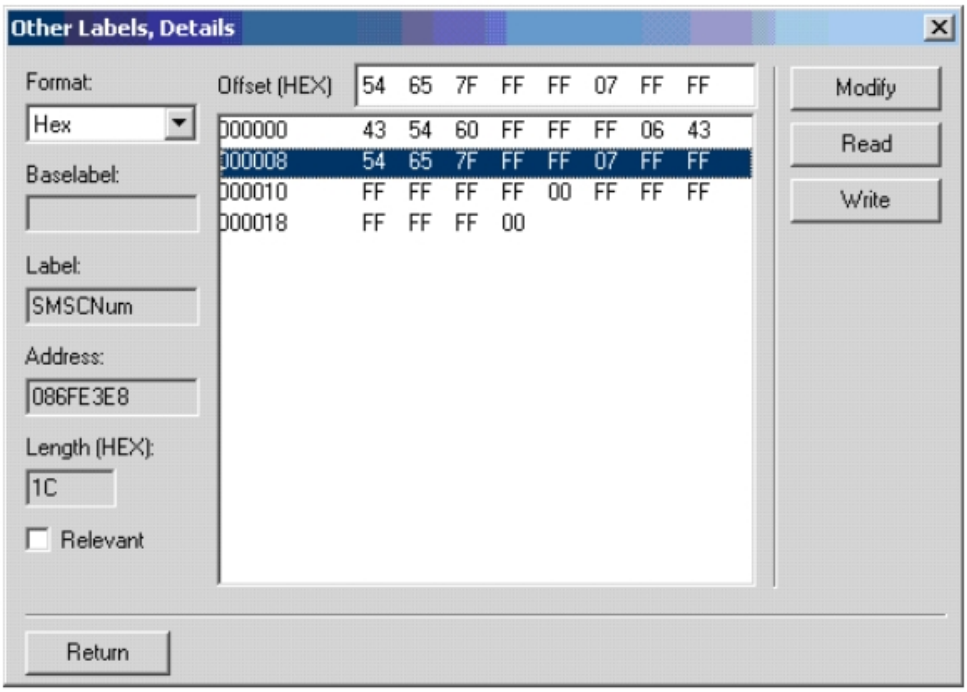
3.49.2.2 SMSCNum label

The SMSCNum label is a 28-byte flag which allows you to define SM-SCs phone numbers (i.e. public numbers without a PBX outgoing prefix).

With the OMC, you can configure 2 different SM-SC providers with two server phone numbers each:

- An incoming SM-SC server phone number: the public phone number of a server which sends SMS messages coming from analog sets via the Alcatel-Lucent OmniPCX Office Communication Server.
- An outgoing SM-SC server phone number: the public phone number of a server which sends the SMS messages to the analogue sets via the Alcatel-Lucent OmniPCX Office Communication Server.

Example of an SMSCNum label:



This figure gives the following information:

- First SM-SC provider:
  Bytes 1 to 6 indicate the SM-SC incoming server number: 43 54 60 FF FF (FF not significant)
  Byte 7 indicates the length of the SM-SC incoming server number: 6 digits
  Bytes 8 to 13 indicate the SM-SC outgoing server number: 43 54 65 7F FF
  Byte 14 indicates the length of the SM-SC outgoing server number: 7 digits
- Second SM-SC provider: (Not defined)
  Bytes 15 to 20 indicate the SM-SC incoming server number

Byte 21 indicates the length of the SM-SC incoming server number
Bytes 22 to 27 indicate the SM-SC outgoing server number
Byte 28 indicates the length of the SM-SC outgoing server number

Note:
If the incoming and outgoing SM-SC servers have the same public number, you must configure this phone number twice in the table.

To modify the SMSCNum label, follow the next procedure:

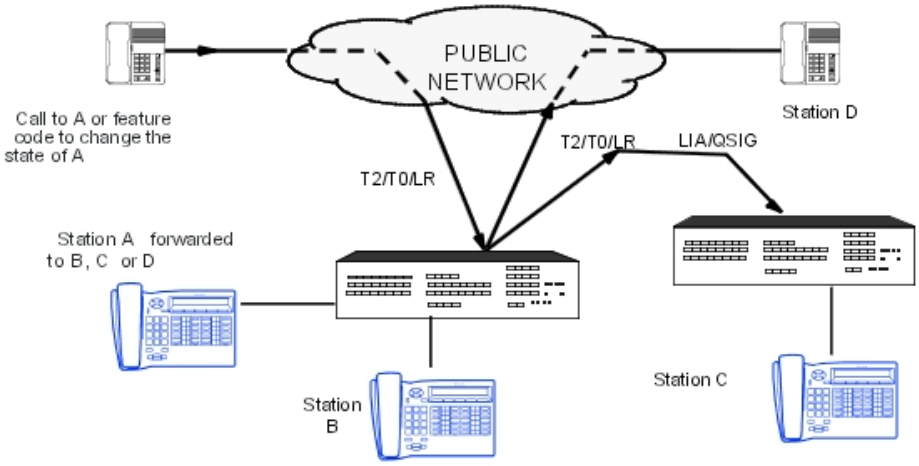
1. In the OMC tree view, expand the Customer PCX/System Miscellaneous/Memory Read/Write folder, and double-click on Other Labels.
2. In the list of other labels, select SMSCNum and click Details.
3. Select a line in the table and modify the desired byte(s).
4. Click Modify, then Write.
5. Select the Relevant check box to identify the labels that have been modified.
6. Click Return.

3.50 RemoteForwarding

3.50.1 Overview

3.50.1.1 DESCRIPTION

The **remote forwarding** service enables an employee who is outside of the business premises, or at home to modify or cancel, from a DTMF dialing set, the unconditional internal or external forwarding active on his station, as if he were at work.



3.50.1.2 ADDITIONAL INFORMATION

- The "Remote Forwarding" feature uses elements of the "Remote Substitution" and "External Forwarding" features; see both corresponding files.
- A single DTMF receiver is available at any given time.

- This service can be used to cancel the "Do Not Disturb (DND)" function.

3.50.2 Configuration procedure

3.50.2.1 CONFIGURATION

- For each set, to authorize or deny use of the "Remote Substitution" feature:

• by OMC (Expert View): **Subscribers/Basestations List** -> **Subscribers/Basestations List** -> **Details** -> **Features** -> **"Remote Substitution"**

- To validate the service in the public numbering plan (operates without base or NMT):

• by OMC (Expert View): **Numbering** -> **Public Numbering Plan** -> **Remote Substitution** • by MMC-Station: **NumPln** -> **PubNum** -> **Disa**

- To define the service access code – OMC (Expert View) only:

External Lines -> Remote substitution -> Access control code

- To define the voice guidance message (none, message 1 to 8) – OMC (expert View) only:

External Lines -> Remote Substitution -> Voice Guidance Message

- To define the system reaction if no DTMF receiver is available (Call Waiting or Release) – OMC (Expert View) only:

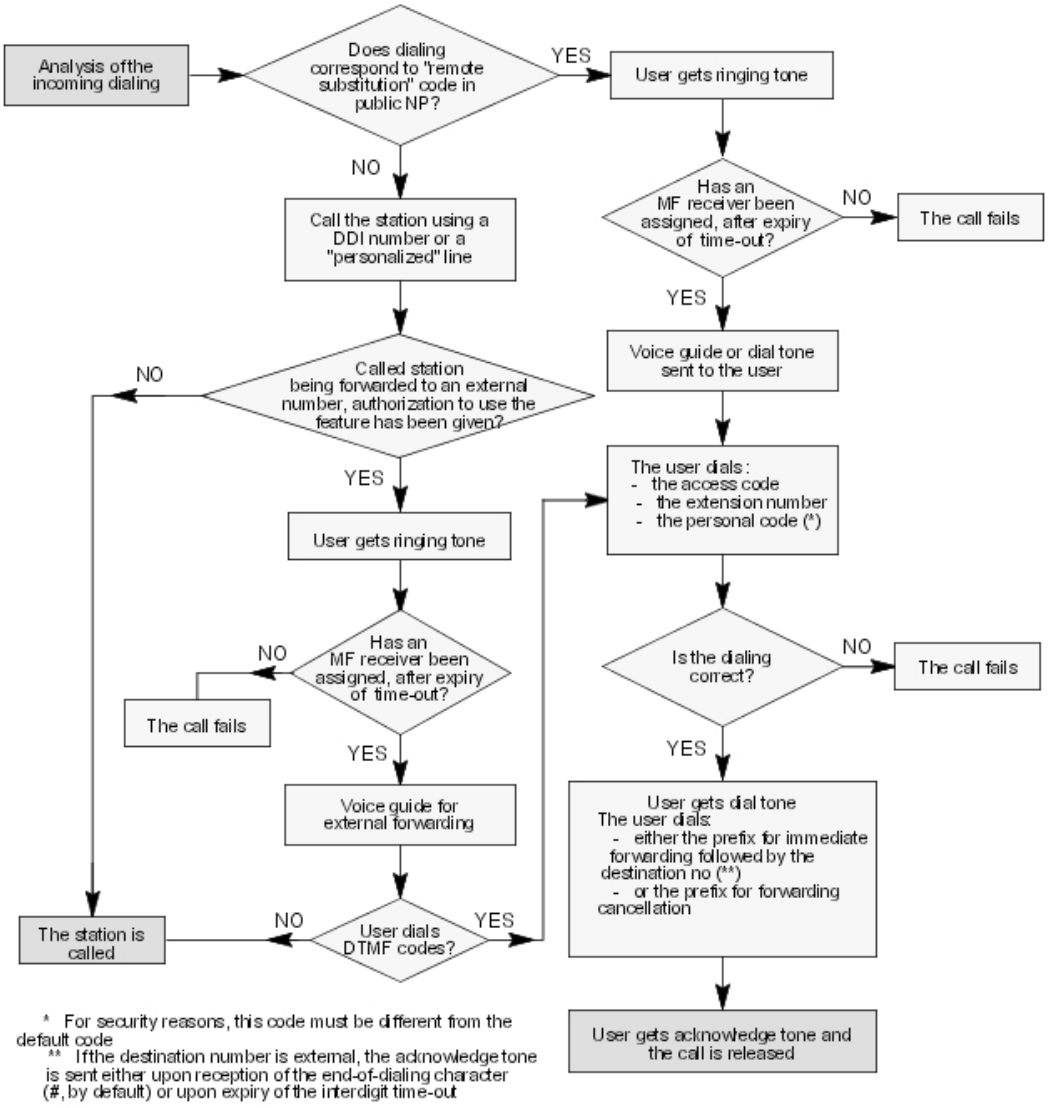
External Lines -> Remote Substitution -> Wait for DTMF Receiver

3.50.3 Operation

3.50.3.1 ACTIVATION/USE

Users can modify their station state remotely by:

- calling their station (necessarily in external forwarding mode). The user can then either **modify** the immediate forwarding destination number or **cancel** forwarding, or
- dialing the feature code for "remote substitution". The user can then **activate** immediate forwarding, **modify** the immediate forwarding destination number or **cancel** forwarding.



3.51 External Forwarding

3.51.1 Overview

3.51.1.1 DESCRIPTION

When external forwarding is activated on a station, its internal and external personal incoming calls are routed to a network destination, programmed in advance or at activation of the service.

For external incoming calls, the system can manage 2 types of external diversion:

- by joining: the incoming analog line (or B channel) is switched to the outgoing line (or B

channel) by the PCX, the latter handles the barring and traffic sharing link categories of the destination station and the lines to be joined (see "Link Categories") and subsequently the connectivity matrix. Both resources are busy during the entire duration of the call. This type of forwarding does not need a subscription..

- by re-routing, for ISDN DDI calls only, and on subscription from the network operator: the system informs the network that the station called is forwarded and specifies the destination. The network then manages the forwarding (no busy lines). The system takes account of the barring and traffic sharing link categories of the destination station and the trunk group programmed into the destination number.

For internal incoming calls, the system performs forwarding by joining.

3.51.1.2 ADDITIONAL INFORMATION

- Any activation of an individual forwarding supersedes the previous one.
- If the station which activates the forwarding has a display, it will show the forwarding and the Destination n#.
- The icon or LED associated with the "Forwarding selection" or "Master Forwarding" programmed key indicates activation of forwarding with this key.
- The "Master Forwarding" or "Forwarding Selection" programmed key for individual calls can also be used to cancel an external forwarding.
- When the link categories do not allow external forwarding:
  - an external caller is re-routed to the O.S.
  - an internal caller is released
- Two analog lines can only be joined if they are configured with Polarity Reversal and if the public exchange sends the corresponding IP.
- When a digital line (ISDN or SIG) is forwarded, it is possible to select which identity is retransmitted by the system to the forwarding destination, either that of the initial caller or that of the forwarded station.

• by OMC (Expert View): **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Features**

# CLI for external diversion # CLI is diverted party	= Identity of caller
# CLI for external diversion # CLI is diverted party	= Identity of forwarded station

- The caller can hear a pre-announcement message before being forwarded (see "Configuration").
- A private station can neither activate an external forwarding nor be forwarded externally.
- Neither the possible UUS nor the sub-address (see "ISDN Services") are retransmitted to the forwarding destination.
- External forwarding can not be activated with an account code.

3.51.2 Configuration procedure

3.51.2.1 CONFIGURATION

- For each station, program the forwarding keys:

• by OMC (Expert View): **Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Keys** • by MMC-Station: **Subscr -> Keys**

- For each station, external forwarding can be authorized:

• by OMC (Expert View): **Subscribers/Basestations List -> Subscribers/Basestations List -> Details - Features -> "External Diversion"**

- Define the type of mechanism used for forwarding an external incoming call to a network number, re-routing or joining:

• by OMC (Expert View): **System Miscellaneous -> Feature Design -> Part 2 -> "External Diversion Mode"** • by MMC-Station: **Global -> Joing -> Divert**

- When the selected mechanism for forwarding external incoming calls to a network number is "joining", fill out the connectivity matrix by OMC (Expert View) only:

Traffic Sharing and Barring -> Joining

- Define the type of identity retransmitted to the forwarding destination:

• by OMC (Expert View): **System Miscellaneous -> Feature Design ->"CLI for external diversion" or "CLI is diverted party"**

- To specify whether or not the caller hears a pre-announcement message before being forwarded – OMC (Expert View) only:

Subscribers Misc. -> Pre-announcement -> Voice Guidance for Diversion to External

3.51.3 Operation

3.51.3.1 ACTIVATION/USE

P.K.: Programmed Key

F.K.: Fixed Key

S.K.: Soft Key

Prefix: Code programmed in the internal numbering plan

Type of station / Service	All stations including Z	Without display (# Z)	With display, no soft keys	With soft keys
Immediate external forwarding	Code + Destination n# (*)	F.K.: **Divert** or (pre-)programmed **(master) indiv. immediate forwarding** + Destination n# (*)	F.K.: **Divert** or (pre-)programmed **M ImmD# or Immed**" (indiv.) + Destination n# (*)	S.K.: **Divert** + **Immed#** + Destination n# (*)

(*) If not a collective speed dial number, the external n# must contain a trunk group number or an RSP or RSB key

3.51.3.2 CANCELLATION

Type of station / Service	All stations including Z	Without display (# Z)	With display, no soft keys	With soft keys
Immediate external forwarding	Prefix **Cancel all forwardings**	P.K.: **Cancel all forwardings**	P.K.: **All**	S.K.: **Divert** + **Cancl#**

3.52 PCX Diversion

3.52.1 Overview

*3.52.1.1 PCX DIVERSION **

* Depending on country; not available in France.

3.52.1.1.1 DESCRIPTION

All the external calls from the digital network (T0 or T2 accesses) intended for the stations in the installation can be re-routed to a destination on the network.

First of all, the system manager will have subscribed to "Call Forwarding Unconditional" (CFU) with the network operator.

There are two subscription versions:

- **fixed** forwarding: the forwarding destination is programmed into the public exchange carrier and is always the same.
- **variable** forwarding: the forwarding destination is specified at activation of the service and can thus be different at each activation.

Note:

PCX forwarding by CFU is only possible with a point-to-point link (ETSI).

Access to the service is controlled by a password, either:

- in the public exchange: the password given by the exchange carrier is retransmitted to the public exchange on activation of forwarding.
- in the system: the password is that of the system operator and is not retransmitted to the public exchange.

To configure the service in the system (so that it correctly transmits the PCX forwarding activation request) the configuration in the public exchange must take account of the installation's digital links. These can be of 3 types:

- configuration of **type 0**: all the digital links connecting the installation to the public exchange are configured into a single "group" (equivalent to a trunk group) in the public exchange.
- configuration of **type 1**: the installation is connected to the public exchange by "groups" of links **and** isolated digital links.
- configuration of **type 2**: the installation is connected to the public exchange by several "groups" of digital links.

Depending on the type of configuration in the public exchange, it waits for one or more PCX forwarding activation requests:

- in a **type 0** configuration, a single activation request for the entire group of links
- in a **type 1** configuration, an activation request for each link connecting the installation to the exchange
- in a **type 2** configuration, an activation request for each group of links

The activation request is made via a trunk group containing one of the installation's digital links, defined either:

- on programming the "PCX diversion" key and, failing which, at the time of service activation, in a **type 0** configuration
- only if diversion is **variable**, at programming of the "PCX diversion" key and, failing which, at the time of service activation, in a **type 1 or 2** configuration
- only if diversion is **variable**, at programming the "PCX diversion" key and, failing which, at the time of service activation, in a **type 2** configuration; However, in this type of configuration, the system will not use this trunk group, but that programmed in address "PbxDBdl" which should contain a single digital link for each of the "groups" in the public exchange allocated to the installation.

3.52.2 Configuration procedure

3.52.2.1 CONFIGURATION

- All configurations are performed under the address "PbxDivVar"

• by OMC (Expert View): **System Miscellaneous** -> **Memory Read/Write** -> **Misc. Labels** -> **"PbxDivVar"**
• by MMC-Station: **Global -> Rd/Wr -> Address -> "PbxDivVar" -> Return -> Memory**

Byte 1 = Request type

- 00 = all accesses (default value)
- 01 = T0 by T0
- 02 = T0 group

Byte 2 = Keypad or facility

- 00 = facility (default value)

- 01 = keypad

Byte 3 = Password

- 00 = local password (default value)
- 01 = network password

Byte 4 = fixed or variable destination

- 00 = variable destination (default value)
- 01 = fixed destination

{0>" Octets 5 et 6 = Numéro de faisceau "<}0{> Bytes 5 and 6 = Trunk group number "<0}

- XX-XX = trunk group number used if the type is a T0 group (last trunk group by default)

3.52.3 Operation

3.52.3.1 ACTIVATION/USE

P.K.:: Programmed Key - defined by OMC (Expert View) or MMC-Station

Type of station / Service	**Station without display (except Z)**	**Station with display**
PCX forwarding	P.K.: **Div PCX** + password (*)	P.K.: **PCX + password (*)**

(*) dial also, if not already pre-programmed in the "forwarding" key, either:

- the directory nº of the trunk group containing the activation request if forwarding is **fixed** and of **type 1**
- or the directory nº of the trunk group containing the activation request and the forwarding destination if forwarding is **variable**.

3.52.3.2 CANCELLATION

Type of station / Service	Station without display (except Z)	**Station with display**
PCX forwarding	P.K.: **Div PCX** + password	P.K.: **PCX + password**

3.52.3.3 ADDITIONAL INFORMATION

- Activation of PCX forwarding is signaled:
  - on the displays of all stations in the installation
  - for a type 1 configuration, by the icon or LED of the forwarded RSP keys.
- After activation of PCX forwarding, outgoing calls are still authorized.
- Two metering proofs are printed: one when the service is activated, the other when it is cancelled.
- The activation request for a "group" in which all the links are busy is rejected. The same applies to an isolated link.
- For countries without this feature, PCX forwarding can be managed using a restricted

public numbering plan in which every DDI number corresponds to a station which will divert to the outside.

3.53 Background Music

3.53.1 Overview

3.53.1.1 DESCRIPTION

When a radio or cassette recorder is connected to the system, a user can activate the broadcast of music through the loudspeaker on his station when it is idle.

3.53.1.2 ACTIVATION/USE

Type of station / Service	**Without loudspeaker**	**With loudspeaker**
Background music	--	F.K.: **LS** or **LS+**
Adjust the volume	--	F.K.: **LS+** and **LS-** or **LS+/-**

3.53.1.3 cancellation

Type of station / Service	**Without loudspeaker**	**With loudspeaker**
Background music	--	F.K.: **LS** or **LS+**

3.53.1.4 ADDITIONAL INFORMATION

The transmission of the music is stopped automatically when a call arrives on the station or when the user makes a call.

3.54 Headset Features

3.54.1 Overview

3.54.1.1 DESCRIPTION

The user of a station with the Handsfree feature can use a headset, connected instead of the handset (for a wired station) and use the features normally accessible from his or her station.

"Headset mode" must be activated by station customization.

To answer a call, three connections can be used, either:

- manual: the user answers the call manually by pressing the resource key signalling the call or the Handsfree key
- a hotline call: the system determines what type of call is at the station (see "Answering camped-on calls")
- in automatic **Interphone** mode: after ringing, the station "answers" the call of highest

priority by switching to handsfree mode. For more information on automatic Interphone mode (also called automatic answer mode or Intercom mode), see: module Making/Answering a Call - Overview § RECEIVING A CALL .

3.54.2 Configuration procedure

3.54.2.1 CONFIGURATION

- To modify the time-out before connection in automatic mode – OMC (Expert View) only:

System Miscellaneous -> Feature Design -> Part 3 -> "Time before auto. conn. in headset mode"

- To activate headset mode (MMC-Station Administrator session only)

Subscr ->No° of station -> Headst -> Choice

Note:
Headset mode can also be activated by customizing the stations; see module Customizing Stations - Detailed description for how this is done.

3.54.3 Operation

3.54.3.1 USE

P.K.: Programmed Key – defined by OMC (Expert View) or MMC-Station

F.K.: Fixed Key

Type of station / Service	**Without Hands-Free feature**,	**With Hands-Free feature**
Answer a call manually	--	Resource Key or F.K.: **Handsfree**
Activate automatic answer mode (*)	--	F.K.: **Intercom** or P.K.: **AutAns** or **Intercom**

(*) When a caller is camped-on on the station in automatic answer mode, the user goes into conversation with the caller after pressing the "End" key and the transmission of a beep.

3.55 Appointment Reminder/Wake Up Call

3.55.1 Overview

3.55.1.1 DESCRIPTION

A user can have his station ring at a time he can program himself. This is the "Appointment Reminder" function in the case of companies and the "Wake-Up" call in the case of a hotel (in the various numbering plans, it is referred to as "Wake-Up").

The "Appointment reminder" can be activated either:

- every day at the programmed time: this is a "permanent" appointment

- or only once in the 24 hours following programming: this is a "temporary" appointment.

3.55.1.2 ADDITIONAL INFORMATION

- When the station is busy at the time the appointment reminder or wake-up call is made, the station does not ring but the user hears a specific tone.
- To avoid traffic overload, stations that have placed wake-up call requests are called in groups of 5, with a default time lapse of 2 seconds between 2 groups
- Number of analog stations called simultaneously: maximum of 4 per SLI board
- You can consult the appointment reminder/wake-up call status for each station in: **Subscribers/Basestations List** -> **Details** -> **WakUp**.

3.55.2 Configuration procedure

3.55.2.1 CONFIGURATION

- To program the time of the appointment or wake-up call for a station:

S.K.: Soft Key

Prefix: Code programmed in the internal numbering plan

Type of station / Service	**Without display**	**With display, no soft keys**	**With soft keys**
Permanent appointment reminder	--	Key **i** + function "**Appmnt**" then function " **Perm** + 4-digit permanent call time	S.K.: **Appmnt** + S.K.: **Param** + 4-digit permanent call time
Temporary appointment reminder	Prefix **Wake-up activation** + 4-digit wake-up call time	Key **i** + function "**Appmnt**" + 4-digit temporary reminder time	S.K.: **Appmnt** + 4-digit temporary reminder time

- To define the number of times temporary appointment reminders/wake-up calls should be repeated (3 by default):

- by OMC (Expert View): **System Miscellaneous -> Memory Read/Write -> Other Labels -> "WakeUpRetr"**
- by MMC-Station: **Global -> Rd/Wr -> Address -> "TonPrCmp" -> Return -> Memory**

- To define the ringing duration (15 seconds by default):

- by OMC (Expert View): **System Miscellaneous -> Memory Read/Write -> Debug Labels -> "TmAppAnTim (temporary appointment) or PmAppAnTim (permanent appointment)"**

- To define the timing between 2 wake-up calls (1 minute by default):

- by OMC (Expert View): **System Miscellaneous -> Memory Read/Write -> Debug Labels -> "TmAppWaTim (temporary appointment) or PmAppWaTim (permanent appointment)"**

- To define the timing between 2 groups of 5 wake-ups when there are too many simultaneous requests (2 seconds by default):

- by OMC (Expert View): **System Miscellaneous -> Memory Read/Write -> Debug Labels -> "InAnnAppTim"**

- To define the reaction in the event of a problem with a wake-up call on a room station (Hotel version)

- by OMC (Expert View): **System Miscellaneous -> Memory Read/Write -> Other Labels -> "WakUpPrbRg"**
- by MMC-Station: **Global -> Rd/Wr -> Address -> "WakUpPrbRg" -> Return -> Memory**

If YES is selected, the reception station rings with a specific call tone and the display shows "Wake-up problem ".

3.55.3 Operation

3.55.3.1 ACTIVATION/USE

At the appointment or wake-up time, the station rings and the display shows the appointment.

Ringing stops when the user acknowledges the appointment reminder or wake-up call, for example by going off hook. If there is no acknowledgement, the station rings for 15 seconds (default setting) and then again one minute later (also by default) and then a third time (by default) after a further minute.

Whether acknowledged or not, a temporary appointment reminder or wake-up call is cancelled and a permanent appointment reminder is retained for the following day at the same time.

3.55.3.2 CANCELLATION

S.K.: Soft Key

Prefix: Code programmed in the internal numbering plan

Type of station / Service	**Without display**	**With display, no soft keys**	**With soft keys**
Permanent appointment reminder	--	Key **i** + function "**Appmnt**" then function "**Perm**" + F.K.: "Cancellation" + F.K.: "OK"	S.K.: **Appmnt** + S.K.: **Perm** S.K.: **Clear** + S.K.: **OK**
Temporary appointment reminder	Prefix **Wake-up activation**	Key **i** + function "**Appmnt**" then function "**Temp**" + F.K.: "Cancellation" + F.K. "OK"	S.K.: **Appmnt** + S.K.: **Temp** + S.K.: **Clear** + S.K.: **OK**

3.56 Call Monitoring

3.56.1 Overview

3.56.1.1 DESCRIPTION

A user can help one or more other users to manage their communications, by means of:

- **supervision** of one or more resource keys on these users" stations, with or without **supervised call ringing**: the incoming calls on the supervised resource key are signaled in the same way as on the associated supervision key
- the **selective monitoring**: the user also receives the calls intended for the selected directory numbers
- **subscriber monitoring**: the user also receives all the calls for the station monitored
- **general monitoring**: the user also receives external calls intended for the operator stations

3.56.2 Configuration procedure

3.56.2.1 CONFIGURATION

- For a Z station wishing to use general monitoring, program a virtual key using OMC (Expert View):

Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Virtual Key -> "General Monitoring"

3.56.3 Operation

3.56.3.1 ACTIVATION/USE

P.K.: Programmed Key – defined by OMC (Expert View) or MMC-Station

Prefix: Code programmed in the internal numbering plan

Type of station / Service	**Z**	**Without display and monoline**	**Without display and multiline**	**With display**
Supervised call ringing	--	--	P.K.: **Supervision melody** or **Ring**	P.K.: **Supervision melody** or **Ring**
Selective monitoring	--	--	P.K.: **Selective monitoring**	P.K.: **Monit**
Answer calls from selective monitoring	--	--	P.K.: **Selective monitoring** when the associated LED flashes	P.K.: **Monit** when the associated LED or icon flashes
Subscriber monitoring	--	--	P.K.: **SubMon** or **Subscriber monitoring**	
Answer calls from subscriber monitoring	--	--	Off-hook or press "Hands Free"	
General monitoring	Prefix **Programming mode** + 6 (*)	P.K.: **General monitoring**		P.K.: **GenMon**

Type of station / Service	Z	Without display and monoline	Without display and multiline	With display
Answer calls from General monitoring	Go off hook	Go off hook	P.K.: **General monitoring** when associated LED or icon flashes	P.K.: **GenMon** when associated LED or icon flashes

(*) If a "General Monitoring" virtual key is programmed on the station.

3.56.3.2 CANCELLATION

P.K.: Programmed Key – defined by OMC (Expert View) or MMC-Station

Prefix: Code programmed in the internal numbering plan

Type of station / Service	Z	Without display and monoline	Without display and multiline	With display
Supervised call ringing	--	--	P.K.: **Supervision melody** or **Ring**	P.K.: **Supervision melody** or **Ring**
Selective monitoring	--	--	P.K.: **Selective monitoring**	P.K.: **Monit**
Subscriber monitoring	--	--	P.K.: **SubMon** or **Subscriber monitoring**	
General monitoring	Prefix **Programming mode** + 7	P.K.: **General monitoring**		P.K.: **GenMon**

3.56.3.3 ADDITIONAL INFORMATION

- A "Selective Monitoring" programmed key can monitor up to 8 directory numbers (a user can have several directory numbers for a single station: for example, an internal number defined in the main numbering plan, and an external number defined in the DDI numbering plan. Thus, in order to monitor both internal and external calls, both directory numbers must be programmed on one or two selective monitoring keys).
- A station can have several selective monitoring keys.
- Selective or subscriber monitoring of a group of stations is impossible. However, when subscriber monitoring is active for a station belonging to a parallel or sequential group, the group calls for this station are monitored.
- Selective monitoring does not work for diverted or monitored calls.
- Subscriber monitoring does not work for calls coming from automatic call back on busy station or trunk group, or from those coming from master recall if transfer fails.
- When all the station resources are busy, new monitored calls are lost.
- A programmed "subscriber monitoring" key can be used to monitor up to 8 directory numbers (if a station has several call numbers, simply program one of them on a "subscriber monitoring" key for all the numbers on this station to be monitored).
- So that a Z station can use general monitoring, the installer must configure a "virtual"

General Monitoring key on it.

3.57 Customising Stations

3.57.1 Detailed description

3.57.1.1 DESCRIPTION

Customization only affects the station on which it is performed (you cannot customize remote stations).

3.57.1.1.1 Switching to Customization mode

Depending on the type of station, press **Custo** (2nd page, Advanced Station in Idle) or **i** + 5, or dial the "Programming Mode" function code.

The following pages describe the tree structures available for each type of station; navigation is done using soft keys or codes (with the help of voice guides).

3.57.1.1.2 Additional Information

- Answer Only mode: activating or deactivating "Answer Only" mode does not modify the greeting in the voice mailbox ; the user has to select the appropriate default message or re-record a new one that corresponds to the selected mode of operation.
- Destination number (personal assistant or message notification):
  - external numbers must include the network access prefix
  - external numbers are subject to barring controls
  - if the pre-defined number is invalid or barred, the call is automatically put through to the destination mailbox (personal assistant) or is not connected (remote notification).
- Time ranges: on initialization, the start time is 00:00 and the end time is 24:00
- Customization validation key: **OK** for stations with soft keys, # for stations without soft keys, **9** for decadic stations.

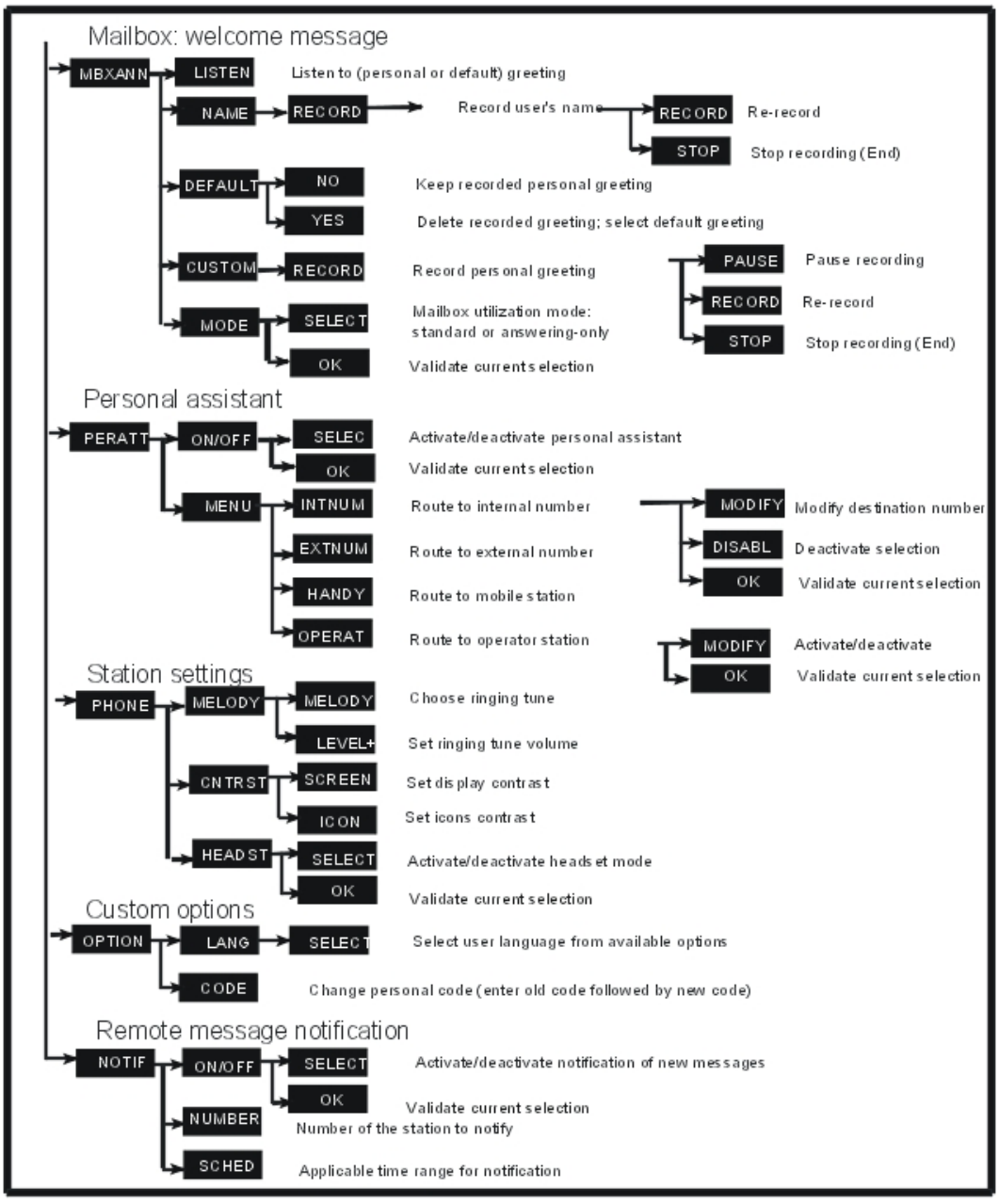
3.57.1.1.3 Other available features:

- **i** key + key programmed with a specific parameter: modify the parameter value.
- Repertory key + **i** key: program personal speed dials.
- **i** key + Appmnt key: program a reminder call.
- **i** key + Divert key: program call types to be forwarded.

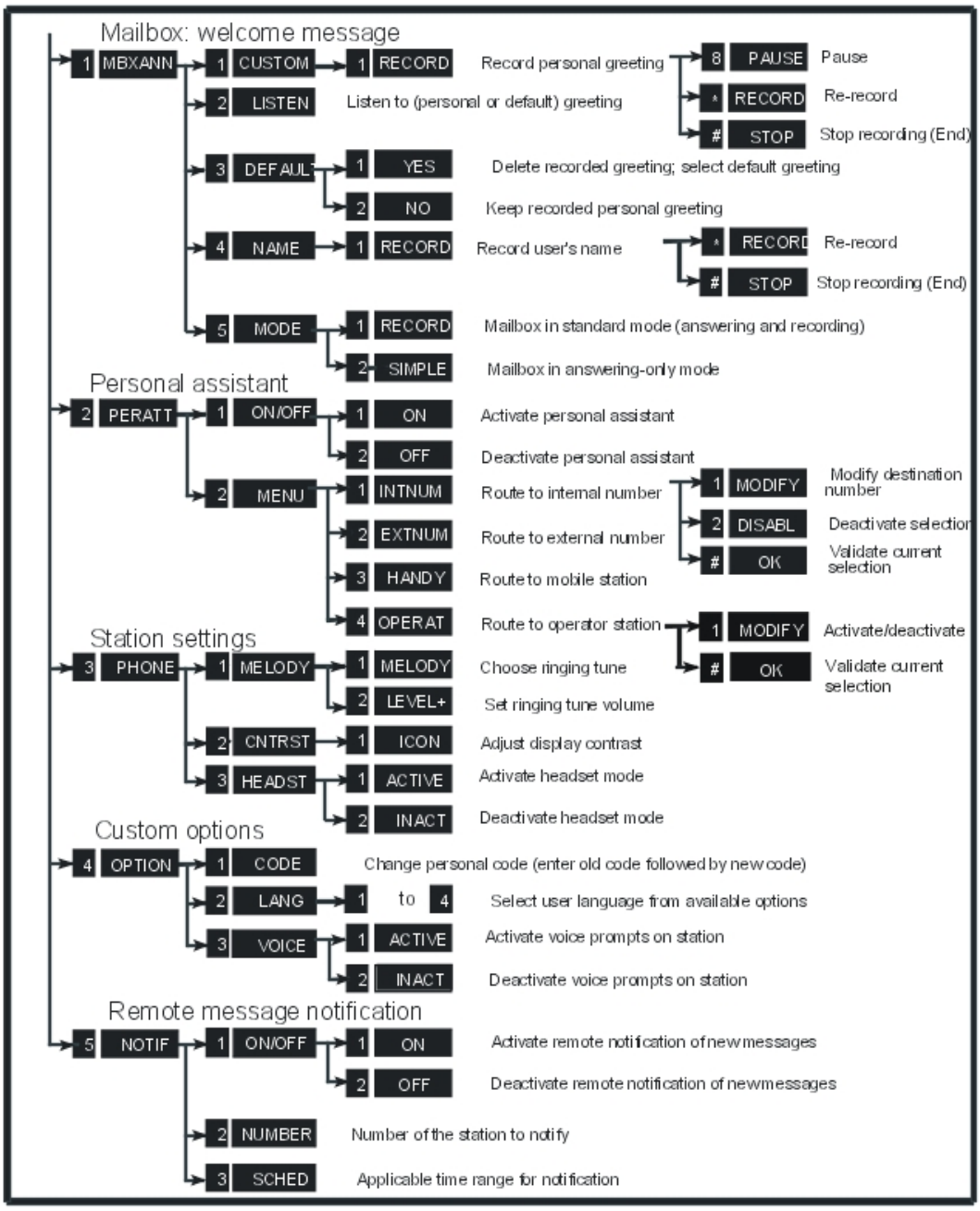
Note:

For a detailed description of how to set up these functions (passing from one function to another, deleting a value, etc), refer to the user guide for the relevant terminal.

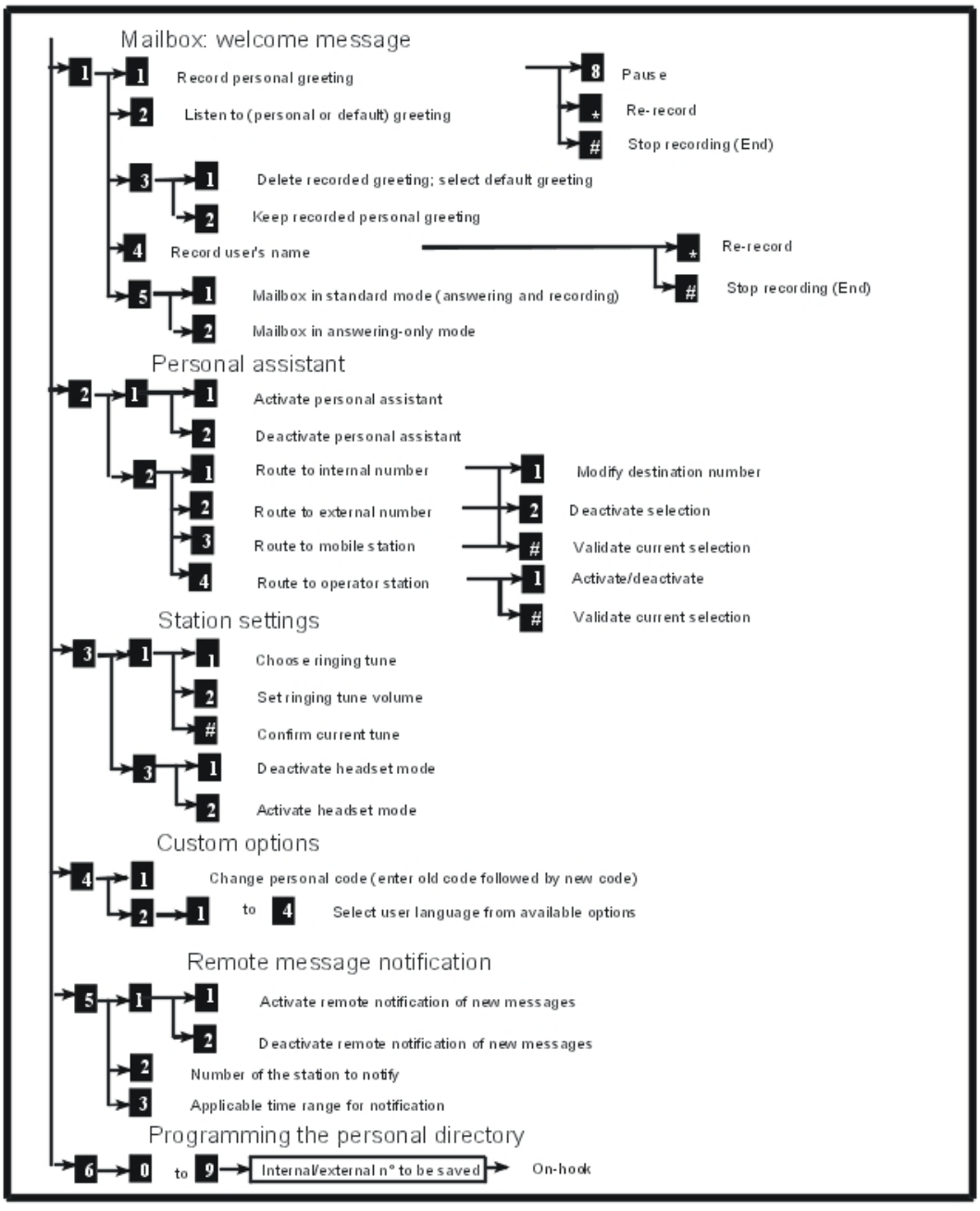
3.57.1.1.4 Stations with soft keys



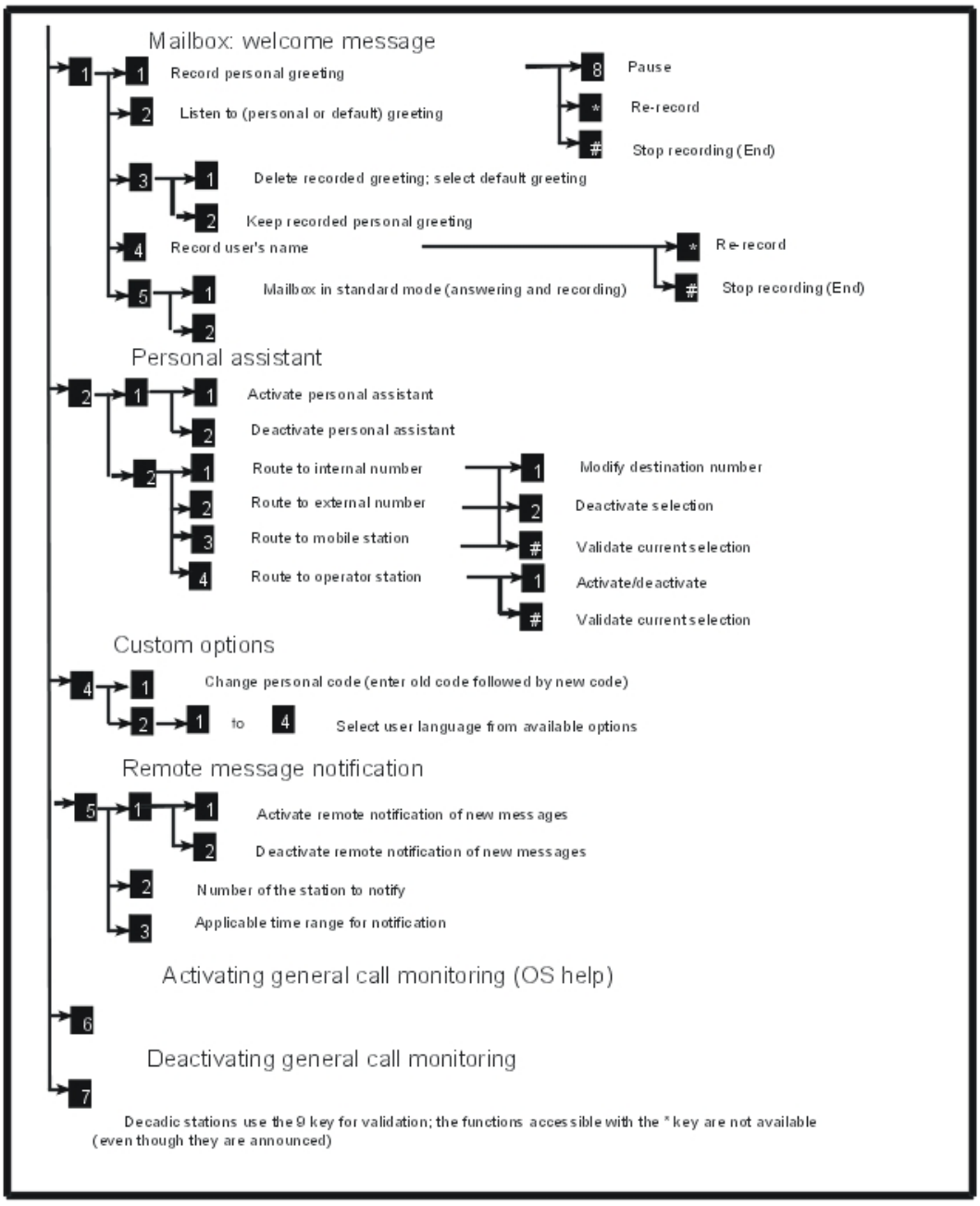
3.57.1.1.5 Stations without soft keys but with displays



3.57.1.1.6 Stations without displays or soft keys



3.57.1.1.7 Analog Z stations



3.58 Teamwork

3.58.1 Overview

3.58.1.1 DESCRIPTION

Teamwork simplifies the call management of all the members in a "work group" by equipping each station with:

- as many RSL keys as there are members in the group less one. Each RSL is programmed with the number of one of the other members of the group. These keys enable:
  - monitoring of the other stations, i.e. knowing whether they are free or occupied
  - direct calls to other members of the group
- one or more selective call monitoring keys (one key makes it possible to monitor up to 8 directory numbers) (see "Call Monitoring")
- a group call pick-up key (see "Call pick-up")

3.58.1.2 ADDITIONAL INFORMATION

- Group call pick-up is used when selective call monitoring is deactivated for the station which is ringing.
- A work group is "virtual", i.e. there is no directory number. To remedy this, it is preferable to create a Hunting Group with parallel management (see "Hunting Groups").
- By adding monitoring resource keys to the other stations in the work group, each member of the group can monitor the other member's calls.

3.58.2 Configuration procedure

3.58.2.1 CONFIGURATION

- To create a work group – MMC-Station only:

TerPro -> TeamWk -> Add

3.59 Account Code/Substitution

3.59.1 Overview

3.59.1.1 DESCRIPTION

3.59.1.1.1 Account code

An account code makes it possible to charge the cost of an external communication to a client account.

During a communication, a dedicated station can modify the account code or add one ; a Z station cannot.

All the account codes are configured in the account code table. For each account code, the installer can state:

- whether or not the client account is identified by a name which can be printed on the metering statement instead of the name of the call initiator
- whether or not the initiator of the call is to be identified by his directory number
- whether or not the initiator of the call must enter a password, either:

  - his personal code, if the user's identity is required ("User-ID" field in OMC = User)
  - the personal code of the station on which the call is made, if the user's identity is not required ("User-ID" field by OMC = No)
- whether the barring and traffic sharing link categories (see "Link Categories" and "Barring") used for the call are:
  - those of the "set" on which the call is made
  - those of the "Guest" (OMC label), i.e. of the station identified for this call
  - the barring link category of the client account (between 1 and 16) and traffic sharing link category of the station on which the call is made
  - no barring: no barring link category but the system uses the traffic sharing link category of the station on which the call is made
- the number of digits of the external number, masked on the metering statement:
  - all: all the digits are masked (priority field in relation to the "Mask last 4 digits" field in the "Metering Printout" menu)
  - 0, 1, ...,9: from 0 to 9 digits masked (priority field relative to the "Mask last 4 digits" field in the "Metering Printout " menu)
  - default: value of the "Mask last 4 digits" field in the "Metering Printout" menu (either 0 or 4 digits masked).

Furthermore, an account code can be:

- defined: in this case, it is composed exclusively of digits (e.g. "987654")
- partially defined: in this case, it is composed of digits and asterisks (e.g.: "1345*****"), the asterisks represent the variable part ; the number of digits in the account code entered must be equal to the number of digits of the defined and asterisk part
- variable: in this case, it is composed exclusively of asterisks ; the number of digits in the account code entered must be equal to the number of asterisks.

When an account code is entered, the system checks first of all, whether it exists as a "defined" code, if not, a "partially defined" code, and finally as a "variable" code.

The installer can configure a code for activating the "Account Code" service in the main numbering plan. The "Base" field can be either:

- empty: in this case, the user enters the code associated with the client account himself
- 4 digits long, 0000 to 9999: in this case, the base refers to an account code configured in the account code table. The four digits of the base can correspond either to the 4 digits of a defined account code or to a variable code of 4 asterisks.

3.59.1.1.2 Substitution

This makes it possible to authorize a user to make **an external call** from any station in the installation, even barred or locked, as if he were making the call from his own station.

Substitution is a particular account code case for which:

- the user's identity is required
- barring and traffic sharing link categories are those of the "guest"
- the password may be required.

3.59.2 Configuration procedure

3.59.2.1 CONFIGURATION

- To create the code for activating the "Account Code" feature in the internal numbering plan:

• by OMC (Expert View): **Numbering -> Internal Numbering Plan ->"Account Code New"** • by MMC-Station: **NumPln -> IntNum -> Accoun**

- To create the account code table:

• by OMC (Expert View): **Traffic Sharing and Barring -> Account Code Table**

- Select the name printed on the metering ticket ; that of the client account or of the initiator of the call – OMC (Expert View) only:

Metering -> Printout -> Fields -> "Subscriber Name"

3.59.3 Operation

3.59.3.1 ACTIVATION/USE

P.K.: Programmed Key – defined by OMC (Expert View) or MMC-Station

Prefix: Code programmed in the internal numbering plan

Type of station / Service	**Z**	**Without display**	**With display**
Before setting up the call	Prefix **New account code** + account code if necessary + n# directory (if identity required) + personal code if required + external n#	P.K.: **New account code**(*) + account code if requested + directory n# if identity requested + personal code if requested + external n#	P.K.: **AccNew** (*) + account code if requested + directory nº if identity requested + personal code if requested + external nº
During communication	--	P.K.: **Account code during communication** + account code if requested + directory nº if identity requested + personal code if requested + external nº	P.K.: **AccCom** + account code if requested + directory nº if identity requested + personal code if requested + external nº

(*) the programmed keys, such as the numbering plan activation prefix, can contain the desired account code.

3.59.3.2 ADDITIONAL INFORMATION

- The system rejects all calls with an account code using the default personal code.
- An account code can have up to 16 digits or asterisks.
- Partially defined account codes in formats "12**34", "1***6**" or "**88" are forbidden.
- FORCED ACCOUNT CODE: the installer can authorize the user to only make external calls using an account code, by:

  - assigning barring link categories specific to the account code on one hand and to the user on the other
  - configuring account code parameters in the following manner: the user's identity is required, barring and traffic sharing link categories are those of the "station" and a password is also required

- The "New Account Code" and "AccNew" programmed key can be replaced by "Macro2" keys containing the external code .
- The account code is not memorized with the number in the Last Number Redial and Temporary memories.
- An account code can be modified several times during communication and until the user enters a "defined" or "partially defined" code.
- Masking of several or of all the digits in the external number dialed makes it possible to keep a call confidential.
- The "names" of the account codes do not figure in the internal directory.
- An account code remains active after activation of a paging, after a recall in the case of a transfer failure, after a call parking, a call pick-up, a forwarding or a transfer.
- The "Account Code" field can only be printed on statements with 132 columns.
- An S0 station cannot use these services.
- What not to do – example of an ineffective account code configuration: the user's identity is required, the barring and traffic sharing link categories are those of the "guest" and the personal code may or may not be required.

3.60 Allocation of a Trunk Line

3.60.1 Overview

3.60.1.1 DESCRIPTION

An authorized user can lease one of the trunk lines in the main trunk group to another barred user so that he may make a single external call. This user keeps his call confidential since he dials the number himself.

The authorized user must be in an internal communication with the user before leasing him the line.

The authorized user can also:

- select the barring level assigned to the call made after allocation of the line: no barring or level 1 to 6
- lease a line with metering reminder (see "Meter Total Recall")
- assign an account code to the communication that the other user is about to make (see "Account Code")

3.60.1.2 ADDITIONAL INFORMATION

- The authorized user and the beneficiary user of the service must be connected to the same PCX.

- The beneficiary user of the service must have an available resource for the external communication.
- Meter total recall can only be requested on a station with display.
- If the service is refused, the beneficiary user hears the fast busy tone.
- The service is refused if the beneficiary station is locked or private without authorization to transfer.
- The allocated line is an analog trunk line or a digital access.
- The beneficiary user cannot use block dialing mode after trunk allocation.
- An S0 station cannot activate the service nor be a beneficiary user of the service.

3.60.2 Configuration procedure

3.60.2.1 CONFIGURATION

- To specify whether or not to authorize a station to allocate one of the lines in the main trunk group:

• by OMC (Expert View):
Subscribers/Basestations List -> **Details** -> **Features** -> **Part 2** -> **"Trunk Allot"**

- For each station, to specify whether or not to program the keys for trunk line allocation, with or without meter total recall:

• by OMC (Expert View):
Subscribers/Basestations List -> **Details** -> **Keys** -> **"Trunk Allot"** or **"Trunk Allot MTR"**
• by MMC-Station: **Subscr** -> **Keys** -> **"AllotN"** or **"AllotM"**

- To create the features in conversation for allocation of the trunk line, with a barring level from 1 to 7 (level 7 being "no barring"), with or without meter total recall:

• by OMC (Expert View):
Numbering -> **FAC Numbering Plan** -> **"Trunk Allot (1 to 7)"** or **"Trunk Allot MTR (1 to 7)"**
• by MMC-Station: **NumPln** -> **Code** -> **"AllotN Cat (1 - 7)"** or **"AllotM Cat (1 - 7)"**

3.60.3 Operation

3.60.3.1 ACTIVATION/USE

P.K.: Programmed Key – defined by OMC (Expert View) or MMC-Station

Prefix: Code programmed in the internal numbering plan

Type of station / Service	**Z**	**Without display (except Z)**	**With display**
During a local communication, the authorized user uses...	Prefix **Trunk allocation with or without MTR, and with or without barring**	P.K.: **Trunk allocation with or without MTR, and with or without barring** (*)	P.K.: **Trunk allocation with or without MTR, and with or without barring** (*)

then the other user...	hears the public network dial tone and makes the external call		
If a meter total recall has been requested...	--	--	the authorized user's station rings and the display indicates the metering

(*) Addition of an account code and the associated parameters must be done before activation of the "trunk allocation" service.

3.61 Meter Total Recall

3.61.1 Overview

3.61.1.1 DESCRIPTION

A user who has a station with a display can request to be called back automatically to find out the cost of an external communication made by another system user.

Meter total recall can be activated either:

- manually: in this case, meter total recall is requested before a single external call is setup.
- automatically, for each station in the installation: in this case, meter total recall is activated after all the external calls on "monitored" stations.

The ringer for a meter total recall is the same as that for an appointment reminder.

3.61.2 Configuration procedure

3.61.2.1 CONFIGURATION

- To create the prefix for activating "Meter Total Recall" in the internal numbering plan:

- by OMC (Expert View):
  Numbering -> **Internal numbering plan** -> **"Meter Total Recall"**
- by MMC-Station: **NumPln** -> **IntNum** -> **Funct** -> **"MTR**

- To specify whether or not to authorize the printing of a metering ticket during a meter total recall:

- by OMC (Expert View):
  System Miscellaneous -> **Memory Read/Write** -> **Misc. Labels** -> **"MTR_Print"**
- by MMC-Station:
  Global -> Rd/Wr -> Address -> "MTR_Print" -> Return -> Memory

- To specify whether or not to monitor a station after each external communication:

- by OMC (Expert View):
  Subscribers/Basestations List -> Details -> Metering ->Monitoring

- For each station, define the meter total recall destination for all external communications:

- by OMC (Expert View):
  Subscribers/Basestations List -> Subscribers/Basestations List -> Details ->Metering ->Metering Total Recall ->Destination n#
  Subscribers/Basestations List -> Subscribers/Basestations List -> Details -> Metering ->Metering Total Recall ->Active

3.61.3 Operation

3.61.3.1 ACTIVATION/USE

P.K.: Programmed Key – defined by OMC (Expert View) or MMC-Station

S.K.: Soft Key

Type of station / Service	**Without display**	**With display, no soft keys**	**With display, with soft keys**
Activating in manual mode, during communication (local)	--	P.K.: **MTR** + external nº + F.K.: Transfer	
Activating in manual mode, when idle	--	P.K.: **MTR** + external nº then, when the outside party answers, internal nº + F.K.: Transfer	
Activating in automatic mode	--	Automatic	
During recall, reading the directory nº of the "monitored" station	--	P.K.: **Read +**	P.K.: **Read +** if required
Printing a metering ticket	--	**2**	S.K.: **Print.**
Stopping the ringer and keeping the metering information on the display	--	**1**	S.K.: **MTR-OK**
Acknowledging the meter total recall	--	**1**	S.K.: **MTR-OK**

3.61.3.2 ADDITIONAL INFORMATION

- The recall is presented for 25 seconds ; if the recall is not acknowledged, the system temporarily cancels the recall: it is presented again after any operation carried out on the station.
- If the destination station for the recall is busy, the metering information is temporarily displayed and a sound signal is transmitted. As soon as it is free, the destination station for the recall should receive the metering information.
- When a station is the destination for several meter total recalls, the one which has been there the longest is presented first.
- The service can only be used on external lines providing metering information (hence, not on analog ATLs).
- A meter total recall does not follow a call forwarding.
- A "meter total recall" can be combined with a "trunk allocation" (see corresponding file).

- The character "#" precedes the number of the metering ticket printed on a meter total recall.

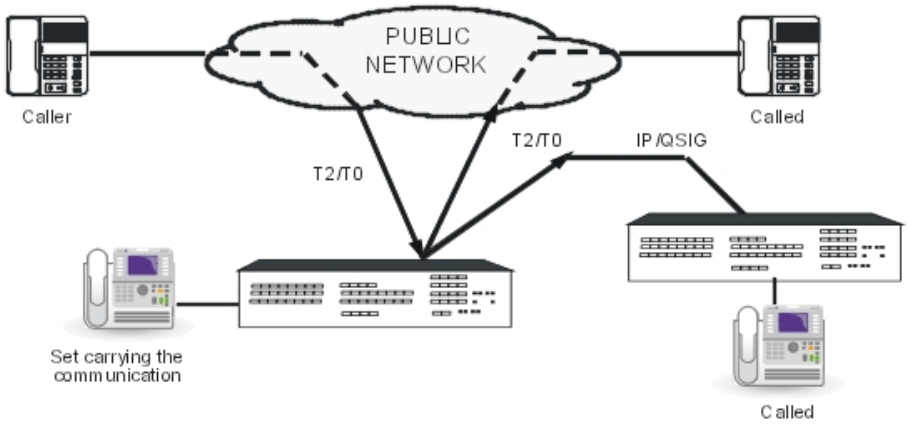
3.62 Remote Substitution

3.62.1 Overview

3.62.1.1 DESCRIPTION

The **remote substitution** service enables an employee who is outside of the business premises or at home to call a correspondent on the public network from a DTMF set (via the T0/T2 access) or a user on a remote PCX on the same private network (via the IP or the QSIG accesses) as if he were at work.

The user must pay for the call to the system; the company is charged for the call between the system and the external caller.



The user authentication can be performed with:

- A DTMF dialogue. On voice guides request, the caller dials his/her personal number and password
- The calling party CLI (Calling Line Identification). If the calling identity received matches one of theconfigured authorized users

3.62.2 Configuration procedure

3.62.2.1 CONFIGURATION

- To authorize or deny access to the service, for each station:

• by OMC (Expert View): **Users/Base stations List** -> **Users/Base stations List** -> **Details** -> **Features** -> **Part 2** -> **"Remote Substitution"**

- To validate the service in the public dialling plan (operates without base or NMT):

• by OMC (Expert View): **Dialling** -> **Public Dialling Plan** -> **Remote Substitution** • by MMC-Station: **NumPln** -> **PubNum** -> **Disa**

- To define the service access code – OMC (Expert View) only:

External Lines -> Remote substitution -> Access control code

- To define the voice guide message (none, message 1 to 8) – OMC (Expert View) only:

External Lines -> Remote Substitution -> Voice Guide Message

- To define the system reaction if no DTMF receiver is available (Call Waiting or Release) – OMC (Expert View) only:

External Lines -> Remote Substitution -> Wait for DTMF Receiver

- To enable the CLI authentication feature – OMC (Expert View) only:

System Miscellaneous > Memory Read/Write > Other Labels

CLICtrl flag values:

- **CLICtrl**=0x00: the CLI authentication feature is disabled
- **CLICtrl**=0x01: the CLI authentication feature is enabled

- To define in which cases a CLI number received from an ISDN trunk group can be trusted for CLI based identification and authorization – OMC (Expert View) only:

System Miscellaneous > Memory Read/Write > Other Labels

CLIISDNCtl flag values:

- **CLIISDNCtl**=0x01: CLI provided by the network is accepted (**network provided**)
- **CLIISDNCtl**=0x02: CLI provided by the user, verified and passed is accepted (**user-provided, verified and passed**)
- **CLIISDNCtl**=0x04: CLI provided by the user, verified and failed is accepted (**user-provided, verified and failed**)
- **CLIISDNCtl**=0x08: CLI unknown is accepted (**user-provided, not screened**)

The **CLIISDNCtl** flag is a bit map. The value 0x03 means that a CLI with the type*CLI provided by the network* or *CLI provided by the user, verified and passed* is accepted.

- To define the number of digits checked in the received CLI – OMC (Expert View) only:

System Miscellaneous > Memory Read/Write > Other Labels

CLINumCtrl flag values:

- **CLINumCtrl**=0x00: the comparison is performed on all digits
- **CLINumCtrl**=0xn: only thelast n digits are checked

Example 1:
*a GSM calls the PCX from abroad, the received CLI contains international prefixes. The national CLI is 06 12 34 56 78, the received CLI is 00 44 6 12 34 56 78. By configuring **CLINumCtrl** to 09h, the PCX checks the last 9 digits of the received CLI : 6 12 34 56 78*

- To define the authorized trunk group types – OMC (Expert View) only:

System Miscellaneous > Memory Read/Write > Other Labels

CLITrkCtrl flag values:

- **CLITrkCtrl**=0x01:CLI authentication is authorized for incoming calls from an ISDN trunk group
- **CLITrkCtrl**=0x02:CLI authentication is authorized for incoming calls from an analog trunk group
- **CLITrkCtrl**=0x04: CLI authentication is authorized for incoming calls from a tie line

The **CLITrkCtrl** flag is a bit map. The value 0x03 means that a call coming from an *ISDN trunk group* or an *analog trunk group* is allowed to perform a CLI authentication.

- To define the external number from which remote substitution is authorized for a given user , enter the CLI with the PCX outgoing prefix in the **Notification destination** field – OMC (Expert View) only:

Subscribers/Basestations List -> Details -> Mailbox -> Notification -> Notification destination

Example 2:
with a PCX outgoing prefix=0 and an external number=06 12 34 56 78, the ***Notification destination*** *field is 0 06 12 34 56 78*

3.62.3 Operation

3.62.3.1 Remote Substitution Access

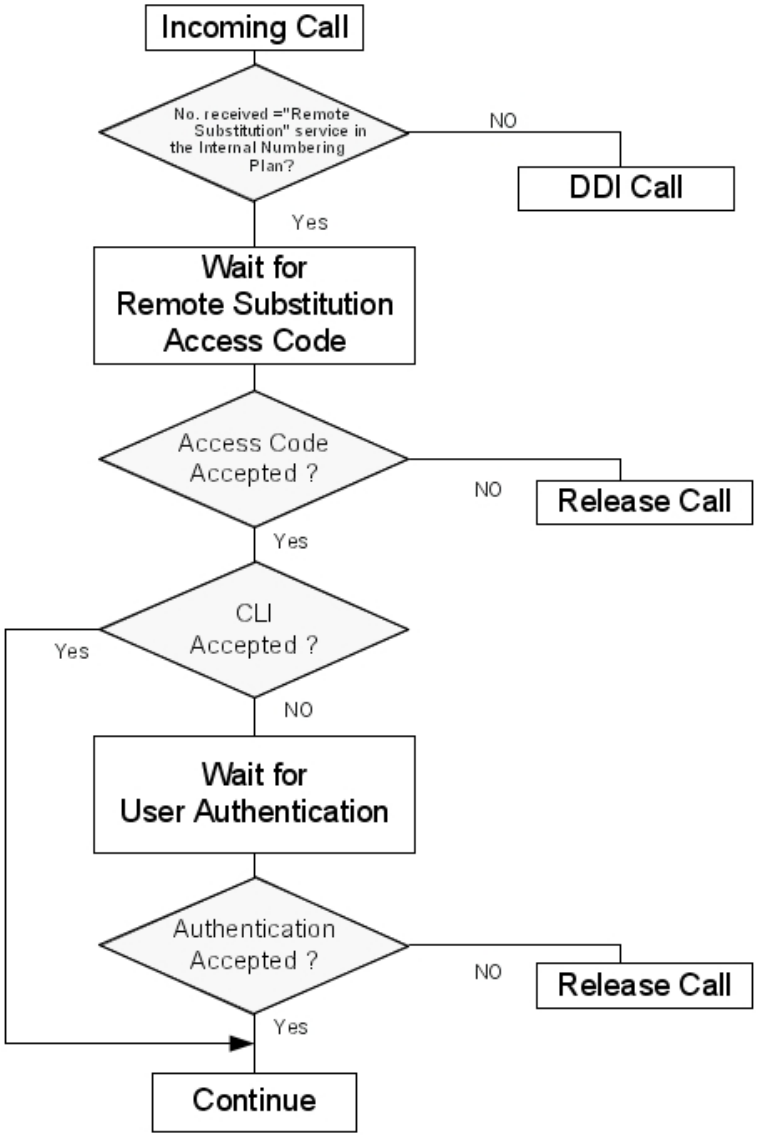


Figure 3.39 : Remote Substitution Access Algorithm

Details of the access algorithm

- **CLI accepted**: this test matches when:
  - The CLI authentication feature is enabled on the system
  - The calling party number is an authorized calling number. The comparison can be performed:
    - On all digits. In this case, the received calling number must match exactly the configured number (including trunk group seizure prefix, national code....)
    - On the last digits only. In this case, the comparison is performed only on the configured number of digits.

  - The incoming call is received from an authorized trunk group type
  - In case of an ISDN incoming call, the calling party number type matches one of the authorized types (also called security policy)
- **User authentication**: the calling party is prompted to enter his/her external directory number and password

3.62.3.2 ADDITIONAL INFORMATION

- The traffic sharing and restriction are those of the internal user.
- A single DTMF receiver is available at any given time.
- Counting: Every call generates 2 statement lines: one line for the incoming call (with Type = incoming transit call using remote substitution), the other is for the outgoing call (with Type = outgoing transit call using remote substitution).

3.63 Fax Notification

3.63.1 Overview

3.63.1.1 DESCRIPTION

The **fax notification** service informs users (whose stations have displays and Message LEDs) when they have just received a fax.

3.63.2 Configuration procedure

3.63.2.1 CONFIGURATION

- Program the "Fax Notification" table by creating the Fax n# <-> Subscriber n# links with:
  - fax numbers from the internal, public or private numbering plans
  - subscriber numbers from the internal numbering plan.

- by OMC (Expert View): **Subscribers Misc.** -> **Fax Notification for Subscribers**
- by MMC-Station: **Global** -> **FaxTab** -> **ReSubs** and **FaxNum**

3.63.3 Operation

3.63.3.1 ACTIVATION/USE

When a fax has been received, the system displays the message: "**Incoming Fax**" on the recipient subscriber's station (depending on the configuration of the "Fax Notification" table) along with the number of the receiving fax machine.

3.63.3.2 ADDITIONAL INFORMATION

- A subscriber can supervise several fax numbers.
- A fax n# can be supervised by several subscribers.
- The "Fax Notification" table is limited to 30 entries.

- To deactivate fax notification on a subscriber station, break the Fax n# <-> Subscriber n# link configured in the "Fax Notification" table.

3.64 Called Party Control

3.64.1 Overview

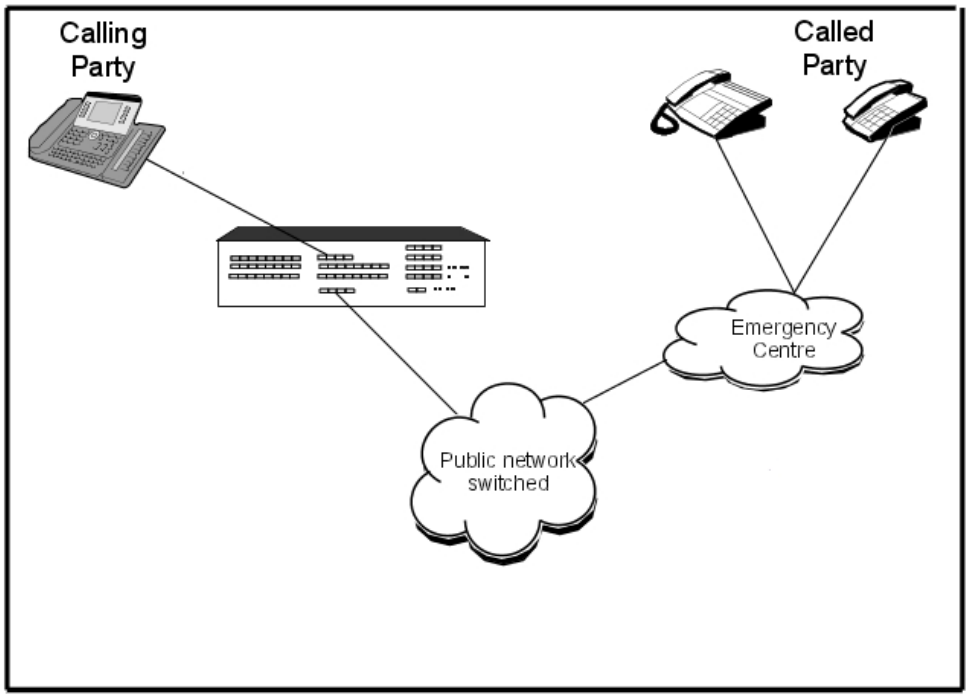
3.64.1.1 Basic Description

The "Called Party Control" feature applies to outgoing calls to emergency numbers via the public network.

The aim of this feature is that emergency call release may only be at the initiative of the emergency centre.

Should the calling party hang up first, the system tries to reestablish the call to the emergency centre. The set having hung up is rung again. A recall timer is started.

- If the calling party picks up the call before the recall timer has expired, the call resumes.
  If the calling party hangs up again, the calling party number is recalled once again by the system.
  The call is released when the called emergency centre hangs up.
- If the calling party does not pick up the call before the recall timer has expired, the call is released or transferred to an attendant. The call is processed as a standard unanswered incoming call (forwarded to attendant or released).
  If the attendant answers the transferred call, the "Called Party Control" feature is disabled. Both the attendant and the emergency centre may release the call.



Note:

- *The feature is not available on S0 stations.*
- *The feature does not support conferences. If a user is in a conference call and starts an emergency call and then hangs up, he/she is not called back by the system*
- *The correct operation of this feature on analog trunks is not guaranteed.*

3.64.2 Configuration procedure

3.64.2.1 Configuration

- Enabling the feature - OMC (Expert View) only:

Set the flag **CalledCtrl** to the value 01: **System Miscellaneous > Memory Read/Write > Other Labels > CalledCtrl**

Note 1:
*The **CalledCtrl** default value is 00 (feature disabled)*

- Configuring the emergency number - OMC (Expert View) only:
  The emergency number 110 is entered as "10 01 00 00 03 00 00 00".
  The first four bytes define the emergency number: an emergency number has a maximal size of 8 digits.
  Possible value is 0 to 9.
  The fifth byte indicates the length of the emergency number (03 = three digits) and sixth/seventh/eighth bytes are system data (do not modify).
  Therefore the emergency number 12345678 is entered as "78 56 34 12 08 00 00 00".

System Miscellaneous > Memory Read/Write > Other Labels > EmergNum > Details

Note 2:
- *For China, the default values of emergency numbers are:*
  - *110 for the police*
  - *119 for fire alarm*
  - *120 for ambulance services*
- *For some other countries, the default values of emergency numbers are 112 and 999*

- Configuring the recall timer - OMC (Expert View) only:

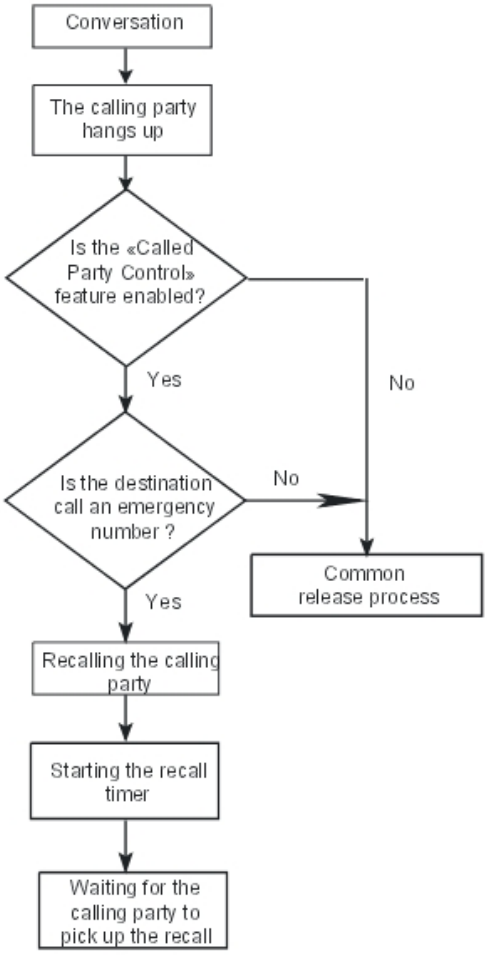
System Miscellaneous > Feature Design > Part 4 > Duration of Hold Recall Ringing

Note 3:
The default value of "Duration of Hold Recall Ringing" is 30s

3.64.3 Operation

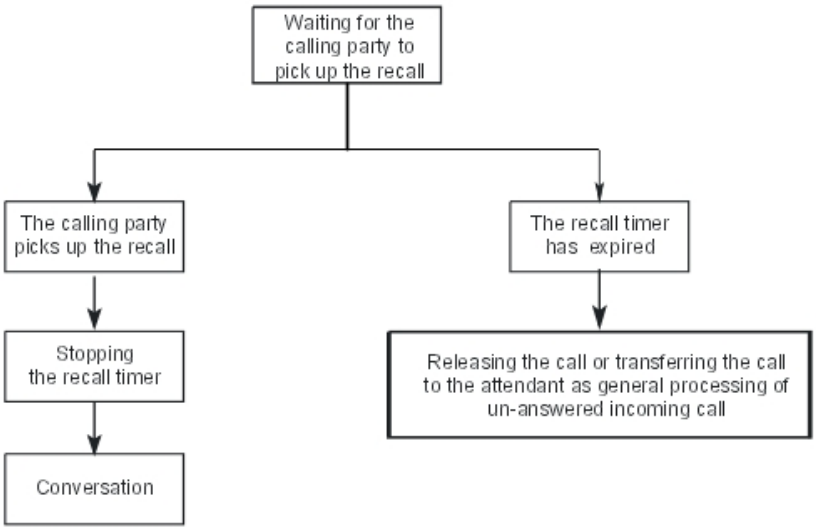
3.64.3.1 Activation/Use

"Called Party Control" feature recall mechanism



If the calling party picks up the call before the timer has expired, the outgoing call resumes. The internal recall mechanism is activated again if the calling party hangs up.

Processing during the recall timer



If the attendant answers the transferred recall, the recall becomes an incoming call from emergency centre.

So the "Called Party Control" feature is disabled and both the attendant and the emergency centre can release the call.

3.65 Outgoing Call Duration Control

3.65.1 Overview

3.65.1.1 Description

The "Outgoing Call Duration Control" feature enables the system to automatically release an outgoing call when the user's maximum Outgoing Call Duration (OCD) is over. This OCD is configured via OMC.

This feature applies to outgoing calls via the public network and but does not apply to emergency calls (see: module Called Party Control - Overview , for more information on emergency calls).

Outgoing calls are limited in time according to the call categories (city/area, national, international) and the OCD class they belong to.

Each outgoing call is released when the maximum OCD is reached.

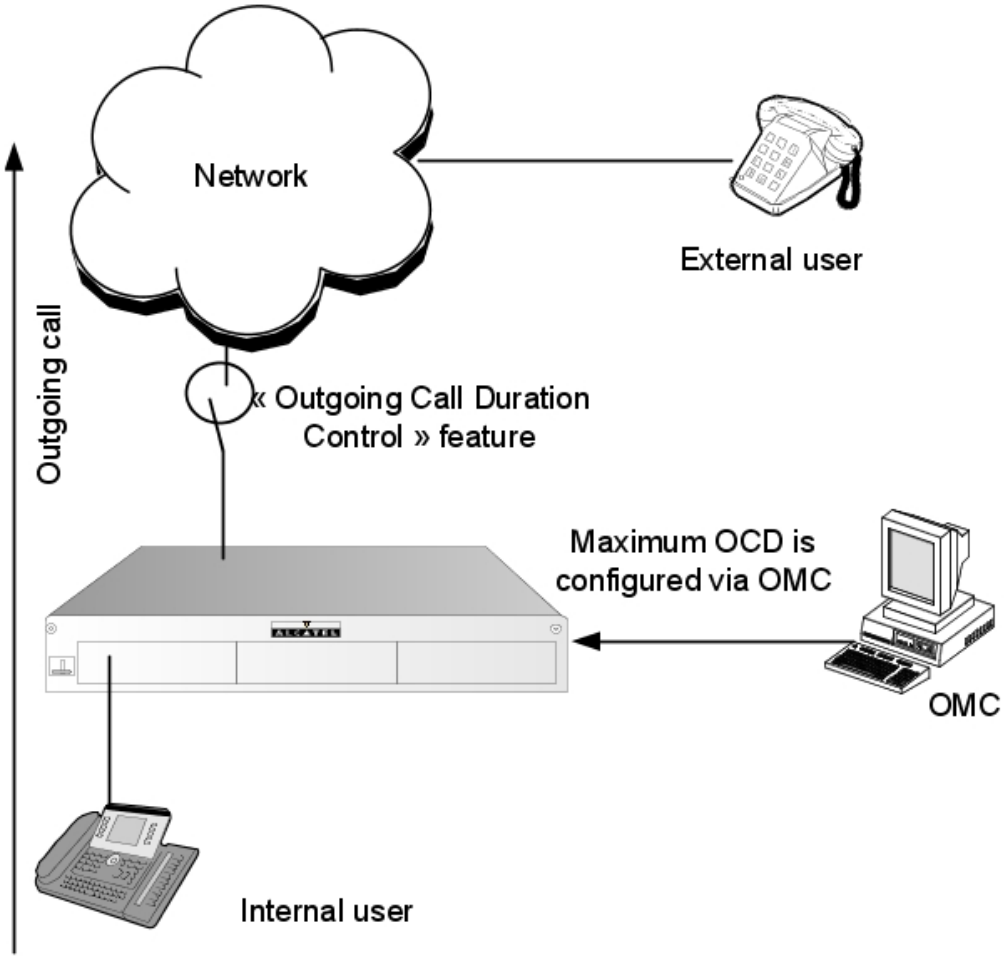


Figure 3.43 : Scenario

3.65.2 Detailed description

3.65.2.1 Detailed Technical Description

The "outgoing call duration control" feature enables the system to release the current outgoing call when the maximum OCD is reached.

The "outgoing call duration control" feature is not available when the set is a guest set or a booth set in a Hotel/Hospital configuration.

Users are limited in time for their outgoing calls according to the OCD class they belong to. Each OCD class (1, 2 and 3) controls the maximum call duration for each call category (city/area, national, international).

The maximum OCD is defined in OMC configuration: each user is assigned an OCD class.

3.65.2.2 Operation

1. Twenty seconds before the OCD is reached, a beep tone is played and a temporary

warning menu is displayed on the set screen (provided the set has a display)

2. When the maximum OCD is reached, the outgoing call is released

3.65.2.3 Interaction with Other Applications

3.65.2.3.1 Transferring an Outgoing Call

When an outgoing call is transferred:

- The OCD timer is reset
- The maximum OCD is set to the maximum OCD of the user to whom the call is transferred

3.65.2.3.2 Parking and Picking up a Call

When an outgoing call is parked, the timer is not stopped and the maximum OCD is not changed.

If the user does not pick up the call before the maximum OCD is reached, the call is released.

3.65.2.3.3 Call on Hold

An outgoing call which is on hold is released when the maximum OCD is reached.

3.65.2.3.4 DISA Transit

This feature operates under DISA transit condition and the maximum OCD is set according to the local user's configuration.

3.65.2.3.5 Forwarding a Call

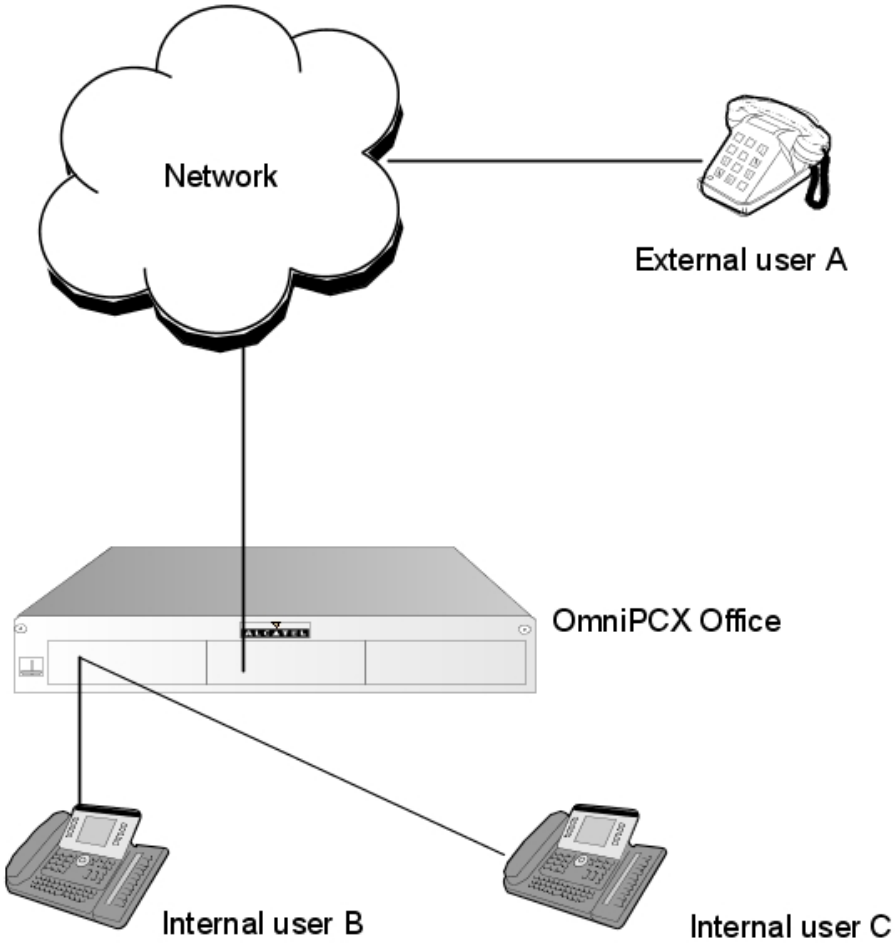


Figure 3.44 : Scenario

Internal user B forwards calls to an external user A.

When an internal user C calls the internal user B, the call is forwarded to the external user A. In this condition, the maximum OCD is set to the internal user B.

3.65.2.3.6 Conferences

This feature does not affect the "Meet Me Conference" feature (Six Party Conference).

This feature applies to the "Three Party Conference" feature. Operation is identical to a typical outgoing call. When the maximum OCD is reached, the outgoing call party is released.

3.65.2.3.7 Account Code/Substitution

This feature does not apply to the account code/substitution. When the user makes an outgoing call using an account code, the outgoing call duration is not limited.

3.65.2.3.8 Multi-set

When a user's phone is set to another user's secondary phone, the secondary phone OCD is

set to the primary phone OCD.

3.65.3 Configuration procedure

3.65.3.1 Configuration

- The feature is active when the outgoing call uses a public trunk group where the **Priv** field is set to **No** - OMC (Expert View) only:

Numbering > Numbering plans > Internal Numbering Plan

- A call category is assigned to an outgoing call:
  - A call is considered as a national call when the dialled number starts with the intercity prefix and the intercity code is not the same as the value configured in **Numbering > Installation numbers > Intercity code**
  - A call is considered as an international call when the dialled number starts with the international prefix and the international code is not the same as the value configured in **Numbering > Installation numbers > International code**

  In order to run this feature correctly, the international/national code and the international/national prefix must be configured properly.
  Call category definition:

Category definition	**City/Area Call**	**National Call**	**International Call**	**Emergency Call**
	Not in other categories	With city/area code prefix	With country code prefix	Emergency numbers

  OMC (Expert View) only:

Numbering > Installation numbers

  Note 1:
  For countries without city/area type of call (for example USA or France), the city/area fields are greyed out.

- To configure the maximum duration of an outgoing call - OMC (Expert View) only:

Traffic Sharing & Barring > Outgoing Calls Duration

  Users are limited in time for their outgoing calls according to the OCD class they belong to. Each OCD class (1, 2 and 3) controls the maximum call duration for each call category (city/area, national, international).

  For each user, the maximum OCD is calculated by the combination of the OCD class level (which the subscriber belongs to) and the outgoing call's call category.
  A "no limit" class is also available. Users assigned this class are not affected by any limit in the duration of their outgoing calls.
  OCD classes definition:
  The maximum OCD is defined per OCD class, for each call category, as follows (default values):

OCD class	**City/Area call**	**National Call**	**International call**
1	No Limit	No Limit	30mn
2	30mn	20mn	10mn

OCD class	City/Area call	National Call	International call
3	20mn	10mn	10mn

Note 2:
For countries without city/area type of call (for example USA or France), the city/area call column is greyed out.
For example:
If the subscriber has OCD class level 2 and the outgoing call category is National Call, the maximum OCD is 20 minutes (default value).

Note 3:
The maximum value for an OCD is 1439 minutes (23 hours 59 minutes).

- To assign an OCD class to the selected user - OMC (Expert View) only:

Users/Base stations List > Users/Base stations List > Details > Restr/Barring > OCD Class Level

Note 4:
By default, each user is configured with "no limit" as OCD class.

Remark:
If the configuration is wrong, a call may not be recognized. In other words, the system does not identify it as an international call, nor a national call, nor a city/area call. The outgoing duration control feature of this call is then processed as if it was a city/area call.

For countries without city/area calls, such a call is still processed with the default value of the OCD class of the user for city/area calls (even though the field is not enabled).

3.66 Nomadic Mode

3.66.1 Overview

3.66.1.1 Overview

From release 3.0 of Alcatel-Lucent OmniPCX Office Communication Server, Nomadic mode can be used to replace a company set with an external set. To do this, the mode must be configured and the external set declared as Nomadic set.

Nomadic operation completes the Web Communication Assistant by offering a telephone application when you are outside the company. Nomadic mode allows an employee on a business trip to use a GSM, a set in the home, a hotel set, etc. to:

- Answer a call
- Listen to a voice mail (via the Web Communication Assistant application)
- Set up a call (via the Web Communication Assistant application)

The workstation of a Nomadic set requires:

- A Nomadic virtual terminal
- A Nomadic PC outside the company (with the Web Communication Assistant)
- A Nomadic set outside the company (GSM, hotel set, etc.)

- A fixed set in the company

3.66.1.2 Nomadic Activation

The Nomadic mode can be activated via:

- Web Communication Assistant
- Extended Communication Server virtual desktop
- Remote customization (as of R7.0). For more details, see module Remote configuration - Detailed description .
- PIMphony

3.66.1.3 Use

An IP connection is essential between the Nomadic application and the system. The caller can either be an internal set or an external party.

3.66.1.3.1 Incoming Call

- The user has enabled Nomadic mode.
- The internal or external party calls the Nomadic worker on a company set connected to the system.
- The Nomadic application presents the incoming call and the caller hears the ring back tone.
- The system automatically calls the Nomadic set and if the call is answered, sets up a call between the 2 parties.

3.66.1.3.2 Outgoing Call

- The Nomadic user via the Web Communication Assistant Nomadic application requests a call from the system. The system then calls the Nomadic set and if the call is answered, calls the requested number. After a few seconds, the ring back tone is heard on the Nomadic set and the system automatically connects the 2 parties.

3.66.1.3.3 Listening to the Voice Mailbox

- Voice mails can be consulted:
  - Directly on the PC with the Nomadic Web Communication Assistant application.
  - On the Nomadic set (via the Web Communication Assistant application).

3.66.2 Configuration procedure

3.66.2.1 Configuration

3.66.2.1.1 Software Keys (OMC)

For Nomadic mode, Alcatel-Lucent OmniPCX Office Premium Edition CS with access to Web Communication Assistant services and Nomadic subscribers is essential.

3.66.2.1.2 Assigning Nomadic Rights (OMC)

To use the Nomadic mode, you must give the Nomadic right to the subscriber's phone set in

OMC:

1. In OMC, click on the **Users/Base stations** icon.
2. Select a subscriber and click **Cent Serv**.
3. On the **User** tab, select the **Nomadic Right** checkbox.

3.66.2.1.3 Creating a Nomadic Virtual Terminal (OMC)

To use Nomadic mode you need to create a Nomadic virtual terminal in the list of users before using the User wizard via Web Communication Assistant. The Nomadic virtual terminals must be called Virtual Nomadic (respect upper/lower case and the space between the words; virtual sets do not operate without this name). The default values of these sets can be kept.

Caution:

Check that the barring on virtual sets allows them to reach the numbers of the "Nomadic" sets.

3.66.2.1.4 Creating a User (WBM)

To create a user with rights to the Web Communication Assistant and to Nomadic mode:

1. Access the **User wizard** window.
2. Complete the fields then click **Next**.
3. Give the user's group then click **Next.**
4. Assign the Web Communication Assistant licence to the user then click **Next.**
5. Click End to validate the data and display the summary.

3.66.2.1.5 Configuring the Nomadic Set

After creating the user, a new icon is displayed in the right corner when connecting to the system via Web Communication Assistant with login and password.

1. Click this icon to start the Nomadic set configuration wizard.
2. Enter the password associated with the company set then click **Next**.
3. Give the name of the Nomadic set then click **Next**.
4. Give the call number of the Nomadic set, adding the public network access code then click **Next**.
5. Click End to enable Nomadic mode.

   Caution:
   If the message "Cannot enable Nomadic mode since there are no more virtual terminals available" is displayed, the Nomadic virtual terminal has not been created. In this case, refer to § Creating a Nomadic Virtual Terminal (OMC) .

3.66.2.1.6 Nomadic Mode Preferences

Once the activation procedure is finished, the new icon with the name of the Nomadic set is displayed in the right corner of the screen.

- Click this icon to modify the Nomadic mode preferences.
- Click "Go to Nomadic mode preferences" to add up to five nomad sets.

Important 1:
Clicking on the Nomadic mode icon enables Nomadic mode; all calls intended for the company set will now be routed to the Nomadic set. The dotted line between the 2 sets of the icon changes into a continuous line.

Click the icon again to disable Nomadic mode.

Important 2:

- When the Web Communication Assistant connection is finished, Nomadic mode is disabled automatically. If the browser is closed immediately, Nomadic mode will be disabled after 2 minutes.
- When Nomadic mode is enabled, "Nomadic mode" is displayed on the company set.
- Personal forwarding of the company set takes priority over Nomadic mode, even if "Nomadic mode" is displayed. Forwarding still operates. By enabling Nomadic mode via Web Communication Assistant, a warning message will be displayed if personal forwarding is enabled on the company set.
- Dynamic forwarding can be used simultaneously with Nomadic mode (pay attention to the time delay which must not be too short: you must add the time to route the call to the Nomadic set).
- The company set remains blocked while Nomadic mode is enabled (it cannot be used).
- Maximum number of Nomadic users: 15.
- IP terminals cannot be Nomadic sets.
- GAP sets are not supported as internal sets.

3.67 List of Services Provided

3.67.1 Services provided

3.67.1.1 LIST OF SERVICES OFFERED

table 3.319 : Services Offered on Alcatel-Lucent 8/9 series Sets

	4008, 4018	**4019**	**4028, 4029**	**4038, 4039, 4068**
Account code before setting up a call	•	•	•	•
Account code during communication	•	•	•	•
Amplification of the handset audio	•	•	•	•
Amplified reception	•	•	•	•
Answering a call (automatic connection)	•	•	•	•
Answering a call (manual connection)	•	•	•	•
Answering camped-on calls	•	•	•	•
Appointment reminder	•	•	•	•

	4008, 4018	4019	4028, 4029	4038, 4039, 4068
Auto. call setup on going off hook	•	•	•	•
Auto-answer mode (intercom mode)	•		•	•
Automatic call-back request on busy station	•	•	•	•
Automatic call-back request on busy trunk group	•	•	•	•
background music	•	•	•	•
Block dialling mode	•	•	•	•
Broadcast call (receive)	•	•	•	•
Broadcast call (send)	•	•	•	•
Call by collective speed dial number	•	•	•	•
Call parking and parked call retrieval	•	•	•	•
Call pick-up within a group	•	•	•	•
Calling Line Identification Restriction (CLIR)	•	•	•	•
Camp-on on busy station or group	•	•	•	•
Cancel all active forwardings	•	•	•	•
Common hold (and retrieval)	•	•	•	•
Conversation mute	•	•	•	•
Conference	•	•	•	•
COnnected Line identification Presentation (COLP)	•	•	•	•
COnnected Line identification Restriction (COLR)	•	•	•	•
Connection handoff				
Consultation of camped-on caller identities			•	•
Contrast of the display and icons	•	•	•	•
Deferred callback request (leave a)	•	•	•	•
Deferred callback request (receive a)	•	•	•	•
Dial by name	•	•	•	•
Digit-by-digit dialling mode	•	•	•	•
Direct internal or external call by programmed key	•	•	•	•
Display correspondent's name or number	•	•	•	•
Display date and time	•	•	•	•

	4008, 4018	4019	4028, 4029	4038, 4039, 4068
Do Not Disturb (DND)	•	•	•	•
DTMF end-to-end signalling	•	•	•	•
Dynamic routing	•	•	•	•
Enquiry call	•	•	•	•
Exclusive hold (and retrieval)	•	•	•	•
External forwarding	•	•	•	•
Fax Notification	•	•	•	•
Follow-me	•	•	•	•
Forced DTMF end-to-end signalling	•	•	•	•
Forward on busy	•	•	•	•
Forwarding to pager	•	•	•	•
Gain switch forcing	•	•	•	•
General tracking	•	•	•	•
Hands free	•		•	•
Headset mode manual or automatic response	•		•	•
Station identity (number and name)	•	•	•	•
Identity of the sub-device connected to the station	•	•	•	•
Immediate forwarding of group calls	•	•	•	•
Immediate forwarding of personal calls	•	•	•	•
Indication of the cost of a communication	•	•	•	•
Individual call pickup	•	•	•	•
Interphone barge-in (intrusion) on free	•	•	•	•
Internal group call	•	•	•	•
Internal station call	•	•	•	•
Barge-in	•	•	•	•
Keypad dialling features	•	•	•	•
Main PCX recall (calibrated loop break)	•	•	•	•
Malicious call identification	•	•	•	•
Count total recall	•	•	•	•
Name/Number display selection during ringing or conversation			•	•

	4008, 4018	4019	4028, 4029	4038, 4039, 4068
Non-answered calls repertory	•	•	•	•
On-hook dialling	•	•	•	•
PCX forwarding	•	•	•	•
Paging	•	•	•	•
Personal Assistant	•	•	•	•
Personal code	•	•	•	•
Personal speed dial numbers	•	•	•	•
Private call	•	•	•	•
Programmable function keys	•	•	•	•
Protection of a call against camp-on and camp-on tone	•	•	•	•
Redial (last number redial)	•	•	•	•
Release-reseize	•	•	•	•
Remote forwarding	•	•	•	•
Remote substitution	•	•	•	•
Roaming				
Screening (manager station)	•	•	•	•
Screening (assistant station)	•	•	•	•
Seamless handoff				
Select the display language	•	•	•	•
Select the ring tone and adjust its volume level	•	•	•	•
Select the type of alphabetical keyboard			•	•
Select the type of calls to be forwarded	•	•	•	•
Selective forwarding	•	•	•	•
Selective monitoring	•	•	•	•
Broker	•	•	•	•
Station lock/unlock	•	•	•	•
Sub-address	•	•	•	•
Supervised call ringing	•	•	•	•
Supervised transfer	•	•	•	•
Switch to normal or restricted mode				•
Teamwork	•	•	•	•
Temporary memory	•	•	•	•
Text answering	•	•	•	•
Text mail	•	•	•	•

	4008, 4018	4019	4028, 4029	4038, 4039, 4068
Transfer of two external lines	•	•	•	•
Transfer to Voice Mail Unit (VMU)	•	•	•	•
Trunk allocation	•	•	•	•
Unassigned night answer	•	•	•	•
Unsupervised transfer (on camp-on)	•	•	•	•
Unsupervised transfer (on no answer)	•	•	•	•
User-to-User Signalling (receiving)	•	•	•	•
User-to-User Signalling (sending)			•	•
Voice mail unit	•	•	•	•
Wake-up				
Unavailable (Withdraw from group)	•	•	•	•

table 3.320 : Services Offered on Other Sets

Service \ Station	First	Easy	Premium	Advanced	Analog (Z)	DECT[1]
Account code before setting up a call	•	•	•	•	•	•
Account code during communication	•	•	•	•		•
Amplification of the handset audio	•	•	•	•		
Amplified reception		•	•	•		•
Answering a call (automatic connection)	•	•	•	•	•	•[2]
Answering a call (manual connection)		•	•	•		•
Answering camped-on calls	•	•	•	•	•	•
Appointment reminder		•	•	•		•
Auto. call setup on going off hook	•	•	•	•	•	•
Auto-answer mode (intercom mode)			•	•		
Automatic call-back request on busy station	•	•	•	•	•	•
Automatic call-back request on busy trunk group	•	•	•	•	•	•
background music		•	•	•		
Block dialling mode		•	•	•		•
Broadcast call (receive)		•	•	•		
Broadcast call (send)	•	•	•	•	•	•

Service \ Station	First	Easy	Premium	Advanced	Analog (Z)	DECT[1]
Call by collective speed dial number	•	•	•	•	•	•
Call parking and parked call retrieval	•	•	•	•	•	•
Call pick-up within a group	•	•	•	•	•	•
Calling Line Identification Restriction (CLIR)	•	•	•	•	•	•
Camp-on on busy station or group	•	•	•	•	•	•
Cancel all active forwardings	•	•	•	•	•	•
Common hold (and retrieval)	•	•	•	•		•
Conversation mute		•	•	•		•
Conference	•	•	•	•	•	•
COnnected Line identification Presentation (COLP)		•	•	•		•
COnnected Line identification Restriction (COLR)	•	•	•	•	•	•
Connection handoff						•
Consultation of camped-on caller identities				•		
Contrast of the display and icons		•	•	•		
Deferred callback request (leave a)	•	•	•	•	•	•
Deferred callback request (receive a)	•	•	•	•	if LED	•
Dial by name		•	•	•		•
Digit-by-digit dialling mode	•	•	•	•	•	•
Direct internal or external call by programmed key	•	•	•	•		•
Display correspondent's name or number		•	•	•		•
Display date and time		•	•	•		•
Do Not Disturb (DND)	•	•	•	•	•	•
DTMF end-to-end signalling	•	•	•	•	•	•
Dynamic routing	•	•	•	•	•	•
Enquiry call	•	•	•	•	•	•
Exclusive hold (and retrieval)	•	•	•	•	•	•
External forwarding	•	•	•	•	•	•
Fax Notification		•	•	•		•
Follow-me	•	•	•	•	•	•

Station / Service	First	Easy	Premium	Advanced	Analog (Z)	DECT[1]
Forced DTMF end-to-end signalling	•	•	•	•	•	•
Forward on busy	•	•	•	•	•	•
Forwarding to pager	•	•	•	•	•	•
Gain switch forcing	•	•	•	•		
General tracking	•	•	•	•	•	
Hands free			•	•		•
Headset mode manual or automatic response			•	•		
Station identity (number and name)		•	•	•		•
Identity of the sub-device connected to the station		•	•	•		
Immediate forwarding of group calls	•	•	•	•	•	•
Immediate forwarding of personal calls	•	•	•	•	•	•
Indication of the cost of a communication		•	•	•		•
Individual call pickup	•	•	•	•	•	•
Interphone barge-in (intrusion) on free	•	•	•	•		•
Internal group call	•	•	•	•	•	•
Internal station call	•	•	•	•	•	•
Barge-in	•	•	•	•	•	•
Keypad dialling features		•	•	•		•
Main PCX recall (calibrated loop break)	•	•	•	•	•	•
Malicious call identification	•	•	•	•	•	•
Count total recall		•	•	•		•
Name/Number display selection during ringing or conversation				•		•
Non-answered calls repertory		•	•	•		•
On-hook dialling	•	•	•	•		
PCX forwarding	•	•	•	•	•	•
Paging	•	•	•	•	•	•
Personal Assistant	•	•	•	•	•	•
Personal code	•	•	•	•	•	•
Personal speed dial numbers	•	•	•	•		•

Service \ Station	First	Easy	Premium	Advanced	Analog (Z)	DECT[1]
Private call	•	•	•	•	•	•
Programmable function keys	•	•	•	•		•
Protection of a call against camp-on and camp-on tone	•	•	•	•	•	•
Redial (last number redial)	•	•	•	•	•	•
Release-reseize		•	•	•		
Remote forwarding	•	•	•	•	•	•
Remote substitution	•	•	•	•	•	•
Roaming						•
Screening (manager station)		•	•	•		
Screening (assistant station)		•	•	•		
Seamless handoff						•
Select the display language		•	•	•		•
Select the ring tone and adjust its volume level	•	•	•	•		•
Select the type of alphabetical keyboard				•		
Select the type of calls to be forwarded	•	•	•	•		•
Selective forwarding	•	•	•	•	•	•
Selective monitoring		•	•	•		
Broker	•	•	•	•	•	•
Station lock/unlock	•	•	•	•	•	•
Sub-address		•	•	•		•
Supervised call ringing		•	•	•		•
Supervised transfer	•	•	•	•	•	•
Switch to normal or restricted mode				•		
Teamwork		•	•	•		•
Temporary memory	•	•	•	•		
Text answering		•	•	•		
Text mail		•	•	•		•
Transfer of two external lines	•	•	•	•	•	•
Transfer to Voice Mail Unit (VMU)	•	•	•	•	•	•
Trunk allocation	•	•	•	•	•	•
Unassigned night answer	•	•	•	•	•	•
Unsupervised transfer (on camp-on)	•	•	•	•	•	•

Service \ Station	First	Easy	Premium	Advanced	Analog (Z)	DECT[1]
Unsupervised transfer (on no answer)	•	•	•	•	•	•
User-to-User Signalling (receiving)		•	•	•		•
User-to-User Signalling (sending)				•		
Voice mail unit	•	•	•	•	•	•
Wake-up	•				•	
Unavailable (Withdraw from group)	•	•	•	•	•	•

[1] Alcatel Mobile Reflexes 100, Alcatel Mobile Reflexes 200, Alcatel-Lucent 300 DECT Handset and Alcatel-Lucent 400 DECT Handset

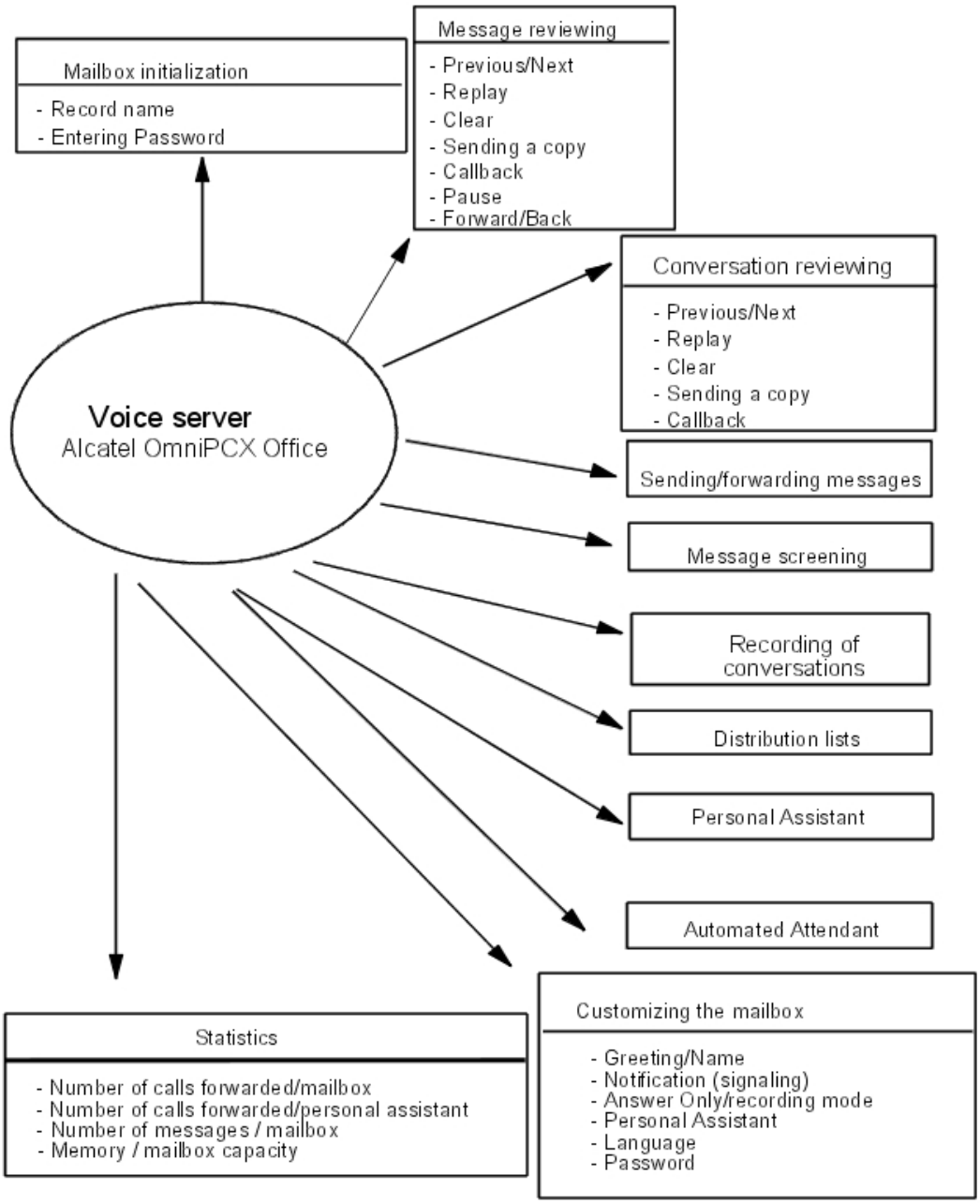
[2] Not available on Alcatel-Lucent 300 DECT Handset.

Chapter 4 Voice Mail

4.1 General Presentation

4.1.1 Overview

The voice server (VMU: Voice Mail Unit) is an integrated Alcatel-Lucent OmniPCX Office Communication Server application which offers the following functions:



4.1.2 Services provided

4.1.2.1 AVAILABLE FEATURES

4.1.2.1.1 BASIC SERVICES

- **Voice Mail Unit**: all the standard voice mail features are provided, including screening, personal assistants, and a mailbox for every user.

- **VMU ports**: 2 ports are provided for voice mail access in Connected mode; they are included in the VMU group (1st system group) and in the default Attendant group.
- **Message storage capacity**: 60 minutes

4.1.2.1.2 OPTIONAL SERVICES

The following services can be accessed with the appropriate software licences:

- **VMU ports**: up to 8 ports; each new port is added to the VMU group and the default Attendant group automatically (or by the installer).
- **Message storage capacity**: the message storage capacity can be extended up to 4 hours with an XMEM128-1 board and up to 200 hours with a hard disk.
- **Automated Attendant**
- **Audiotex**
- **Distribution lists**
- **Recording of conversations**

Note:

If the Automated Attendant is not open, calls pass through to the general mailbox.

4.1.3 Characteristics

4.1.3.1 OPERATING MODES: CONNECTED/APPLICATION/CSTA

4.1.3.1.1 Application mode (or VMU user with the Mail key)

This mode can only be used by Alcatel-Lucent OmniPCX Office Communication Server system users. The voice server is not affected by incoming calls, but is activated like any other system application - in this case, by a Mail key or by dialling the Mail code defined in the internal numbering plan.

If the required DSP resources (monitoring, recording, and MF detection for analog terminals) are unavailable, the server will not be activated.

User interface

In this mode, the method for navigating through the voice server menus depends on the type of terminal:

- **Alcatel-Lucent 8/9 series (except Alcatel-Lucent IP Touch 4008/4018, Alcatel-Lucent 4019 Digital Phone) and Advanced stations** : operations are performed using soft keys and are guided by hints on the display.
- **Alcatel-Lucent IP Touch 4008/4018, Alcatel-Lucent 4019 Digital Phone, Easy and Premium stations**: operations are performed using the keypad and are guided by hints on the display as well as by voice prompts and the dynamic menu called up by the **i** key.
- **First and analog stations**: operations are performed using the keypad and are guided by voice prompts.

Port assignment

Analog ports are not used in Application mode.

4.1.3.1.2 Connected mode (or user with VMU group access code)

In this mode:

- the VMU is accessed by dialling the VMU group directory number (in France, 500).
- the Automated Attendant is accessed by dialling the Attendant group (in France, 9)
- Audio Text is accessed via the DID and internal numbering plans.

If the required DSP resources (tracking recording, silence/noise, DTMF) are unavailable, the activation of the server is postponed and the user is camped on.

User interface

In this mode, navigation is performed with the aid of voice prompts, depending on the type of terminal.

Port assignment

The CPU board provides from 2 to 8 ports, meaning that up to 8 users in Connected mode can simultaneously access the Voice Mail Unit, the Automated Attendant and Audiotex.

Port addresses: 91-001-1 to 91-008-1; all ports are seen at all times; those that are not "In Service" are seen as "Out-of-Service".

Each service is accessed using the number of a group containing one or more ports. A same port can be assigned to one or more groups.

Reaction on VMU busy

If the server is called by a port directory number, the system recognises two types of busy status:

- 1st-degree busy (up to 2 calls on the same port): new calls are camped on until the port is released.
- 2nd-degree busy (more than 2 calls on the same port): new calls are immediately rejected.

If the server is called by a group number, call distribution on group busy is applied; the caller is camped on the group, depending on the number of terminals in the group.

4.1.3.1.3 CSTA

This is used when the server is accessed via the CSTA interface; for details of how this is used, see “Visual Mailbox Interface".

4.1.4 Limits

4.1.4.1 SYSTEM LIMITS

4.1.4.1.1 Global constraints (dependent on software keys)

- 2 to 8 VMU ports
- Storage capacity 60 minutes (CPU-4 without extension memory), 4 hours (with XMEM128-1) or 200 hours (with hard disk)
- 2 to 4 languages

4.1.4.1.2 Voice mail unit

- 250 user mailboxes + 1 general (or common) mailbox

- up to 51 distribution lists (including one broadcast list for all users)
- recording times are limited:

Service	Limit	Default value
Welcome message	120 seconds maximum with a hard disk on the CPU. 30 seconds maximum without hard disk	None
Mailbox name	Max. 5 seconds	None
Message recording	Max. 180 seconds	120 seconds
Recording a conversation	Depends on voice server storage capacity	
Remote notification message	Max. 20 seconds	

- access to certain features may be barred or dependent on access rights

Service	Barring	Access right
Remote message notification	YES	YES
Remote consultation of a mailbox after message notification	N/A	YES
Recording a conversation	N/A	YES
Personal Assistant	YES for external destinations	NO
Remote Configuration	N/A	YES for the configuration of remote notification parameters

4.1.4.1.3 Automated Attendant

- recording times are limited:

Service	Limit	Default value
Company welcome message	Max. 120 seconds	None
Announcement menus and sub-menus	Max. 120 seconds	None
Goodbye message	Max. 20 seconds	None

- users with the necessary rights may customise Automated Attendant messages remotely (this feature right must be enabled for the user in the OMC Feature Rights screen)

4.1.4.1.4 Audiotex - information messages

- up to 50 information messages
- recording times are limited:

Service	Limit	Default value
Company welcome message	Max. 20 seconds	None
Goodbye message	Max. 20 seconds	None
Information message	Max. 240 seconds	120 seconds

4.1.5 Configuration examples

4.1.5.1 CONFIGURATION TOOLS

The voice server is configured using the system configuration tool OMC. **The configuration PC must have a sound card** to record the welcome messages and the Automated Attendant menus (for more information, see "Voice prompts management" in the section "OMC: System configuration").

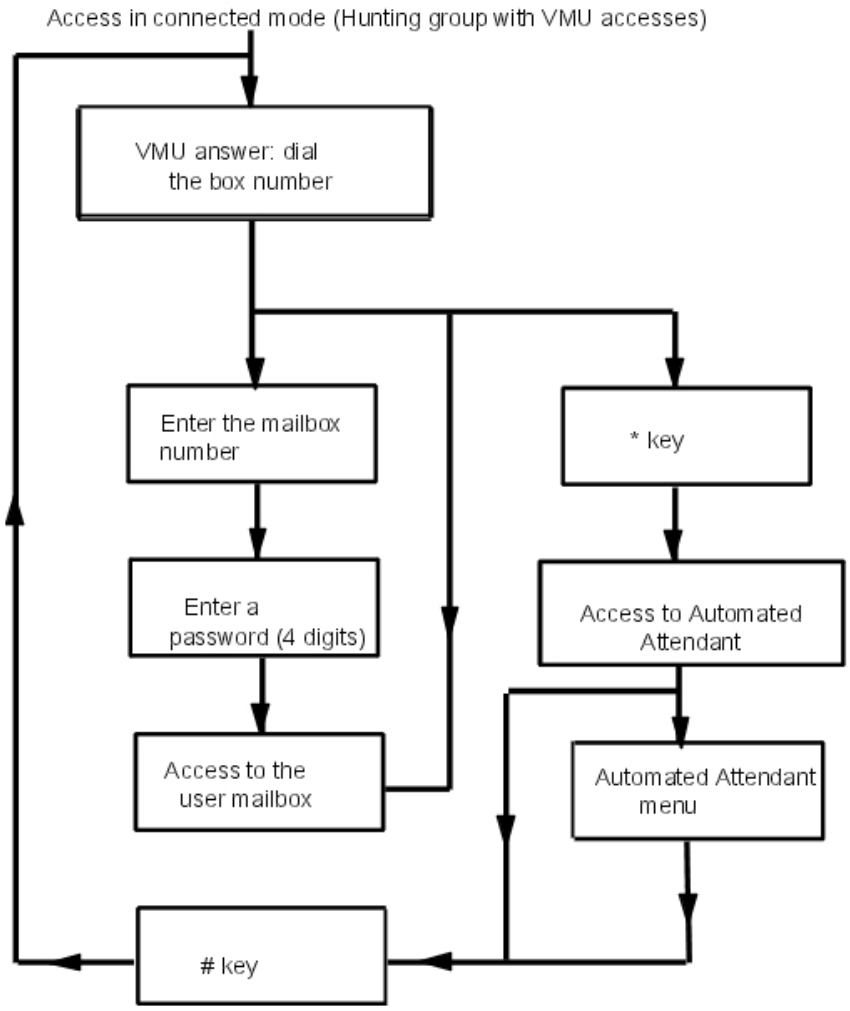
If the PC does not have a sound card, the MMC-station can be used to record business welcome messages and good-bye messages, Automated Attendant menus and sub-menus, Audiotex messages, distribution list names and the welcome message for the general mailbox.

4.2 System Operation

4.2.1 Accessing VMU/the attendant

4.2.1.1 Overview

4.2.1.1.1 ACCESS TO THE VMU OR TO THE AUTOMATED ATTENDANT



Note:
*You can switch from the VMU to the Automated Attendant at any time by pressing the * key and switch back again by pressing the # key.*

4.2.2 Automated attendant

4.2.2.1 Overview

4.2.2.1.1 Description

The Automated Attendant is only accessible in voice server Connected mode:

- by dialing the company's public number (incoming calls to Attendant group containing VMU accesses);
- by dialing the VMU group number (internal call) or the directory number for the VMU port.

The user then presses the * key to access the Automated Attendant Main menu;

- exclusively by dialing the VMU group number if the Mailbox Access flag (**OMC -> Voice Processing -> General Parameters -> Mailbox Consultation**) is inactive;
- By dynamic routing:
  - level 1: an internal or external call is routed through to the user's mailbox if it exists. If not, the "no mailbox" default function is activated and the call goes through to the Automated Attendant.
  - level 2: an external call is routed through to the Attendant group; if there is no answer, the default Attendant group is used and the call goes through to the Automated Attendant (if the VMU ports are included in the default Attendant group).
  - level 1 or 2: if the "Auto. Attendant (lev.1)" or "Auto. Attendant (lev. 2)" flags are activated at the station's dynamic routing level.

The Automated Attendant greets the caller with the company welcome message and transfers the call to the appropriate destination. To establish communication, all the possibilities open to the caller are set out in a Main voice menu and/or submenus.

The Automated Attendant can be customized to suit the individual requirements of the company. For this reason, the range of options available during working hours is different from that offered out of working hours. There are consequently two Automated Attendant menus, completely independent from each other. The switch between the "Opening Hours" menu and the "Closing Hours" menu can be made either manually by the Administrator (by forcing restricted or normal mode) or automatically, according to a pre-programmed schedule defined in the system opening hours settings (opening hours = normal mode, closing hours = restricted mode).

The Automated Attendant is multilingual: the voice prompt language can be selected by the caller.

Note 1:

Only the menus of the main language can be customized.

Note 2:

If multi language is selected, Automated Attendant submenus are no longer available.

The Automated Attendant greetings (for opening and closing hours) can be configured remotely by users with sufficient rights (set in the OMC Feature Rights screen), allowing new greetings to be recorded or the default greetings to be restored.

Call processing example

For a more detailed look, take the example of a caller picked up by the Automated Attendant. First of all, the caller hears the company welcome message. Then he is instructed to press the star key (optional).

The "Press Star" question is a specific function for establishing whether the caller has a set with a voice frequency keyboard.

He can then select the language for the voice prompts (optional).

The caller now comes to the Automated Attendant Main menu, in which specific menus are assigned to the keyboard keys. He can choose from the proposed Main menu functions:

- Free dialing: the caller is prompted to dial an internal destination number.
- Transfer to user: the caller is routed to a predefined internal number.
- Transfer to attendant: the caller is routed to the Attendant station.

- External transfer: the caller is routed to an external number. If the transfer recipient is not available, the transfer fails and the call returns to the Automated Attendant main menu.

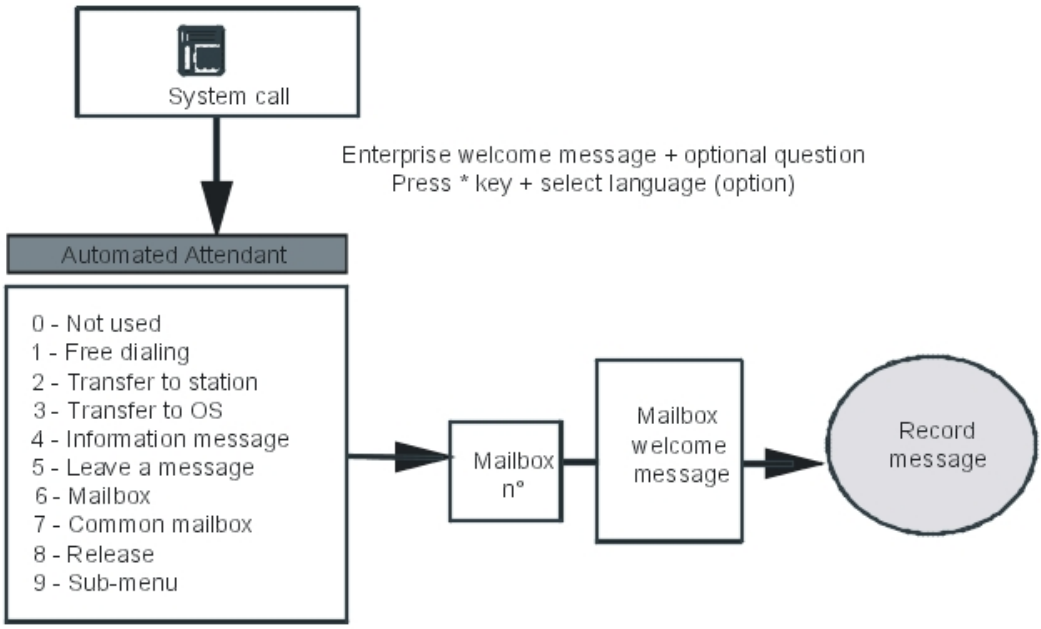
  Remark:
  external transfer is applied after configuration of a speed dial number in OMC (Voice Processing/ Automated Attendant/Automated Attendant Menu/Transfer to Station/Group).

- Information message: the caller hears an information message that may be chained with other information messages.
- General mailbox: the caller is routed to the general mailbox.
- Leave a message: the caller is prompted to enter a mailbox number in order to leave a message.
- Mailbox: the caller is routed to a predefined mailbox.

Note 3:

The possibilities available on initialization are specific to each country and to the software license level.

Example of Automated Attendant structure



4.2.2.1.2 Default function

The "Default function" is obtained when the caller fails to choose a function from the proposed list or when the application cannot interpret his choice (the caller may not have a voice frequency terminal).

On initialization, the default function is "Transfer to Attendant".

4.2.2.1.3 Direct call

The Automated Attendant can be used at a simple level, replacing the Main menu with a single

possibility. The Direct Call function routes the caller directly to a predefined function after the welcome message and the optional "Press Star" and "Select Language" questions.

4.2.2.1.4 Consulting a mailbox

Once he has got through to the Automated Attendant, the caller can access his mailbox directly (if he has one) by pressing the # key and entering his user number and password. For a more detailed description, see the "Consulting a mailbox" section under "Services available to users".

Note:

This possibility is not announced by the voice server.

4.2.2.2 Configuration procedure

4.2.2.2.1 Configuration

- To record the 2 welcome messages (opening hours/closing hours):

• By OMC (Expert View): **Voice Processing -> Automated Attendant -> Greeting** -> **Opening Hours/Closing Hours**-> **Voice Prompt - Greeting** • By MMC-Station: **VMU -> AutoAt -> Day** or **Night**

- To record the good-bye message:

• by OMC (Expert View): **Voice Processing -> Automated Attendant -> Good-bye** -> **Voice Prompt - Good-bye** • By MMC-Station: **VMU -> AutoAt -> Gdbye**

- To enable/disable the "Press Star" question:

• By OMC (Expert View): **Voice Processing -> Automated Attendant -> Greeting** -> **Opening Hours/Closing Hours** -> **"Press Star" question**

- To enable/disable the "Select Language" question:

• By OMC (Expert View): **Voice Processing -> Automated Attendant -> Greeting** -> **Opening Hours/Closing Hours** -> **"Select language" question**

- To define the "Direct Call" function (opening hours/closing hours):

• By OMC (Expert View): **Voice Processing -> Automated Attendant -> Greeting** -> **Opening Hours/Closing Hours** -> **Single function AA**

- To define the action to be taken in the event of transfer to a non-existent mailbox or in answering-only mode:

• By OMC (Expert View): **Voice Processing -> Automated Attendant -> Greeting** -> **Opening Hours/Closing Hours** -> **Mailbox function**

- To define the "Default" function (opening hours/closing hours):

• By OMC (Expert View): **Voice Processing -> Automated Attendant -> Greeting** -> **Opening Hours/Closing Hours** -> **Automated Attendant function**

- Choose the type of transfer:

• by OMC (Expert View): **System Miscellaneous** -> **Memory Read/Write** -> **Misc. Labels** -> **"AATypTrf" = 0 if blind transfer or = 1 if semi-supervised transfer"** • by MMC-Station: **Global -> Rd/Wr -> Address -> "AATypTrf = 0 if blind transfer or = 1 if semi-supervised transfer" -> Return -> Memory**

4.2.2.2.2 Remote Configuration

The Automated Attendant welcome messages can be configured remotely, from an external telephone. For each greeting (opening hours greeting and closing hours greeting), you can:

- listen to the current greeting
- record a new (custom) greeting
- restore the default greeting (in which case the custom greeting is lost)

Note:

If no custom greeting has been recorded (or is currently in the system), the default greeting will play.

In order to remotely configure the Automated Attendant greetings, you must have sufficient rights. The corresponding feature right (remote customization of company greeting) must be enabled for an individual user in the OMC Feature Rights screen reached via the following path:

- By OMC (Expert View): **Subscribers/Basestations List -> Details -> Features**

For a user with sufficient rights, the procedure to remotely configure the Automated Attendant greetings is as follows:

1. Dial into your mailbox and respond to the voice guide as described in the following steps.

2. Select the Personal option.

3. Within the Personal option menu, select option 5 to customize the company greetings.

4. Select the greeting you wish to access:
- Press 1 for the opening hours greeting.
- Press 2 for the closing hours greeting.

5. Select the action you wish to perform:
- Press 1 to record a new (custom) greeting.
- Press 2 to listen to the current greeting.
- Press 3 to restore the default greeting.

When recording a new greeting, start to speak after you have pressed 1 and use the # key to stop the recording when required. Once the recording has stopped, you are asked to either accept the recording by pressing # (again) or start the recording again by pressing the * key.

6. If you need to modify the other greeting, return to Step 3.

4.2.2.2.3 Additional Information

- 2 types of transfers are offered: semi-supervised transfer or blind transfer.
- Semi-supervised transfer: The Automated Attendant only transfers calls to available internal users:

  - if the user does not answer: the call is transferred and dynamic routing is activated.
  - if the user is busy (degree 1 or 2): the call is not transferred and the user is returned to the Automated Attendant Main menu.
- Blind transfer: The Automated Attendant transfers calls to available internal or busy grade 1 users:
  - if the user does not answer: the call is transferred and dynamic routing is activated.
  - if the user is grade 1 busy: the call is transferred and put on hold: the call on hold is indicated on the destination set display.
  - if the user is busy grade 2: the call is not transferred and the user is returned to the Automated Attendant Main menu.
- For outside transfers, there is no grade 1 busy state; if the transfer recipient is not available, the transfer fails and the call comes back to the Automated Attendant Main menu.
- Role of the * key
  - on connection to the Automated Attendant: the business welcome message and the "Press Star" question are skipped and the caller is prompted to select his preferred language (if configured) or is put through directly to the Main menu.
  - while listening to an information message:
    - if the caller accessed the information message from the Automated Attendant Main menu, pressing the * key while listening to the message returns the caller to the Main menu, where all the options are listed.
    - if the caller accessed the information message from one of the Automated Attendant sub-menus, pressing the * key while listening to the message returns the caller to the sub-menu, where all the options are listed.
- Role of the # key
  - on connection to the Automated Attendant: the caller can consult his mailbox (if he has one); during the business greeting, "Press Star" question and "Select Language" question are skipped.
  - while listening to an information message: enable the user to skip the message.

4.2.3 Audio Text

4.2.3.1 Overview

4.2.3.1.1 Description

An Audiotex consists of a sequence of information messages.

2 mutually independent Audiotex services are provided: one for opening hours, the other for the company's closing hours.

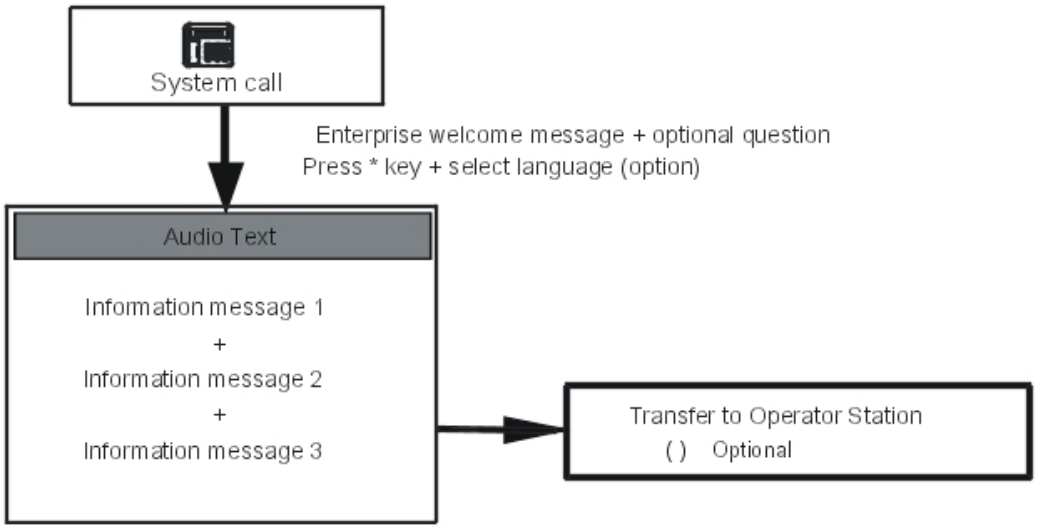
One can switch between them either manually or automatically, using the same time ranges as defined in the Alcatel-Lucent OmniPCX Office Communication Server system.

4.2.3.1.2 Activation

Audiotex can be accessed in either of 2 ways (if a menu is available for access to an information message):

- by an external call - dialling the Audiotex DID number, or

- by an internal call - dialling the internal number for the Automated Attendant.



When the caller dials the DID number for the Audiotex service, he automatically hears the business welcome message. The next two steps are optional:

- He is asked to press the * key to check that he has a voice frequency terminal (this option can be configured by OMC);
- Then he can select his preferred language for navigating in Audiotex (configurable using OMC).

Finally he will be put through to the first information message; this message may be chained to others or followed by forwarding to the Attendant, for example.

4.2.3.1.3 Default function

The default function is obtained when the application cannot interpret the numbers dialled by the caller (for example, at the end of an information message, the caller is prompted to dial the number of the person he wants to contact) or if the caller does not dial a choice. This default function is identical to the one used for the Automated Attendant and must be configured from within the Automated Attendant (see "Default function" in the "Automated Attendant" chapter).

4.2.3.1.4 Role of the * and # keys

- * key:
  - on connection to Audiotex: the company's welcome message and "Press Star" question are skipped and the caller is prompted to select his preferred language (if configured) or is played the first information message.
  - while listening to a message: the voice server is released after playing a good-bye message.
- # key: skips the current information message and moves on to the next

4.2.3.2 Configuration procedure

4.2.3.2.1 Message configuration

- To set the first information message:

By MMC-OMC (Expert View): **Voice Processing -> Information Messages -> Audio Text**

- To set the information messages:

By MMC-OMC (Expert View): **Voice Processing -> Information Messages**

Number of configurable messages: 50
The various functions at the end of the welcome message are only available with OMC:

- Not used: if the caller is in the Automated Attendant, then he is returned to the previous level; if the caller is in Audiotex, the good-bye message is played and the voice server is released.
- Free dialling: the caller is prompted to dial an internal destination number.
- Transfer to user: the caller is routed to a predefined internal number.
- Transfer to attendant: the caller is routed to the Attendant station.
- Information message: the caller is played an information message.
- General mailbox: the caller is routed to the general mailbox.
- Leave a message: the caller is prompted to enter a mailbox number in order to leave a message.
- Mailbox: the caller is routed to a predefined mailbox.
- Release: the call is released after playing a good-bye message.

- To record the information messages:

• By MMC-OMC (Expert View): **Voice Processing -> Information Messages** • By MMC-Station: **VMU -> InfMsg**

- To record the 2 welcome messages (day and night):

By MMC-Station: **VMU -> AudTx -> Day** or **Night**

- To record the good-bye message:

By MMC-Station: **VMU -> AudTx -> Gdbye**

- To enable/disable the "Press Star" question:

By MMC-OMC (Expert View): **Voice Processing -> Information Messages ->Audio Text -> Opening Hours/Closing Hours -> "Press Star" question**

- To enable/disable the "Select Language" question:

By MMC-OMC (Expert View): **Voice Processing -> Information Messages ->Audio Text -> Opening Hours/Closing Hours -> "Select language" question**

4.2.3.2.2 Configuration of the Audiotex DDI number in the numbering plan

1. Open an OMC session.
2. Go to the **Numbering Plans** window by clicking **Numbering** and then **Numbering Plans**.

3. Select the **Restricted Public Numbering Plan** tab.
4. From the **Function** drop-down menu, select **Audiotex**.
5. Complete the fields:
   - **Start** and **End**: these fields contain the DDI call number of the system Audio Text service consisting of 8 characters maximum from 0 to 9, * and #.
   - **Base**: in general, the base is equal to the internal directory number of the automated attendant. It is used to ensure correspondence between the DDI number of the Audio Text and the internal directory number (IDN) of the automatic attendant. This correspondence is based on the formula IDN = DDI number of Audio Text service - Start + Base.

   All incoming calls are routed to Audio Text. The caller is played the welcome message, then the information message. He can then access the services configured.

4.2.4 Managing Mailboxes

4.2.4.1 Operation

4.2.4.1.1 MANAGING MAILBOXES

Description

On initialization, every subscriber in the installation is automatically allocated a mailbox (except analog Z stations).

Each mailbox can operate in any of 3 modes. The operating mode of each mailbox is configured by the installation Administrator (standard mode on initialization):

- **Mailbox in standard mode**
  This mode provides access to a range of functions. The owner can switch between standard mode and answering-only mode, but not into guest mode.
- **Mailbox in guest mode**
  This mode, designed for Hotel use, offers more limited functions. Only the "Leave Message" and "Consult Message" functions are available; any caller can leave a message to be consulted by the guest, but under no circumstances can the guest send any messages. The password is only required when the guest remotely accesses his mailbox. The guest cannot switch his mailbox into standard or answering-only mode.
- **Mailbox in answering-only mode**
  This mode can be adopted by users who do not want to receive messages; the caller hears the welcome message but cannot leave a message, then the server releases the call (if a personal greeting has been recorded).
  The owner of a mailbox in answering-only mode can switch it into standard mode and vice versa (see "Customization"), but not into guest mode.

First access

When the mailbox is used for the first time, the messaging service must be activated from the terminal in Application mode. The user is then asked to enter a password and register his name; the mailbox is then initialized.

If the user accidentally activates the voice mail unit in while Connected, he will find that he is refused access to his mailbox.

Subsequent accesses can be made in Application mode or Connected mode (see "Operating modes: Connected/Application/CSTA")

Note:

*The password is only required if the parameter **Password required for mailbox access** (OMC -> Voice Processing -> General Parameters) is selected; if not, the password is not necessary.*

Deleting a mailbox

The Administrator can delete mailboxes. If the mailbox contains messages (read or unread), these are kept for X minutes and can be accessed/reviewed by the user while in Application; if the mailbox is assigned to someone else within the period of X minutes, the messages are lost.

Deleting mailboxes

From version R2.0, you may use OMC to delete the mailboxes of all the selected users: **Users/Basestations List -> Del. Mailboxes**

Dead mailbox timeout durations:

- System is in "Business" mode: timeout X = 5 minutes
- System is in "Hotel" mode: timeout X = 50 minutes

This value can be modified in OMC (unit = 100 milliseconds; min value = 0; max value = 32767 i.e. about 54 minutes): **System Miscellaneous -> Memory Read/Write -> Debug Labels -> DeadMbTo**

Non-Existent Mailbox

This function offers the following possibilities in the event of a call being forwarded or put through by the Automated Attendant to a non-existent mailbox:

- Not used: the caller is routed to the Automated Attendant (default setting).
- Free dialing: the caller is prompted to dial an internal destination number.
- Transfer to user: the caller is routed to a predefined internal number.
- Transfer to attendant: the caller is routed to the Attendant station.
- Information message: the caller is played an information message chained with the welcome message.
- General mailbox: the caller is routed to the general mailbox.
- Leave a message: the caller is prompted to enter a mailbox number in order to leave a message.
- Mailbox: the caller is routed to a predefined mailbox.
- Release: the call is released after playing the good-bye message.

Note:

This function is also activated for mailboxes in Answer Only mode when the user has not customized the greeting.

Configuration

- To define the type of each mailbox:

- by OMC (Expert View): **Users/Base stations List -> Users/Base stations List -> Details** -> **Mailbox** -> **Options** -> **Mailbox Mode**
- By customization: **MbxAnn** -> **Mode** -> **Select**

- To define the action to be taken in the event of transfer to a non-existent mailbox or in answering-only mode:

- By OMC (Expert View): **Voice Processing -> Automated Attendant -> Greeting** -> **Opening Hours/Closing Hours** -> **Mailbox function**

Voicemail for attendant groups

On initialization and unlike the handsets, there is no automatic allocation of voicemail to groups.

From version R2.0, it is possible to allocate, by OMC, a voicemail to each group via the configuration of a virtual terminal; virtual terminals correspond to physical addresses 96-001-01, 96-002-01, etc.).

The virtual terminal is configured in diversion on the group concerned; in fact the group is called by the directory number of the terminal.

Remote customization enables a name to be allocated to a voicemail, a welcome message to be recorded or the password to be changed (the default password is used to access the mail in on-line mode while the mailbox is not initialized).

Should the current password be lost, it is possible, for a virtual terminal to retrieve the default password by **OMC ->List of Subscribers/Basestations ->Details -> Personal code -> Reset**.

The allocation of a Voicemail unit key to each dedicated handset of the group enables these handsets to:

- be alerted to a new message in the group voicemail.
- to check the group voicemail; while voicemail is not initialized, access by this key prompts the start up of the initialization sequence (change of password and saving of the name).

Dynamic routing must be configured to direct unanswered calls to the VMU (500) group.

Configuration

- To create virtual terminals (one per group):

- By OMC (Expert View): **Subscribers/Base stations List -> Subscribers/Base stations List -> Add -> check "Virtual Terminals" and enter the number**

- To allocate a voicemail to each virtual terminal:

- By DHM-OMC (Expert View): **Subscribers/Base stations Lists -> List of Subscribers/Base stations -> Details -> Voicemail -> "Yes" to the question "Subscriber XXX does not have voicemail, do you wish to create one?"**

- To allocate to each attendant group a Voicemail unit key:

- by OMC (Expert View): **Subscribers/Base stations List -> Subscribers/Base stations List -> Details -> Function Key = Voicemail Unit**.

Note:

After a cold reset, ensure voicemail is reallocated to the virtual terminals in an orderly fashion, that is, to the related groups following the order of creation prior to the reset.

4.2.5 Managing the General Mailbox

4.2.5.1 Operation

4.2.5.1.1 MANAGING THE GENERAL MAILBOX

Description

On initialisation, a general (or common) mailbox is created. This mailbox, accessible in access/review-only mode from the Attendant station, enables the messages left there to be forwarded to other users in the installation.

The caller accesses the general mailbox via the Automated Attendant or Audiotex, providing the General mailbox function has been configured by the Administrator.

Activation

The general mailbox is accessed from an Attendant station or from another station belonging to the installation (equipped with soft keys) by:

- pressing the fixed Mail key
- pressing the GalMbx soft key
- enter the Attendant password ('help1954' by default).

Note 1:

For stations with soft keys and with a number pad, proceed as follows:

- press the fixed Mail key.
- press the Voice key.
- press the Return or code * key.
- enter the general mailbox number (= operator/attendant call number as defined in the internal numbering plan, 9 for example).
- enter the Attendant password ('help1954' by default).

Note 2:

To access the general mailbox while in Connected from inside or outside the company, it is necessary to change the attendant's password so that it contains numbers only (corresponding to Q23 frequencies) and no letters.

Additional Information

- Not being assigned to any individual user, the general mailbox cannot be customised; only the welcome message can be configured.
- For the Attendant, there is no difference in the way general mailbox and private mailbox messages are notified.
- As with other mailboxes, the general mailbox can only be accessed by one station at a

time.

- When the attendant forwards messages left in the general mailbox, the transfer data (identification, date and time) are those of the initial message.
- The operator station can use the general mailbox in the dynamic routing, attendant diversion and/or restricted mode services; then, the Automated Attendant will be used with a direct call to the general mailbox access. The operator can redirect the external incoming calls to the general mailbox. Different solutions are available (in all cases, the Automated Attendant will be dedicated to the direct function "General Mailbox"; to do this, it is mandatory to record (by OMC -> Automated Attendant) a welcome message and to activate the Direct Access = General mailbox function):
  - **dynamic routing after X seconds to the general mailbox in the event of no answer from the Attendant:** to do this, program for the OS group nº 1 (or the current group within the time range) a level 1 dynamic routing to group 500 (default group containing the VMU accesses) with a timeout of X seconds. It is also possible to program a level 2 dynamic routing at general level if the VMU accesses are configured in OS group nº 8.
  - **Immediate forwarding to general mailbox:**
    - 1st solution: use Attendant group Forwarding towards the group containing the VMU accesses (group 500 by default).
    - 2nd solution: use restricted mode provided the VMU accesses are in OS group nº 8.

Configuration

- To record the general mailbox welcome message:

- By MMC-OMC (Expert View): **Voice Processing -> Mailboxes -> General Mailbox** -> **Voice Prompt - General Mailbox**
- By MMC-Station: **VMU -> GalMbx**

4.2.6 Distribution list

4.2.6.1 Overview

Distribution lists enable users to send and copy messages to all the members on the list simply by dialing the list name or number.

The system allows for a maximum of 51 lists to be compiled:

- 1 general broadcast list (number 000); this list is used to send a message to every voice mailbox in the system
- 50 distribution lists (001 to 050)
- distribution lists can only be configured by the installation Administrator.

4.2.6.2 Configuration procedure

4.2.6.2.1 Configuration

- To configure the distribution lists by means of users' directory numbers:

- By MMC-OMC (Expert View): **Voice Processing -> Mailboxes -> Distribution Lists**
- By MMC-Station: **VMU -> List**

Note:

The content of distribution lists cannot be deleted or modified by the users.

- To record the distribution list names:

- By MMC-OMC (Expert View): **Voice Processing -> Mailboxes -> Distribution Lists**
- By MMC-Station: **VMU -> List** -> **Record**

- To key in the distribution list names:

- By MMC-OMC (Expert View): **Voice Processing -> Mailboxes -> Distribution Lists**
- By MMC-Station: **VMU -> List** -> **Edit**-> **Name**

4.2.7 Statistics

4.2.7.1 Overview

4.2.7.1.1 Description

The statistics are intended for:

- the administrator or operator (i.e. the person responsible for managing the messaging service on the client side)
- the maintenance service (the distributor, for example).

The statistical function gathers data on the voice server and how it is used. The counter readings correspond to the server activity since the last Reset.

Depending on the results, appropriate changes can be made to the settings in order to improve the service.

4.2.7.2 Operation

4.2.7.2.1 Statistics on the Automated Attendant

- To read and reset the counters:

By MMC-OMC (Expert View): **Voice Processing -> Statistics** -> **Automated Attendant**

- Number of calls received by the Automated Attendant (= number of times the welcome message was heard).
- Duration of calls for the Automated Attendant.
- Number of failed calls (no response to the "Press Star" question or no caller selection in the Automated Attendant Main menu).

Note:

*All of these counters can be reset using the **Reset** function.*

4.2.7.2.2 Statistics on Audiotex

- To read and reset the counters:

By MMC-OMC (Expert View): **Voice Processing -> Statistics** -> **Audiotex**

- Number of calls received by Audiotex (= number of times the welcome message was heard).
- Length of calls for Audiotex.
- Number of aborted calls (no response to the "Press Star" question or no selection by caller in the Audiotex main menu).

Note:

These statistics are provided for opening and closing hours. All of these counters can be reset using the ***Reset*** *function.*

4.2.7.2.3 Information messages statistics

- To read and reset the information message counters:

By MMC-OMC (Expert View): **Voice Processing -> Statistics** -> **Information Messages**

- Number of times each information message was heard (via the Automated Attendant or Audiotex).

4.2.7.2.4 Mailbox statistics

- To read and reset the mailbox counters for all users:

By MMC-OMC (Expert View): **Voice Processing -> Statistics** -> **Mailboxes**

- Number of calls received by each user (= number of times the welcome message was heard).
- Number of calls received by the personal assistant of each terminal.
- Number of messages left by callers.
- Length of recording of the messages not read by each user.
- Length of recording of the messages read by each user.
- Length of recording of conversations by each user.

4.2.7.2.5 Statistics on VMU resources

- To read and reset the counters:

By MMC-OMC (Expert View): **Voice Processing -> Statistics** -> **Resources**

- Accumulated total of voice messages as a percentage of available memory capacity.
- Record of use over the last 7 days.

4.2.8 Hotel features

4.2.8.1 Overview

4.2.8.1.1 HOTEL FEATURES

This chapter deals exclusively with the features provided in Hotel mode (as opposed to Business mode, which concerns all the other chapters).

Check-in

When guests check in, they are automatically allocated a mailbox; its mode of operation (guest mode), the password, and the language used for the voice prompts are all assigned automatically on check-in.

On consulting the mailbox for the first time, the guest must enter a password and register his or her name. Until the name has been registered, the guest cannot consult his or her mailbox.

Consulting the mailbox

First consultation

Until the user name has been registered, the guest cannot access his or her mailbox. The first consultation must be in Application mode (by dialing the Mail code or pressing the Mail key); the guest is put directly through to his mailbox and must only register his name.

Subsequent consultations

The mailbox can subsequently be consulted in Application mode or in Connected mode (by dialing the VMU or port number).

In Connected mode, the guest has to enter his mailbox number followed by his password. The password may be read by the operator station via the "Hotel" key.

In Application mode, the guest is directly connected to his messages.

The messages received are automatically played back in sequence. The guest can replay messages and use the Return, Pause, Next or Delete functions. Messages that have been listened to but not deleted are kept.

Check-out

When the guest checks out, the mailbox is automatically unallocated if it contains no messages. If any messages remain, they are kept for 50 minutes, after which time the mailbox is definitively deleted. They can be consulted in all modes.

4.3 User Services

4.3.1 Users interfaces

4.3.1.1 Overview

4.3.1.1.1 Description

The interface available for using the voice server depends on the type of terminal:

- **stations without displays**: voice prompts only; the options offered by the voice prompts are selected using the keypad.
- **stations with displays but without soft keys**: voice prompts as well as display menus (using the keypad to navigate.

Voice prompt guidance can be disabled using Customization (it is enabled on initialization).

- **stations with soft keys**: navigation is done exclusively with soft keys, depending on the menu displayed.

4.3.1.1.2 Specific functions

The # key can be used for:

- confirming the previous data
- skipping the current voice prompt and moving on to the next (e.g. skipping a mailbox greeting to go straight to the recording stage, or skipping a message in order to access the processing options: replay, delete, callback, send a copy, etc.).
- accessing a mailbox from within the Automated Attendant.

Note:

*For decadic stations, the **9** key is used in place of the # key.*

The ***** key can be used for:

- deleting an item of data
- returning to the previous menu.
- returning to the Automated Attendant menu from the Mailbox menu.

The **0** key can be used to access any additional menu options when a user accesses his or her mailbox.

4.3.1.2 Configuration procedure

4.3.1.2.1 Configuration

- To set the maximum waiting time for a response from the user (input a value, for example: 5 seconds by default, configurable from 5 to 15 seconds in 1-second increments):

• By MMC-OMC (Expert View): **Voice Processing -> General Parameters** -> **Timeout for user's response**

- To set the number of times the server should repeat messages requiring a response from the user (to input a value, for example): 2 by default, configurable from 0 to 5:

• By MMC-OMC (Expert View): **Voice Processing -> General Parameters** -> **Number of warnings if no response**

4.3.2 Initializing mailboxes

4.3.2.1 Detailed description

4.3.2.1.1 Description

Mailboxes are initialized by their owners when they entering their individual passwords and register their names. These operations are performed when the mailbox is first opened (**Application mode only**).

4.3.2.1.2 Mise en service

Service	Sets without soft keys	Sets with soft keys (SK)
Initialization on first access	F.K.: **Mail** FK (or "Mail" code) + Password + Record name	F.K.: **Mail** FK + Password + Record name

4.3.2.1.3 Additional Information

- On first opening the mailbox: while recording the name, the user can (these options are displayed, but not announced in the voice prompt):
  - restart the recording from the beginning (* key);
  - stop and terminate the recording (# key).

4.3.3 Consulting a mailbox

4.3.3.1 Detailed description

The diagram on the next page summarizes the mailbox access steps and options.

4.3.3.1.1 Description

This service enables users to call their mailbox and listen to any messages received (whether new or already heard), listen to recorded conversations, send messages, or remotely configure some mailbox parameters (see appropriate paragraph).

This service is protected by a password (the same as for the subscriber). In Application mode however consultation is possible without a password, depending on the state of the mailbox consultation flag (**OMC -> Voice Processing -> General Parameters -> Mailbox Consultation**). The default value is no password.

4.3.3.1.2 Commissioning

Users access their mailboxes:

- in Application mode:
  - sets with a fixed Mail key: using this key (or the appropriate code)
  - stations with displays: Voice key + password
  - stations without displays: password.
  - stations without a fixed Mail key: Mail service code or programmed key + password

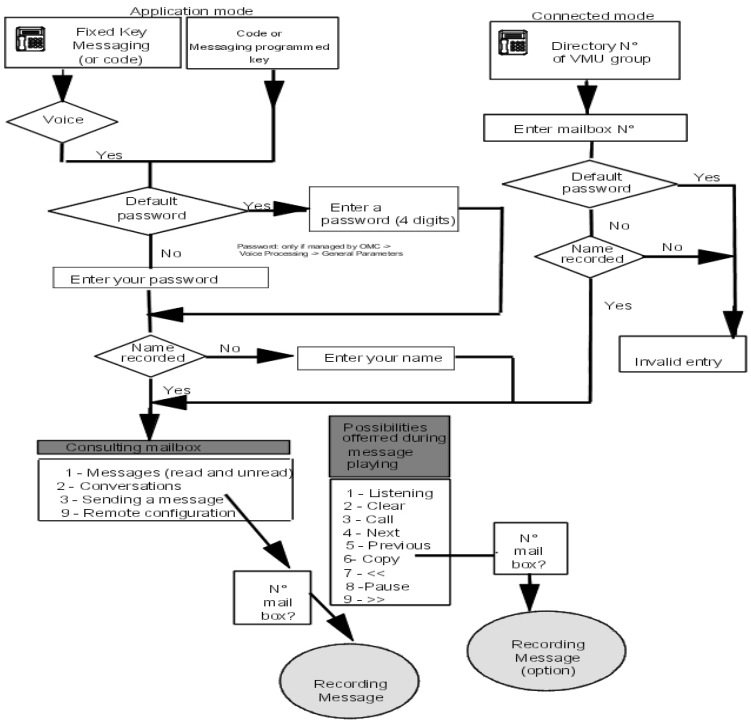
4.3.3.1.3 Additional Information

- The new message notification mode (voice prompt on going off-hook, LED or icon) depends on the type of terminal; for analog sets with a LED, a virtual key has to be created. Conversation recordings are not notified.
- Number of messages/conversations:
  - stations with display: the number of messages (old and new) and the number of conversations recorded are displayed at the start of the access.
  - stations without displays:
  - case 1: mailbox containing new messages only: a voice prompt indicates the number of new messages.
  - case 2: mailbox containing old messages only: a voice prompt indicates the number of messages already heard.

- case 3: mailbox containing new and old messages: only the number of new messages is announced.
- case 4: the number of conversations is never announced.

- When accessing the mailbox (Connected or Application mode) the "Mailbox -> Please enter the mailbox number" menu can be opened by pressing the ***** key before entering the password (this enables users to access their chosen mailbox).

- **Email notification of new messages:**
  In R2.0 (Premium solutions only), an Email (HTML format, or text format if display with HTML is not possible) is sent when a new message is left in the mailbox. The voice mail is sent as an attachment in the form of a .WAV file (16 bits, 8 kHz). A voice mail that has been listened to via e-mail is still regarded as a new message when accessing the mailbox.
  Via the WBM, access the **User Settings** window. In the **Voice messages** field of the **Absence** tab, check the **Display voice message as an attachment (WAV)** box to be notified when a voice message is deposited in the box and to listen to it. For more information, see the User and User groups section.



4.3.4 Playing back messages

4.3.4.1 Detailed description

4.3.4.1.1 Description

If at least one message has been left, the user can play back the messages in his mailbox, using a range of possible functions (delete, next, replay, send a copy, call back, etc).

Messages are played back in two series: the new messages first, then the old ones. Each series is in chronological order.

4.3.4.1.2 Caller identification

While the messages are played back, the terminal display indicates:

- the name of the caller - if known, and if the user has the corresponding feature rights
- otherwise, the caller's number
- **** if the caller has activated the CLIR or “Secrecy" service
- “Unknown" if the caller number is not recognized by the system.

The identity of the caller is never announced.

4.3.4.1.3 Date and time

The date and time of arrival are displayed on the terminal and announced before the message is played back.

4.3.4.1.4 Call-back

When the caller's identity is known to the system (Calling Line Identification Presentation), this service enables the user to immediately call back correspondents (whether internal or external) who leave a message. The call-back number can contain a maximum of 20 digits. Call-back can be requested while still listening to the message, or afterwards.

There are several possibilities:

- **Internal call**: internal callers can be called back without restriction.
  - If the VMU was activated in Connected mode, the transfer is of the semi-supervised type:
  - if the user does not answer: the call is transferred and dynamic routing to the called-back station is activated.
  - if the user is busy (degree 1 or 2): the call is not transferred and the user is returned to the message playback menu.
  - If the VMU was activated in Application mode, the transfer is of the blind type: the application transfers the call regardless of caller status and immediately goes on-hook; if the call-back fails, the user has to hang up and call back the VMU (or press Redial).
- **External call**: the call-back of external callers is governed by barring mechanisms. The VMU transfers the call when the connection is established (correspondent off-hook) or simulated.

4.3.5 Sending messages

4.3.5.1 Detailed description

4.3.5.1.1 Description

From the consultation menu, the user can send a voice message directly to the recipient's mailbox by performing the following operations:

- pressing the Send soft key or dialing code 3
- defining the destination(s) for the message
- recording the message; validating the message sends it to its destination.

4.3.5.1.2 Defining the destination

The destination can be:

- the user's name (display terminals only)
- a distribution list name (display terminals only)
- the user's directory number (up to 8 digits)
- a distribution list number (000 to 050).

Note:

If the terminal has soft keys, the user can browse the destination list. He can then:

- go to the next member
- go back to the previous member
- delete a member
- delete all the members in the list
- insert a distribution list.

4.3.5.1.3 Recording the message

While recording the message, the user can pause (key 8) and then continue the recording (key 8 again). He can also stop the recording (# key) or start over from the beginning (* key). These options are available even though they are not announced (they are displayed, however).

4.3.6 Sending copies of messages

4.3.6.1 Detailed description

4.3.6.1.1 Description

This function is identical to sending a message except that the user can also add an introduction (a comment telling the recipient that the message is a copy).

4.3.7 Filtering mails

4.3.7.1 Detailed description

4.3.7.1.1 Description

This function enables users, with the terminal on idle, to monitor messages being left and answer a call if desired.

4.3.7.1.2 Activation/Deactivation

Service	**Activation/Deactivation**
To activate filtering	P.K.: **VMU: Filtering** + Password
Deactivate filtering	P.K.: **VMU: Filtering**
Deactivate call monitoring	P.K.: **VMU: Filtering**: stops monitoring and deactivates filtering. Fixed **End** key: monitoring of the filtered call is deactivated; the user cannot replay the message currently being filtered, but filtering remains active for other incoming calls, which can still be monitored.

4.3.7.1.3 Additional Information

- The set's speaker is automatically activated when the message is left.
- This function is only available for idle sets with programmable keys and a loudspeaker.
- The messages that can be filtered correspond to calls to users with fixed or dynamic routing on their lines; messages sent from a mailbox cannot be filtered.
- The general mailbox cannot be filtered; messages sent from the "Mailbox" menu cannot be filtered.
- Filtering can only be activated for a single message at a time.
- If filtering is activated while a message is being left, there is no effect.
- The call can be answered by pressing the “Hands Free" key or going off-hook. The part of the message left before answering is wiped. After going back on hook, filtering remains active for any new incoming call.

4.3.8 Remote notification

4.3.8.1 Overview

4.3.8.1.1 Description

This feature notifies users when someone has left a message for them; a call is sent by the voice server. On answering, the recipient can access his/her mailbox, if the service is active.

Notification can be validated for a specific time period.

4.3.8.2 Configuration procedure

4.3.8.2.1 Configuration

- To enable external notification, for each user:

- By MMC-OMC (Expert View): **Subscribers/Base stations List -> Subscribers/Base stations List -> Details -> Voice Mailbox -> Notification** -> check **? The subscriber is allowed to activate notification**

In the case of external notification, the call is subject to restrictions.

- To activate remote notification of messages in mailbox, for each user:

- By MMC-OMC (Expert View): **Subscribers/Base stations List -> Subscribers/Base stations List -> Details -> Voice Mailbox -> Notification ->** check **? Notification activated**
- By customization: **Notif** (or **5)** -> **On/Off** (or **1)**

- To set the internal or external destination to be notified, for each user (in the case of external numbers: 22 digits max., including trunk code):

- By MMC-OMC (Expert View): **Users/Base stations List -> Users/Base stations List -> Details -> Mailbox -> Notification ->** -> **Notification Destination**
- By customization: **Notif** (or **5)** -> **Desti** (or **2**)

- To define the type of notification, for each user (with or without access to mail):

- By MMC-OMC (Expert View): **users/Base stations List -> Users/Base stations List -> Details -> Mailbox -> Notification ->** -> **Kind of Notification**

- To define the applicable time range for notification, for each user:

- By MMC-OMC (Expert View): **Users/Base stations List -> Users/Base stations List -> Details -> Mailbox -> Notification** -> **Notify Destination**
- By customization: **Notif** (or **5**) -> **Sched** (or **3)**

- To define, for all users, the delay before the 2nd and 3rd notification call (the default values are country-specific):

- By MMC-OMC (Expert View): **Voice Processing -> Mailboxes -> Misc.**-> **Notification: Minutes till second/third alert**

4.3.9 Recording a conversation

4.3.9.1 Overview

4.3.9.1.1 Description

This function enables authorized users to record ongoing telephone conversations. The recorded conversation is stored, with its date and time stamp, in the user's mailbox.

4.3.9.2 Operation

4.3.9.2.1 Activation/Deactivation

Type of station / Service	Sets without soft keys	Stations with soft keys
To activate recording	P.K.: **VMU: Conversation Recording** or dial the function code	S.K.: **Record** SK with pause and re-record options
Deactivate recording (the conversation continues)	P.K.: **VMU / Conversation Recording** or dial the function code	S.K.: **Stop**

4.3.9.3 Configuration procedure

4.3.9.3.1 Configuration

- To authorize conversation recording, for each user:

• By MMC-OMC (Expert View): **Subscribers/Base stations List -> Subscribers/Base stations List -> Details -> Voice Mailbox -> Options** -> check **? Recording of conversation allowed**

- To program a key with the “Conversation recording" function:

• By MMC-OMC (Expert View): **Users/BasestationsList -> Users/Basestations List -> Details -> Keys** -> **Voice Mail: Conversation recording**.

4.3.9.3.2 Additional Information

- The maximum recording time depends on the server's memory capacity.

4.3.10 Playing back recorded conversations

4.3.10.1 Detailed description

4.3.10.1.1 Description

This function enables authorized users to listen to the conversations they have recorded, using replay, delete, send a copy, call-back, etc.

Conversations are played back in reverse chronological order.

4.3.10.1.2 Activation/Deactivation

Type of station / Service	Sets without soft keys (with display)	Stations with soft keys
To activate playback	Fixed **Mail** key + **1** + Password + **2**	Fixed **Mail** key + **Voice** SK + Password + **Conv SK**

4.3.11 Personal assistant

4.3.11.1 Overview

4.3.11.1.1 Description

Incoming calls forwarded to the voice server are routed to the user's mailbox or the user's

personal assistant (depending on the configuration).

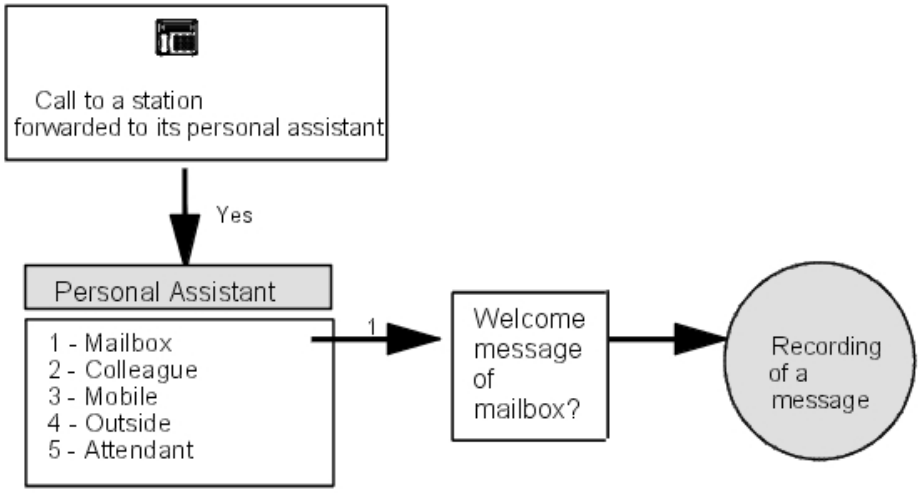
If the call is forwarded to the personal assistant, the caller is put through to the Main menu, enabling him for example to leave a message (so that he can be called back) or to be transferred to the recipient's mobile terminal.

For the caller, forwarding to the mailbox or personal assistant is guided by voice prompts only.

If the personal assistant is activated:

- the caller is informed that the person cannot be reached
- he then listens to the various options offered by the personal assistant (transfer to the operator station or to a predefined internal/external destination)
- then he hears the voice prompt for his chosen option.

Forwarding to the personal assistant is immediate, and is activated from the set customization menu; the personal assistant voice prompt is pre-recorded and cannot be customized.



Note:

Option 1 - Mailbox is proposed automatically, even if the personal assistant has not been configured, whenever the function is validated.

Even if the personal assistant has not been validated, the Operator station can still be reached by dialing the attendant (operator) number during the mailbox announcement (blind transfer to OS).

4.3.11.2 Configuration procedure

4.3.11.2.1 Configuration

- To activate the personal assistant, for each user:

• By customization: **Assist** (or **2)** -> **On/Off** (or **1)**

- To configure, for each user, the options proposed by the personal assistant (in the case of external numbers: 22 digits max., including trunk code):

- By MMC-OMC (Expert View): **Users/Base stations List -> Users/Base stations List -> Details -> Mailbox -> Personal Assistant** -> **Transfer to secretary/operator/home/mobile phone**
- By customization: **Assist** (or **2)** -> **Menu** (or **2**)-> **IntNum, ExtNum, Mobile or Operat** (or **1, 2, 3 or 4**)

- To enable an external caller getting through to a personal assistant to reach an outside number. If these parameters are not configured, the external-to-external transfer will fail (see "Additional information"):
  - For each VMU port: flags **"Join Incoming/Outgoing"** and **"Join Incoming/Outgoing"** are inactive (default values)
  - For each user authorised to effect joinings (and the external forwarding via the personal assistant will also be authorized):

- By MMC-OMC (Expert View): **Subscribers/Base stations List** -> **Subscribers/Base stations List** -> **Details** -> **Features** -> **Part2** -> check **"Join incoming/Outgoing"** and **"Join Outgoing/Outgoing"**

  - For the system as a whole:

- By MMC-OMC (Expert View): **System Miscellaneous** -> **Feature Design** -> **Transfert Ext/Ext**

- by MMC-OMC (Expert View): **System Miscellaneous** -> **Feature Design** -> check **Transfert Ext/Ext by on-hook**

4.3.11.2.2 Additional Information

- Blind transfers are used.
- If the external/external transfer fails, the system's response will depend on the configuration and in particular on the **Go to initiator if transfer fails** notification (accessible via OMC under **System Miscellaneous** -> **Feature Design**):
  - If the notification is not set (the default setting for France, Italy and Spain), the call is routed to the Attendant station.
  - If the flag is positioned (the default setting for all other countries), the voice server is called back in Automated Attendant mode. If the Automated Attendant is not open, the call goes through to the general mailbox.
- Destination number:
  - external numbers must include the network access prefix
  - external numbers are subject to restrictions
  - if the predefined number is invalid or restricted, the call is returned to the personal assistant menu.

4.3.12 Customisation

4.3.12.1 Detailed description

4.3.12.1.1 Description

Customization allows users to define their own set, voice mail and personal assistant settings.

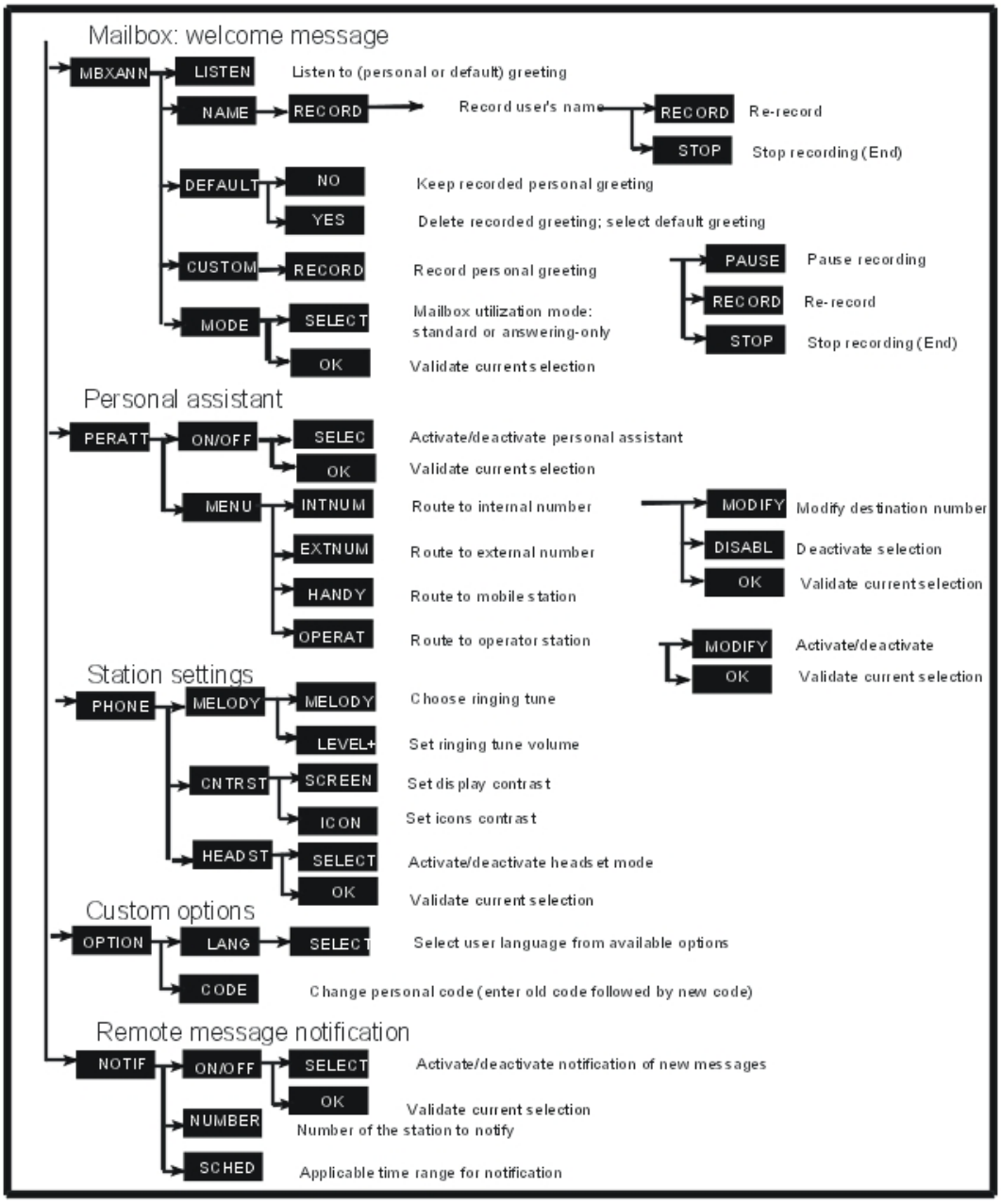
4.3.12.1.2 Switching to Customization mode

Depending on the type of station, press **Custo** (2nd page, Advanced Station in Idle) or **i** + 5, or

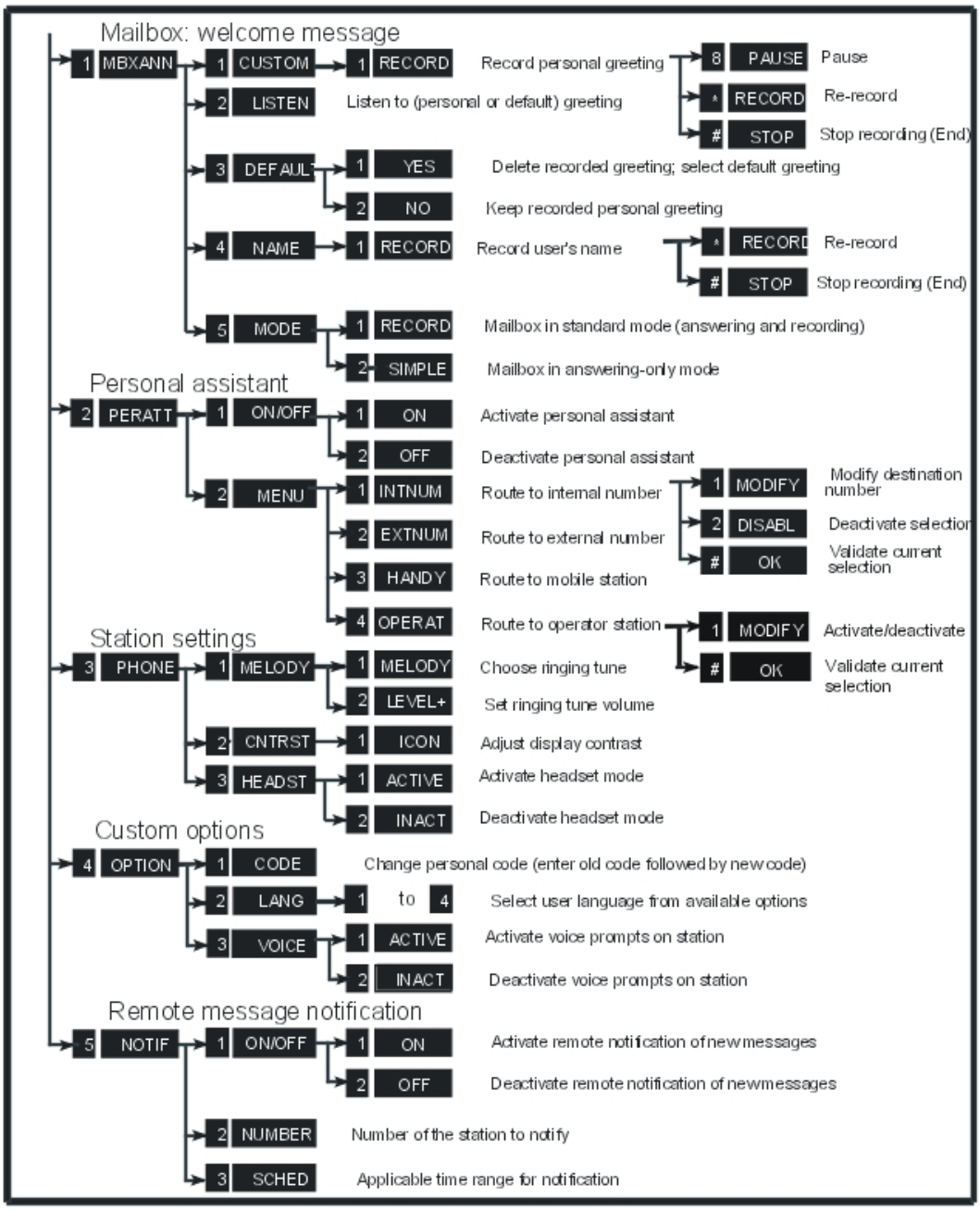
dial the “Programming Mode" function code.

The following pages describe the tree structures available for each type of station; navigation is done using soft keys or codes (with the help of voice guides).

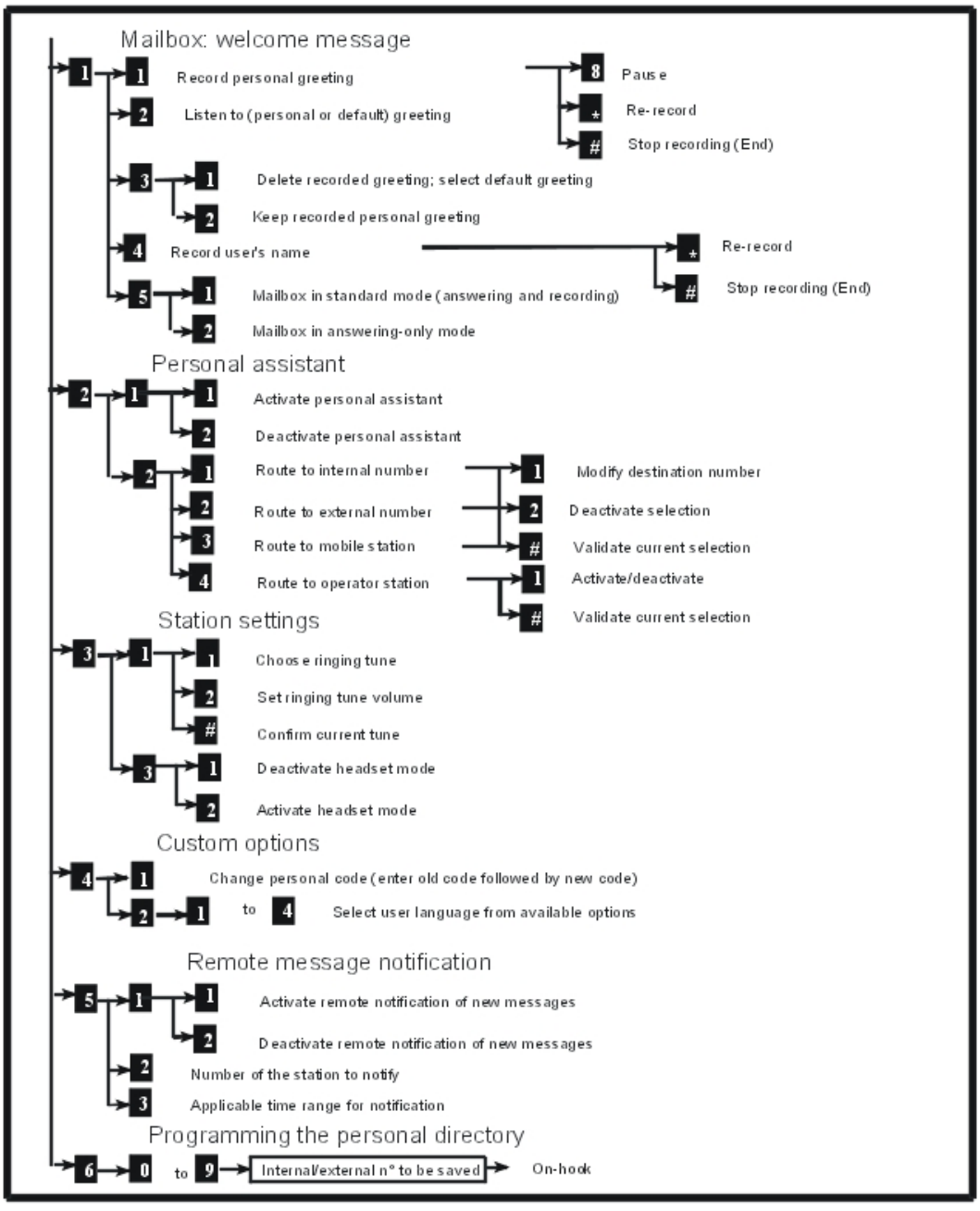
4.3.12.1.3 Stations with soft keys



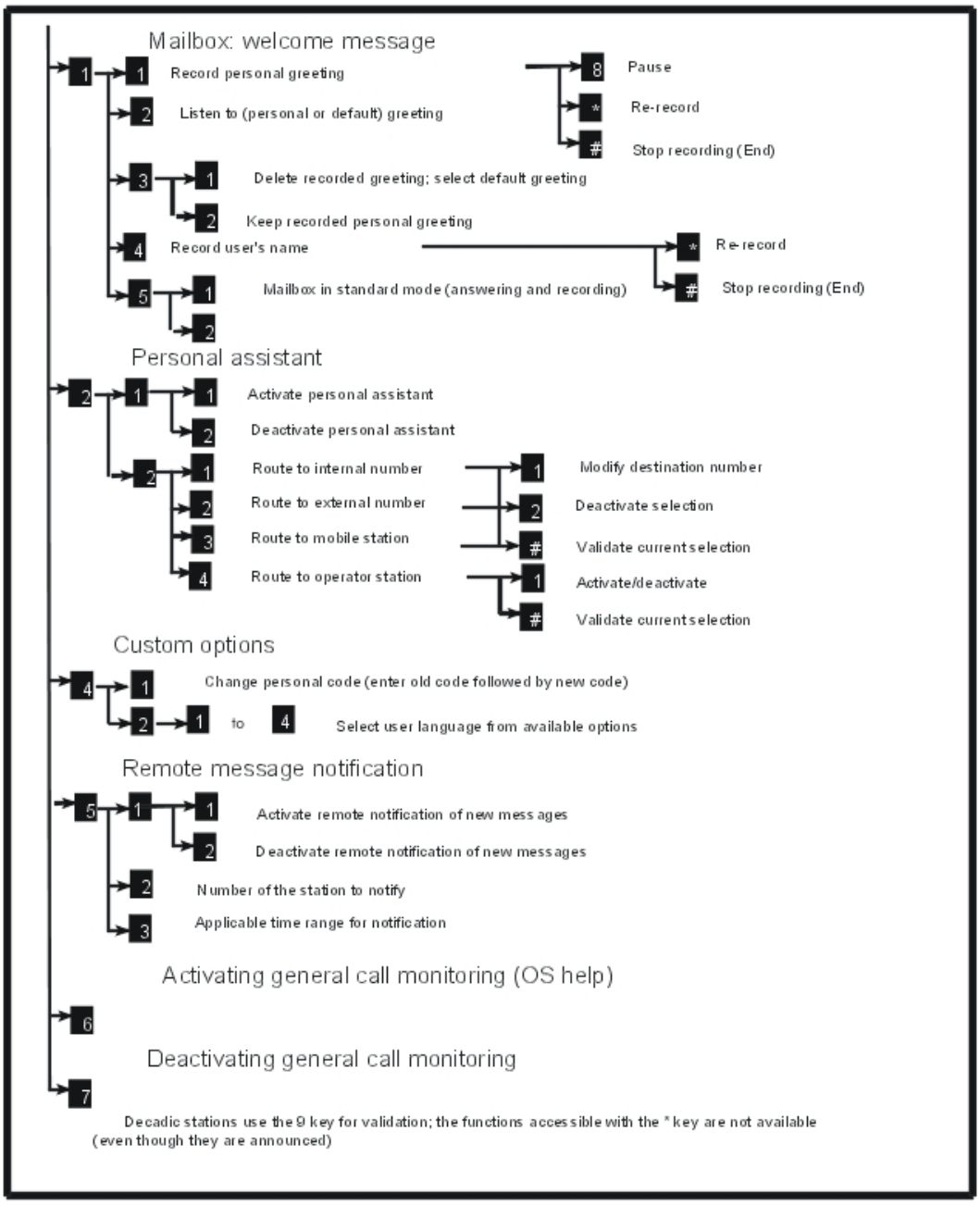
4.3.12.1.4 Stations without soft keys but with displays



4.3.12.1.5 Stations without displays or soft keys



4.3.12.1.6 Analog Z stations



4.3.13 Remote configuration

4.3.13.1 Detailed description

This function (choice 9 in the Mailbox consultation menu) is controlled by a software key.

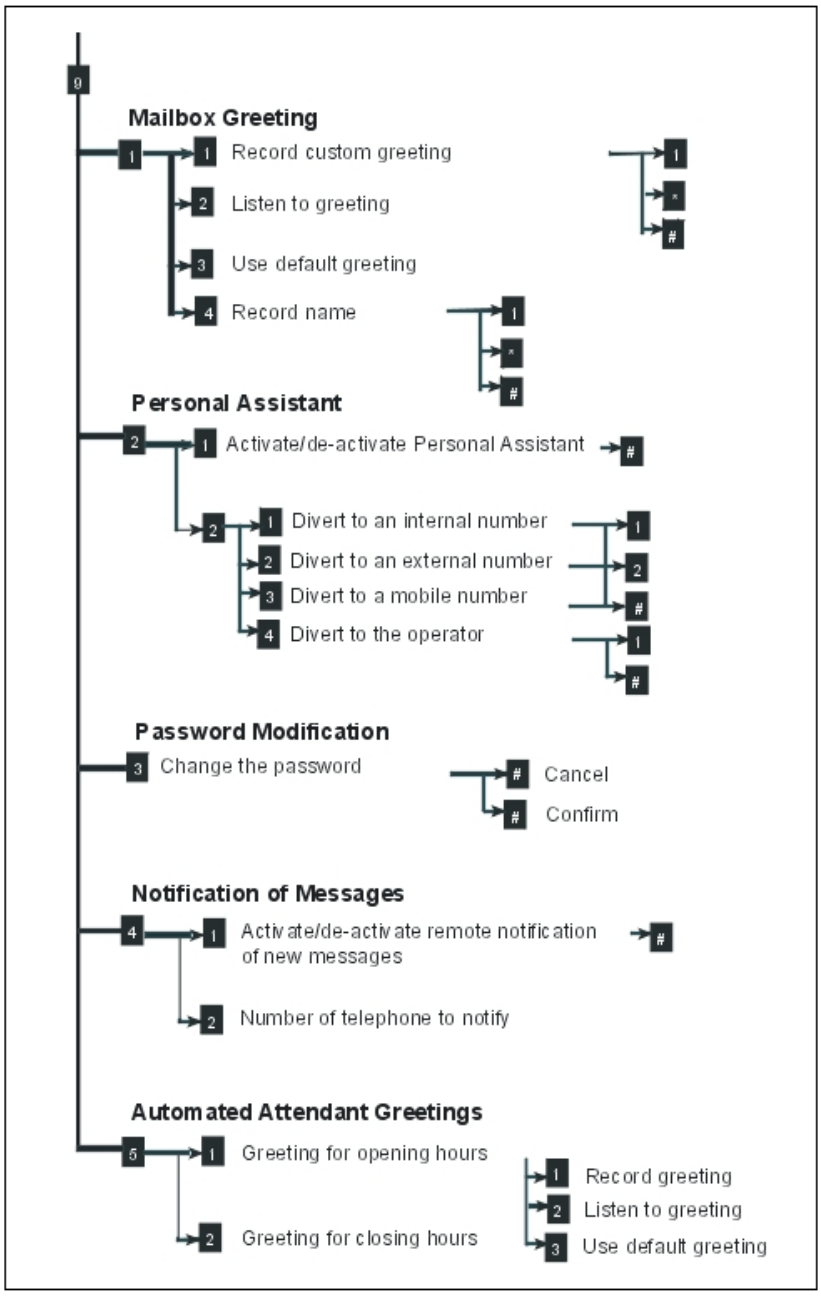
The remote configuration feature allows users who mainly work outside the company to

configure some items in their mailbox. It is part of mailbox consultation and is only offered when connected. Various options are offered, including:

- Recording the mailbox welcome message.
- Activation/deactivation of the personal assistant. Configuration of the personal assistant: configuration and activation of the routing to an internal, external or mobile destination number or to the attendant station.
- Changing Password.
- Remote message notification (only available if user is entitled to use this functionality): activation/deactivation and configuration of internal or external destination.
- Customisation of the Automated Attendant company greetings (for opening hours and closing hours).
- Activation/deactivation of the Nomadic mode: consultation of the current nomadic status (enabled or disabled), activation/deactivation of the Nomadic mode and configuration of the destination phone number.

  This option is offered when the Nomadic right is active for the concerned set and the virtual Nomadic set exists in the configuration.
- Activation/deactivation of immediate call forwarding: consultation of the current forwarding status, configuration and activation of immediate call forwarding to the Voice Mail or to a destination phone number.

The key sequences for the different options are detailed in the figure below.



Note 1:
The remote configuration of the Automated Attendant company greetings can only be performed by users with the necessary rights. The right to this feature must be enabled for the user in the OMC Feature Rights screen.

Note 2:

The remote configuration of Nomadic Mode Settings can only be performed by authorized users. The right to the Nomadic feature must be enabled for the user in the "Central Services User Configuration" OMC screen. At least, one Nomadic Virtual Terminal must be present in the Subscribers list.

4.3.13.2 Authentication

4.3.13.2.1 Overview

To access his/her voice mail box, the external (also called remote) caller must be authenticated.

The user authentication can be performed with:

- The calling party CLI (Calling Line Identification). The CLI received must match the identity of an authorized user
- A DTMF dialogue. On voice guides request, the caller dials his/her personal number and password

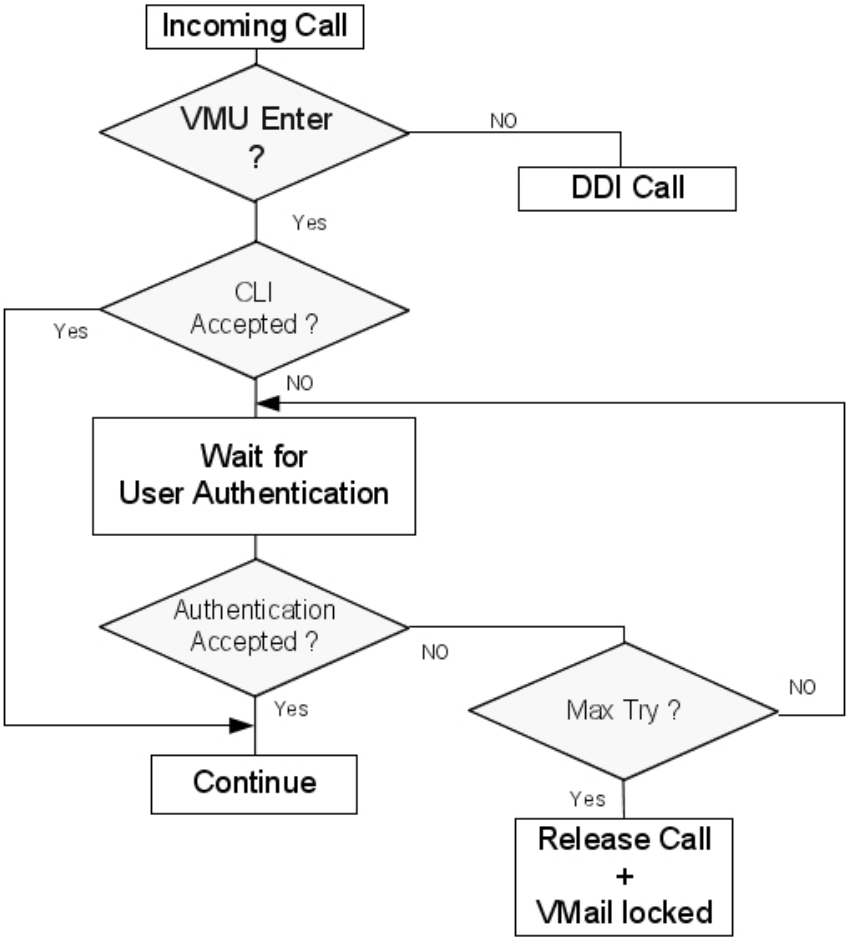


Figure 4.11 : Remote Access Authentication Diagram

4.3.13.2.2 CLI Authentication

For more information on:

- The CLI authentication process: see module Remote Substitution - Operation § Remote Substitution Access
- The CLI authentication configuration: see module Remote Substitution - Configuration procedure § CONFIGURATION

4.3.13.2.3 User Authentication

Overview

The "Password Control" feature is used to enhance security for remote access to voice mails.

To prevent a malicious external caller from finding a user's password and making unlimited calls and inputting passwords, a maximum number of attempts is defined.

When the maximum number of attempts is reached for a user's voice mail, the remote access to the voice mail is blocked.

The Alcatel-Lucent OmniPCX Office Communication Server denies remote access to the voice mail until this number of attempts is reset. This can be done by users on their local phone set, or via PIMphony, or by an attendant.

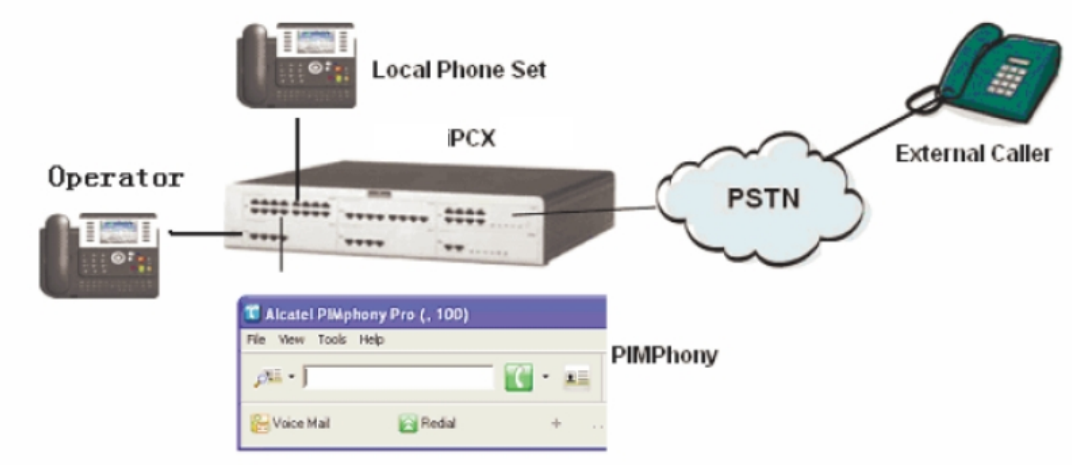


Figure 4.12 : Scenario

Locking Remote Access to Voice Mail

When this "Password Control" feature is active, all the sets of the installation are concerned. This is not a feature which can be activated set by set.

To configure the maximum number of attempts, a noteworthy address can be set - OMC (Expert View) only:

System Miscellaneous > **Memory Read/Write** > **Debug Labels** >**VMUMaxTry** > **Details**

The same "**VMUMaxTry**" value is active for all the sets of the installation.

Values of maximum number of attempts:

- From 0 to 255
- Default value: 20
- 0: no limitation for remote access to voice mails (the feature is disabled)

When the maximum number of attempts is reached, the remote connection is disabled even if the password is correct.

Before releasing the call, a voice-prompt "Remote access to voice mail is currently locked" is played.

Unlocking the Remote Access to Voice Mail

To unlock the remote access to the voice mail, there are three methods:

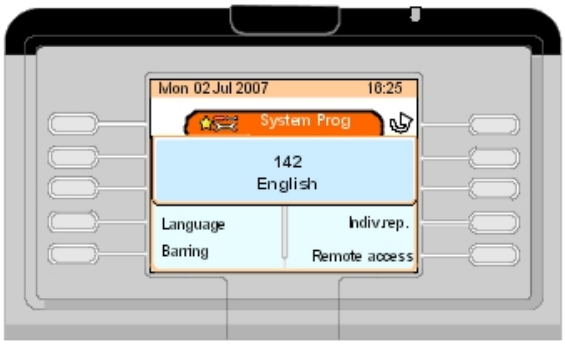
- Local unlocking service
  Users can connect to their voice mail from their local phone set in "application" mode or

"connected" mode using the correct password. Once connected to their voice mail, the remote access to voice mail is unlocked and the number of attempts is reset.

- Remote unlocking service
  The Remote unlocking service is available via the PIMphony application.
  Users can remotely connect to their voice mail via the PIMphony application.
  When users log in successfully, the remote access to voice mail is unlocked and the attempts number is reset.
- Attendant unlocking service
  This service is available on the following sets:
  - Alcatel-Lucent 8 series sets, namely:
    - Alcatel-Lucent IP Touch 4038 Phone
    - Alcatel-Lucent IP Touch 4068 Phone
  - Alcatel-Lucent 9 series sets, namely:
    - Alcatel-Lucent 4039 Digital Phone

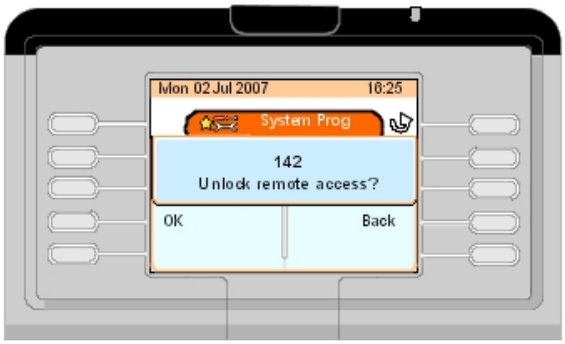
To unlock remote access to the voice mail:

1. Open **Operator session** > **Subscriber**.
   The following screen is displayed:



Note:
If the remote access current state is unlocked, the "Remote access" key is not displayed.

2. Press the "**Remote access**" softkey.
   The following screen is displayed:



3. Click **OK**.
   The remote access is unlocked.

Log Event Notification

When the remote access is locked, the "Voice mail locked" event is saved in the *History Table* (in the OMC application).

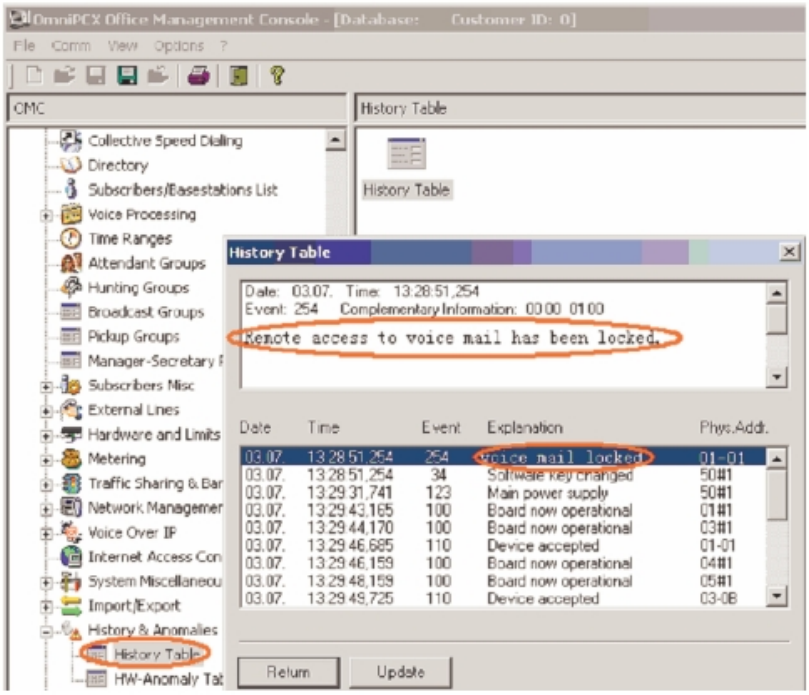


Figure 4.15 : OMC - History Table

Pre-defined Voice Message Notification

When remote access is locked, the user's mailbox receives the following pre-defined voice message: "Remote access to voice mail is currently locked".

Locally: the user is notified by the blinking mailbox led.

Remotely: when logging in, the user is notified by the voice prompt "Remote access to voice mail is currently locked".

4.3.13.2.4 Using the Remote Substitution Service

Using the "remote substitution" service, the user inputs the set number and the user's password (whether the DISA access code is disabled or not).

In case of failure in entering the password, the counter of attempts is increased: the counter is the same as the one used for remote access to voice mail.

When the maximum number of attempts is reached, the "remote substitution" service is locked.

Note:

For the "remote substitution" service, the voice prompt is absent. Then, when the remote access is

locked, the pre-defined voice message is not sent to the user's mailbox and the voice prompt is not played.

4.4 Visual Mail Box Interface

4.4.1 Overview

4.4.1.1 Description

The "Visual Mailbox" interface gives Alcatel-Lucent OmniPCX Office Communication Server users access to mailboxes via the PC-based application PIMphony. It provides:

- easier and more intuitive navigation thanks to the services offered by the integrated voice server;
- direct access to voice server functionality without having to manipulate the telephone.

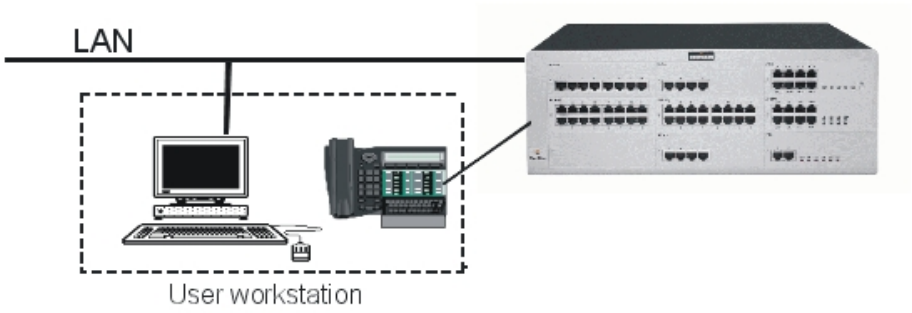
The main services available are:

- Backup messages/conversations on the PC
- Access new mail
- Access recorded conversations
- Insert into Outlook
- Send mail
- Record new messages. Copy messages with or without adding a comment.

The "Visual Mailbox" interface can be used either:

- on the telephone terminal, or
- on the PC, if it has a sound card.

4.4.1.2 Environment



The user workstation consists of:

- a Z, DECT or dedicated terminal (connected to the system by a UA, DECT, analog or IP link) and a PC connected to the LAN (the system must also be connected to the LAN);

- or a multimedia PC (PIMphony IP Edition) connected to the LAN.

4.4.2 Services provided

The application enables you to initialize and configure the password required for access to the messages window.

4.4.2.1 Mailbox supervision

The "Mailbox" icon in the toolbar indicates whether all the messages have been heard or whether there is at least one new message.

Clicking the icon opens the "Visual Mailbox" window, containing information on all the messages and conversations stored in the mailbox:

- date and time of message
- type of message: voice mail or recorded conversation
- caller identity: name registered in PIMphony, PCX name or number
- the length of the message
- message status: new or old.

The information list is updated dynamically each time a message arrives in, or is deleted from, the mailbox, or changes status from "new" to "read". This is represented by 2 distinct icons: the application also synchronizes the status of the LED on the set (signaling the presence or absence of new messages).

4.4.2.2 Handling messages

Messages/conversations are viewed in list form in the "Visual Mailbox" window.

A set of static buttons are available for:

- deleting items
- playing them back
- copying them, with or without a comment
- recording a new message
- creating or displaying the caller's Outlook file
- calling back the person who left the message (if their identity is linked to the voice message).

Dynamic buttons appear during playback.

4.4.2.3 Remote notification of new messages (copy to Outlook mail client)

The "Follow Me" function enables authorized users to receive e-mail on the local PC to advise them that a new message has arrived in their mailbox.

The voice message is inserted as an attachment to a new message in the main Outlook message list.

This option is configurable.

This function requires Outlook to be installed locally.

4.4.2.4 MANAGING THE TERMINAL

4.4.3 Managing the terminal

4.4.3.1 Operation

4.4.3.1.1 Entering VMB mode

The terminal acts as the audio input/output for recording and playback services.

When a new voice mail is detected, the server informs the terminal (the LED flashes) and the PC (the "Mailbox" icon changes state). Pressing the "Listen" key in the "Visual Mailbox" window has the following effect:

- the terminal goes directly to Hands Free mode; alternatively, it rings and the user has to pick up the receiver. The user then hears the new message.
- the display is updated ("Visual Mailbox").
- all the terminal keys except End, Loud+, Loud-, off-hook and on-hook are disabled.
- the terminal is now considered busy (incoming calls entrants are camped on); with PIMphony, calls can still be taken.

4.4.3.1.2 Quitting VMB mode

The terminal quits this mode after:

- going on-hook or pressing END
- closing the VMB window
- after an inactivity timeout of 2 min 30 sec.

4.5 External Voice Mail Unit

4.5.1 Overview

From version R1.1 onwards, an External Voice Mail Unit ("external VMU"), using the VPS protocol, can be used in place of the integrated voice server.

The external VMU is connected to the Alcatel-Lucent OmniPCX Office Communication Server system by analog links (SLI boards).

The following integrated voice server features are no longer available when an external VMU is used:

- Personal Assistant
- conversation recording
- voice mail filtering
- Audiotex
- integrated Automated Attendant
- general mailbox

- visual mailbox (PIMphony)

4.5.1.1 ADDITIONAL INFORMATION

For systems operating with an external VMU, the following specifics need to be considered:

- Message notification: as with the integrated voice server, the presence of new messages is signalled by icon/LED or by voice prompt on going off-hook, depending on the type of terminal.
- Number of messages: with the external VMU, users are not shown the number of messages:
  - sets with displays: the sign "+1" means at least one message is available;
  - sets without displays: on picking up the handset, the user hears a specific tone signalling the presence of new messages.
- Consulting the mailbox: mailbox consultation is still accessed by pressing the Mail key or by dialling the Mail function code; on connection to the external Voice Mail Unit, the user is guided by the voice prompts (soft key navigation is no longer available).
- Customization: all the voice server options contained in the customization tree structure are disabled.
- General Mailbox soft key: the display on terminals in the Attendant group no longer offers a soft key for calling the general mailbox.

4.5.2 Operation

4.5.2.1 ACTIVATION/DEACTIVATION

4.5.2.1.1 Activating the external Voice Mail Unit

Activating the external VMU has the following effects:

- The keys and other data defined for the integrated voice server are not used by the external VMU;
- on each terminal, the number of messages received is set at 0 and the Message LED is off.

4.5.2.1.2 Reactivating the integrated voice server

When reactivated using OMC, and provided the settings are coherent, the voice server takes up from where it left off (with all statuses and voice mail recorded) before the switch to the external VMU.

4.5.3 Configuration procedure

The integrated voice server is used by default.

With OMC (but not with MMC-station), the integrated voice server can be deactivated in order to operate with the external VMU. This deactivation has to be confirmed; using the external VMU calls for the following additional adjustments:

- defining the links between the external VMU and the SLI equipment
- allocating the external VMU ports to the OS group and VMU group

- checking that the VPS codes are compatible with the numbering plan
- reprogramming the VMU access keys
- adapting the dynamic routing settings to the VMU for each user with a mailbox.
- To deactivate the integrated voice server:

By MMC-OMC (Expert View): **Voice Processing -> Activate Voice Processing -> ? Deactivate Voice Processing ->** click **Yes** to confirm

- To specify the SLI equipment for connection to the external VMU:

By MMC-OMC (Expert View): **Users/Base stations List -> Users/Base stations List -> Details -> Misc -> Special function = Voice Mail Unit**

- To check, for each SLI device, that camp-on on busy is authorised and that it has barge-in and warn tone protection:

By MMC-OMC (Expert View): **Subscribers/Base stations List -> Subscribers/Base stations List -> Details - > Features -> check ? Camp-On Allowed, ? Intrusion Protection ? Warntone Protection**

- To add the directory numbers of the Voice mail equipment to the Attendant group in order to run the Automated Attendant feature with the external VMU:

By MMC-OMC (Expert View): **Attendant Group List -> Details -> Modify -> Add**

- To create a VMU group:

By MMC-OMC (Expert View): **List groups -> Details -> Modify -> Add**

- For Reflexes terminals and analogue sets with a Message LED: to create a "Voice Mail" key (virtual in the case of analogue terminals) assigned with the VMU group number:

By MMC-OMC (Expert View): **Subscribers/Base stations List -> Subscribers/Base stations List -> Details -> Keys -> Function Keys = Voice Mail Unit (or Vir. keys -> check ? Voice Mail Unit and enter the VMU group number)**

- To adapt dynamic routing of level 1 and/or 2 (forwarding to general level): if the box is checked, the call is forwarded to the Automated Attendant on the external VMU; otherwise it goes through to the user's mailbox.

By MMC-OMC (Expert View): **Subscribers/Base stations List -> Subscribers/Base stations List -> Details -> Dyn. Rout. -> check or uncheck ? VMU as Auto. Attendant (lev 1) and/or ? VMU as Auto. Attendant (lev. 2)**

- To check the coherence of the internal numbering plan for the "Mail Booking" and "Cancel Mail Booking" functions (used by the VPS protocol):

By MMC-OMC (Expert View): **Numbering -> Numbering Plans -> Internal Numbering Plan**

- To check the values of the other VPS codes defined by labelled addresses relative to the numbering plan:

By MMC-OMC (Expert View): **System Miscellaneous -> Memory Read/Write -> Other labels -> VMCodBsyTo, VMCodCall, VMCodCnsTo, VMCodDiaTo, VMCodDirCl, VMCodFwdCl, VMCodOosTo, VMCodRecCl, VMCodRecal, VMCodRelea, VMCodRgToE, VMCodRngTo**

- To return to integrated voice server mode (check that the settings are coherent!):

By MMC-OMC (Expert View): **Voice Processing -> Activate Voice Processing -> ? Activate Voice Processing**

Chapter 4 *Voice Mail*

Chapter 5

OmniMobility

5.1 DECT

5.1.1 DECT Overview

5.1.1.1 Presentation

5.1.1.1.1 Overview

ETSI STANDARD

The DECT protocol is based on pico-cellular technology (cells of 30 to 150 m depending on the environment) allowing high traffic throughput: up to 10000 E/km2.

The frequency band used is between 1,880 MHz and 1,900 MHz (UHF) i.e. a passband of 20 MHz. These 20 MHz are split into 10 radio channels.

The passband of a radio channel is 1,728 MHz and radio channels are spaced 2 MHz apart to avoid interference between adjacent channels.

The DECT system is based on the use of FDMA (frequency multiplexing) and TDMA (time multiplexing) techniques. It thus has a maximum capacity of 120 simultaneous communication channels (10 radio frequencies x 12 time slots).

GAP (Generic Access Profile): part of the DECT protocol required for interworking by wireless handsets from different manufacturers.

PRINCIPLES

The DECT features integrated into the Alcatel-Lucent OmniPCX Office Communication Server system allow for the creation of a wireless PCX.

The DECT features are offered by 4070 IO/EO base stations connected to digital interfaces (UAI boards).

A radio base station can support up to 6 communication channels simultaneously, on 2 UA links.

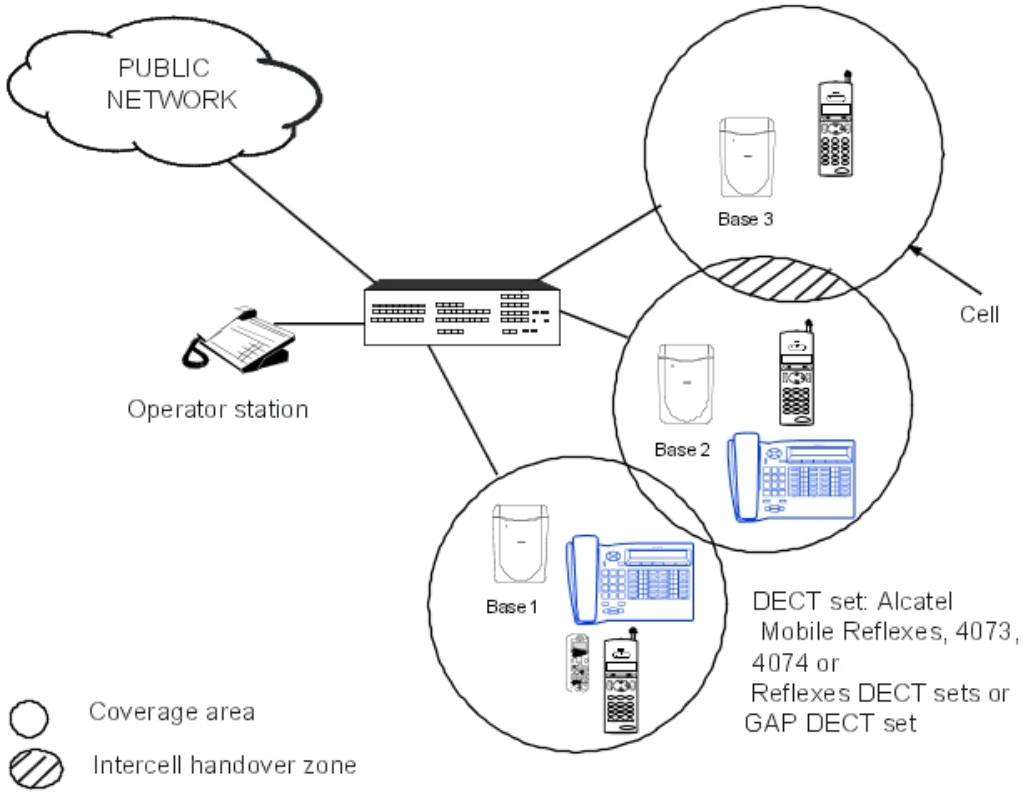
The base stations have a range of:

- 150 meters over open ground
- 30 to 50 meters horizontally and 7.5 meters vertically in an enclosed space

DECT UA/GAP SYSTEM

A DECT system managing the UA/GAP (Generic Access Profile) protocols allows simultaneous use of the following wireless handsets:

- DECT + GAP cordless handsets
- third party DECT GAP wireless handsets (the available features may differ).



AVAILABLE FEATURES

Mobility management

- roaming
- intracell handoff (on the same base station)
- intercell handoff (between base stations).

System access and dynamic channel selection

Before making or receiving calls, the handset must obtain information about the environment in which it is being used to ensure that it does in fact have access to the system.

To enable the handset to synchronise itself with the system, each base station is always active on at least one radio channel (the dummy bearer), broadcasting information concerning the system and its identity.

Any handset will thus be able to recognise the system coverage area in which it is working. When on standby, each handset is tuned to the nearest base station, receptive to search messages indicating an incoming call.

Channels are assigned dynamically when requested by the handset. Once synchronised with the system, the handset decides on the most appropriate channel for a call. It chooses the least disrupted of the free channels.

Inter- and intra-cell handoff procedures

The coverage radius of a DECT radio base station forms a "cell".

Intercell handoffs to another cell are commanded by the handset when the signal from the active base is weak and there is a stronger base in the vicinity. During the call, the mobile requests an appropriate available channel from the second base. Once the second link has been established, it releases the first one, maintaining the call on the second base.

If transmission errors arise, an intracell handoff is performed on the same base station towards a higher quality channel.

GAP MODE: GENERAL

By default, Alcatel-Lucent Enterprise DECT GAP handsets operate in proprietary mode (i.e. like Reflexes sets); third party DECT GAP handsets usually operate in basic mode (though some may operate in advanced mode):

- Basic mode: This mode offers a reduced level of features (no consultation call, no call waiting, no display management, etc.)
- Advanced mode: This mode offers access to a level of operation essentially equivalent to that of an analog Z terminal (all features defined by feature access codes).

With OMC, the mode of each set can be modified individually at the registration stage.

5.1.1.1.2 List of countries by region for DECT

For the DECT frequencies range to be well covered, and the handset to function correctly, use the World Wide feature to register a DECT handset. You need to select the right region or zone for a country of registration.

Alcatel-Lucent strongly recommends that you follow the regulations which exist for inclusion of specific countries in a region.

Consult the table below, which gives the region denomination (1- 4). Alcatel-Lucent DECT handset availability is also shown, by inclusion in its catalogue and approval zone.

table 5.1 : DECT list of countries and regions

Country or zone of registration	**Corresponding region denomination**	**Alcatel-Lucent DECT availability**	
		Approval	**Catalogue**
All EC countries	1	Eur	Eur
US+Canada	2	US	US
APAC/ ASIA			
Australia	1	Eur	Eur
Bangladesh (2T)	1	Eur	Eur
Bangladesh (2T)			
Cambodia	1	Eur	Closed
China	4	Asia	Asia
Hong Kong	1	Eur	Eur
India	1	Eur	Eur

Country or zone of registration	Corresponding region denomination	Alcatel-Lucent DECT availability	
		Approval	Catalogue
Indonesia	1	Eur	Eur
Japan	Forbidden		
Korea	Forbidden		
Laos	1	Eur	Closed
Malaysia	1	Eur	Eur
Maldives (2T)	1	Eur	Eur
Mongolia			Closed
Myanmar (2T)	1	Eur	Eur
Nepal (2T)			Closed
New Zealand	1	Eur	Eur
Philippines	1	Eur	Eur
Singapore	1	Eur	Eur
Sri Lanka (2T)	Forbidden		Closed
Taiwan	1	Eur	Eur
Thailand	4	Asia	Asia
Vietnam	1	Eur	Eur
LATAM Latin/ South America			
Argentina	3	Latam	Latam
Bolivia	3	Latam	Latam
Brazil	3	Latam	Latam
Chile	3	Latam	Latam
Colombia	3	Latam	Latam
Costa Rica	1 + 3	Eur+Latam	Eur+Latam
Cuba	3	Latam	Latam
Dominican Republic (2T)			Closed
Ecuador	1 + 3	Eur+Latam	Eur+Latam
El Salvador	3	Latam	Latam
Guatemala	1 + 3	Eur+Latam	Eur+Latam
Haiti			Closed
Honduras	1 + 3	Eur+Latam	Eur+Latam
Jamaica (2T)			Closed
Mexico	3	Latam	Latam
Nicaragua			Closed
Panama	1 + 3	Eur+Latam	Eur+Latam
Paraguay			Closed

Country or zone of registration	Corresponding region denomination	Alcatel-Lucent DECT availability	
		Approval	**Catalogue**
Peru	3	Latam	Closed
Uruguay	3	Latam	Latam
Venezuela	1	Eur	Eur
Africa/ Middle East			
Algeria	1	Eur	Eur
Angola (2T)			Closed
Bahrain	1	Eur	Eur
Benin			Closed
Burkina Faso			Closed
Burundi			Closed
Cameroon	1	Eur	Eur
Chad (2T)			Closed
Central Afr. Rep.			Closed
Comores (Rep Dem)			Closed
Comores (Rep Isl)			Closed
Congo			Closed
Djibouti			Closed
Egypt	1	Eur	Eur
Erythrea			Closed
Ethiopia			Closed
Gabon	1	Eur	Eur
Gambia			Closed
Ghana	1	Eur	Eur
Guinea			Closed
Iran	1	Eur	Eur
Israel			Closed
Ivory coast	1	Eur	Eur
Jordan	1	Eur	Eur
Kenya	1	Eur	Eur
Kuwait			Closed
Lebanon	1	Eur	Eur
Libya			Closed
Madagascar			Closed
Malawi			Closed
Mali			Closed
Mauritania			Closed

Country or zone of registration	Corresponding region denomination	Alcatel-Lucent DECT availability	
		Approval	**Catalogue**
Mauritius	1	Eur	Eur
Morocco	1	Eur	Eur
Mozambique (2T)			Closed
Niger			Closed
Nigeria	1	Eur	Eur
Oman			Closed
Pakistan			Closed
Qatar (2T)		?	?
Rwanda			Closed
Saudi Arabia	1	Eur	Eur
Senegal	1	Eur	Eur
Seychelles			Closed
South Africa	1	Eur	Eur
Sudan			Closed
Syria			Closed
Tanzania			Closed
Togo			Closed
Tunisia	1	Eur	Eur
UAE			Closed
Uganda (2T)			Closed
Yemen			Closed
Zambia			Closed
Zimbabwe			Closed
East/South Europe			
Albania	1	Eur	Eur
Armenia	1	Eur	Eur
Azerbaijan (2T)	1	Eur	Eur
Bielorussia (2T)	1	Eur	Eur
Bosnia Herzegovina (2T)	1	Eur	Eur
Bulgaria	1	Eur	Eur
Croatia	1	Eur	Eur
Cyprus	1	Eur	Eur
Czech Rep	1	Eur	Eur
Estonia (2T)	1	Eur	Eur
Georgia (2T)	1	Eur	Eur

Country or zone of registration	Corresponding region denomination	Alcatel-Lucent DECT availability	
		Approval	Catalogue
Hungary	1	Eur	Eur
Kazakhstan	1	Eur	Eur
Kyrgyzstan (2T)	1	Eur	Eur
Latvia	1	Eur	Eur
Lithuania (2T)	1	Eur	Eur
Macedonia (2T)	1	Eur	Eur
Malta	1	Eur	Eur
Moldavia (2T)	1	Eur	Eur
Poland	1	Eur	Eur
Romania	1	Eur	Eur
Russia	1	Eur	Eur
Slovakia	1	Eur	Eur
Slovenia	1	Eur	Eur
Tajikistan (2T)	1	Eur	Eur
Turkey	1	Eur	Eur
Turkmenistan	1	Eur	Eur
Ukraine (2T)	1	Eur	Eur
Uzbekistan (2T)	1	Eur	Eur
(Yugoslavia Rep Fed.) Serbia and Montenegro	1	Eur	Eur

5.1.1.2 Engineering Rules

5.1.1.2.1 Engineering rules

Purpose of this Document

The purpose of this document is to define the engineering rules relative to the DECT technology.

These recommendations cover the technical and methodology aspects from the offer to the maintenance on DECT projects.

The introduction of new products, as well as the complex product developments, means these rules will evolve and this will result in our recommendations being changed accordingly.

The aim is to optimize our offer by reducing the risks for Alcatel-Lucent Enterprise while meeting more precisely the expectations of our customers.

Radio Systems Overview

Introduction

Radio transmission is evolving and subject to numerous parameters, making it a medium that is not easy to control. Radio waves propagate differently according to the materials they have to traverse and on which they will reflect.

The behaviour is similar to that of light. There will be:

- **Diffraction** and **attenuation** according to the materials to pass through. If there are no windows or glass areas, there may be shadow areas
- **Reflections** as on mirrors (large metallic surfaces) which will entail standing wave effects resulting in amplitude differences in the RF field

All these phenomena will restrict the radio coverage from the base stations and the quality level of the wave received at one point. In DECT technology, the mobile phone plays a major role since cell changes are based on algorithms that are specific to the station (field level, quality criterion) which means that it determines the end quality seen by the subscriber.

Three important elements must be processed either sequentially or simultaneously:

- Covering the area where the service is to be provided
  Coverage=Accessibility
- Ensuring the establishment of communications to stations in a zone with heavy communication users
  Capacity=Availability
- Ensuring user satisfaction
  Audio Quality=Comfort

Quality for radio systems is a term that can include all of these topics. It is referred to as **Quality of Service (QoS)**.

The base station technology also impacts on this quality.

For these three elements, the stations have a crucial role because:

- Their sensitivity will intervene to determine the coverage and capacity.
- Their algorithms and Handover thresholds will impact on the capacity and quality.
  The Handover function is essential for mobile phones but also for cordless fixed office sets. It enables the set to switch to another base station, should the first one be saturated

The actions to carry out to ensure QoS are:

1. Determine the aims and needs of the customer
2. Select the best position for the terminals and the type of antenna to be used
3. Check the resulting traffic capacity
4. Identify whether the previous results need to be adapted according to the sets used and the quality of service expected by the customer

Coverage

This initial function is fundamental for radio systems.

The choice of base station positions is crucial for correct coverage.

Identifying the materials present on the site, zone or in the building is essential.

The presence of metal surfaces and dense structures can result, on the one hand, in partial or total screening (partitions, pipes, machines, etc.) but can also become a good wave guide. Therefore, it is essential to visit the site when this is possible or to undertake in-depth drawing

analysis with the architect taking into account the materials used.

Important:

The rules for calculating the number of base stations based on a number of bases per square metre can only be used if this visit has qualified the site as being exempt of coverage difficulties.

Traffic

The notion of traffic is often raised following the initial coverage study.

The capacity calculations can lead to a significant increase in the number of bases to be installed and a reappraisal of base station distribution.

Important:

Non homogenous distribution of the traffic may entail dividing the site up into several zones.

Audio Quality

The quality of a system is the quality as seen by subscribers and, ultimately, it is the end appreciation that will make the DECT system a success or a solution that is not totally satisfactory.

This is obviously linked to the first two functions because a subscriber who is not covered or has no channels available will not be satisfied. It is also associated closely with the performance of the products.

Important:

The quality level also depends on the service expected by customers; for example, a company that wants to be able to reach a small number of its employees on the move will put up with a few imperfections whereas in the case of Full DECT a quality equivalent to fixed wired sets will be demanded on the office sets.

DECT Offer Process

The entire offer process must be founded on a formal QoS commitment.

Project Classification

The aim of this classification is to assist sales and pre-sales technical support managers in asking themselves a series of questions regarding offer optimization and the identification of technical and sales risks.

The radio measurement services on site are the only means of securing the offer. Recommendations regarding sizing and methods are detailed in § General Rules .

Classification of Customer Objectives

The customer's objectives in terms of mobility and business approach may be as follows:

- **Mobility "DECT"**
  Part of the company is mobile. The aim is for these mobile phones to be accessible at all times.
- **Installation of a "Full DECT" completely wireless PBX**
  The interest lies in doing away with the wiring and in the High-Tech aspect afforded to the company. We talk of Full DECT or Full Wireless when more than 80% of users are in DECT cordless. In this type of installation, two types of implementation are possible:
  - With **operating/running costs optimization** by doing away with office moving costs

- With **investment costs optimization**
  The customer's requirement may be a Full DECT system:
  - Without a 100% coverage obligation
  - without the obligation to do away with office moving costs totally

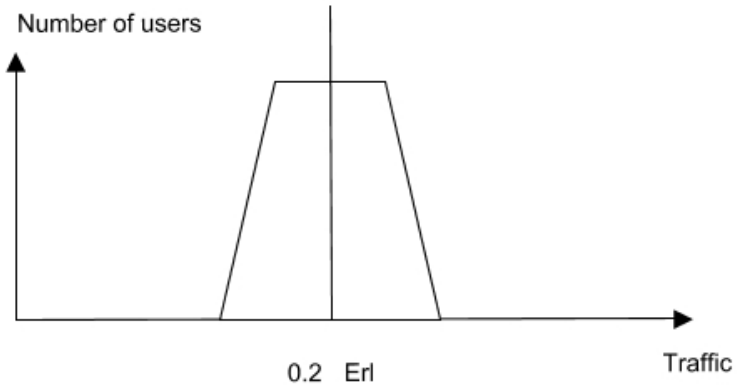
The use of this mobility may be just as important in the QoS choices. Therefore, you must specify the type of users (discussions, basement or roof maintenance, etc. sales agents, hot line, etc.)

Classification of User Distribution

The different business activities in some companies may result in classifying a site by geographic zones according to user homogeneity criteria.

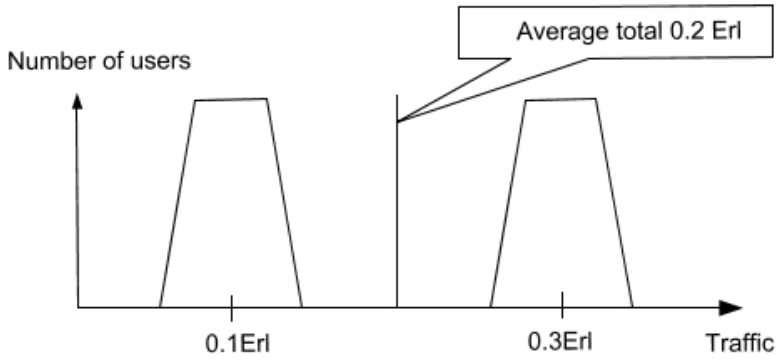
A very different example of distribution is shown in the 2 diagrams below even though the average traffic is the same. The calculations according to average traffic must not be done without prior analysis regarding homogeneity.

- **Homogenous distribution:**
  Well-distributed user population with a majority centred on the average.



- **Non-homogenous distribution:**
  Company made up of several professions with extremely different traffic needs.
  There are two possible cases:
  - The geographic distribution is common
  - The geographic distribution is separate

  Depending on the case, this results in very variable capacity in traffic density, in turn resulting in a different base station density.



Technical Classification of the Site

This classification is used to determine the QoS expected by the customer at a given point. It is based on two parameters: capacity and coverage.

Capacity Objectives

The traffic capacity notion is an important aspect that must be integrated in this classification approach.

table 5.2 : Capacity according to Activities

Very high traffic	Telemarketing, Hot Line, market rooms, etc.	(>0.3Erl)
High traffic	Sales, buyers, etc.	(0.3E> >0.2E)
Average traffic	Technique, project, administration, etc.	(0.2E> >0.11E)
Low traffic	Store, lab, storage, etc.	(<0.1 Erl)

These figures can be used for sizing if the customer has no accurate idea of the actual traffic.

Radio Coverage Classification of the Site

The site can be classified in two coverage categories:

- Site with no coverage problem(s) (= Easy)
  Offices, service sector, store rooms (no obstacles and metallic partitions), etc.
  Watch out for ordinary office metal doors which can change the complexity of the site by producing field variations
- Site with difficult coverage (Metallic environment) (= Tricky)
  Production plant, certain buildings using metallic partitions, clean rooms, etc.

A real life fading measurement (door openings, usual circulation, etc.) is essential to classify the site as easy (fading <20dB) or tricky (fading >20dB).

However, the delay spread parameter, resulting from multiple reflections in the case of large metallic buildings (>30m x 30m), may be critical.

This risk is detected by associating a poor quality level (< 8) and a good radio field level.

Classification as Zone

A **zone** is a space where the characteristics in terms of customer objectives, traffic distribution

and coverage difficulties are homogenous.

Eliminating disparities in a zone is used to obtain a result that is optimized as regards the service expected by the customer. A site can include several zones.

This classification also allows the customer's QoS objectives to be specified better and to limit our commitment to the real requirement zone by zone.

Classification Summary Tables

The tables below are intended to assist offer managers and measurement managers in their approach. The first column shows the customer's objective and the other columns the classifications in profiles, traffic and coverage, finishing with the recommendation in terms of principles

DECT case	User profiles	Traffic	Coverage	Principle
Ordinary mobility	Homogenous over the entire site	Low risk, users are mobile A final calculation indicating the capacity per m² must be handed over to the customer	Easy: Calculate the number of base stations required to cover the site with a ceiling of -70 dBm (*)	**Terminals per m²** See coverage in § Coverage Performance Principles .
			Tricky: Preliminary coverage study with measurements and ceiling of -60 dBm and quality level of >=12	**Preliminary coverage study**
			Several zones with different difficulties	Apply the previous 2 principles to each zone

(*): The ceiling recommended for coverage calculation, while maintaining a quality level of >-12 for a DECT network and depending on the type of mobile handset is:

Type of station	4074	4036	DECT Reflexes
Ceiling for easy coverage (fading < 20 dB)	- 70 dBm	- 70 dBm	- 70 dBm
Ceiling for tricky coverage (fading < 20 dB)	- 60 dBm	- 60 dBm	- 60 dBm

An additional margin of 10 dB should be taken into account (- 60 dBm and - 50 dBm) in the case of a request for a Full DECT QoS level close to fixed (wired) line quality.

In addition, be careful and do not apply this rule on specific sites producing cavity type effects where the resonance effects may corrupt this measurement. In this case, do a specific study.

Case of a Full DECT optimization of running costs	User profiles	Traffic	Coverage	Principle
No cost office moving	Homogenous over the entire site.	Calculate the number of base stations required to handle the site traffic with a margin. Indicate the hypotheses.	Easy: Calculate the number of base stations required to cover the site with a ceiling depending on the mobile sets used (use the least good sets).	Take the highest number of base stations from the 2 calculations and **distribute** them as equally as possible on the site. Take a 5% base stations margin to add to cover one-off traffic situations
			Tricky: Preliminary coverage study with radio measurements to determine the number of base stations. The ceiling is dependent on the mobile sets used (use the least good sets). And also take a quality level of >=12	Take the highest number of base stations from the 2 calculations and **adapt the coverage study result** if necessary. A check on the capacity must be carried out.
			Several zones with different difficulties	Apply the previous 2 principles to each zone
	Not Homogenous There are zones with very different traffic values	Calculate the number of base stations required to handle the traffic starting with the highest traffic density and applying it to the entire site. Indicate the hypotheses. Specify assumptions. **(Traffic density uniformization**)	Easy: Calculate the number of base stations required to cover the site with a ceiling depending on the mobile sets used (use the least good sets).	Take the highest number of base stations from the 2 calculations and **distribute** them as equally as possible on the site. Take a 5% base stations margin to add for one-off traffic situations

Case of a Full DECT optimization of running costs	User profiles	Traffic	Coverage	Principle
			Tricky: Preliminary coverage study to determine the number of base stations. The ceiling is dependent on the mobile sets used (take the least good sets) and also take a quality level of >=12	Take the highest number of base stations from the 2 calculations and **adapt the coverage study result** if necessary. A check on the capacity must be carried out.
			Several zones with different difficulties	Apply the previous two principles on the different zones

Case of a Full DECT **Optimization of investment costs**	User profiles	Traffic	Coverage	Principle
	Homogenous over the entire site	Same as the previous case except for the fact that the **traffic value used as hypothesis must not be increased**.		
	Not Homogenous There are zones with very different traffic values	**Divide into zones and treat each zone as the case of a Full DECT site with running costs optimization**		

Offer Completion Methodology

The completion of a Radio offer must follow the following stages:

Stage 1: Collection of Customer Requirements

1. **Phase 1:** Determine the customer's objectives
   This initial phase is usually conducted by the commercial manager.
   - Objectives:
     - Determine the customer's requirements per zone
     - Determine the site complexity
     - Retrieve the plans/drawings
     - Retrieve the information relative to the traffic and user distribution
   - Results:
     - Classification of the project and associated risks
     - Completion of the costs hypotheses dossier
2. **Phase 2:** Analysis of the site
   This second phase can be completed by the commercial manager, offer technical support or radio measurements manager, preferably on site.

- Objectives:
  - Confirm the project complexity
  - Complete the information retrieved in phase 1 (plans/drawings, traffic, distribution)
  - Retrieve information relative to the site
- Results:
  - Confirm classification of the project and associated risks
  - Quantify the measurements services to be carried out
  - Propose an initial approach for base station numbers by integrating the traffic and coverage data and their positions

This phase is preferable to activate phase 3 in good conditions for the sizing of the resources needed by the service and to provide an initial strategy recommendation to follow as regards the measurements to be carried out.

3. **Phase 3:** Radio coverage study
   In all cases, **real life** radio measurements are recommended to confirm the positioning and quantity of the base stations (field, fading level and quality level measurements using a portable tester equipped with 4074 and Reflexes 200 mobile testers).
   They are **essential in the zones classified as tricky coverage**.
   - Objectives:
     - Confirm the number of zones
     - Determine the characteristics of the building, partitions and environment
     - Determine the field and Audio Quality levels Audio (measurement of the Q quality factor) at the strategic points on the site
   - Results:
     - Identify the different zones and give the following results per zone
     - Measurement dossier confirming the real coverage and associated audio quality level
     - Confirm the quantity and positioning of the base stations
     - Identify the residual risks
     - Propose QoS levels per zone on which Alcatel-Lucent Enterprise could give a commitment

   If this measurement reveals that the environment is disruptive, the network will be declared as tricky Radio Coverage and its classification may be changed.
   If the site does not exist when the offer is made, this first stage will be replaced by the drafting of more advanced hypotheses.

Stage 2: Drafting of the Offer

The offer will be drafted in the light of the coverage study and the hypotheses retained. Different zones are displayed according to the QoS.

Stage 3: Drafting of the Commitment Limits

The commitment level per zone, the average of all the sets in this zone, must be specified by a QoS level. It will be based on a DECT mobile set in static position, with the following two notions:

- **Call establishment success rate** = Accessibility, availability
- **Audio quality rate** = Quality, comfort
  corresponding to the absence of cut-offs and interference on an established communication

Four levels are recommended:

1. **Level 1**
   The coverage is perfect on this zone, i.e. no cut-offs, no interference and no failure in call establishment.
   Seen by the user as almost the same as a wired set, this corresponds to the Full DECT request.
   A commitment of this type is always with a limit of less than 100%. The recommended values are:
   - Call establishment success rate >99.5%
   - Audio quality rate >98%

   Precautions:
   Clearly specify the zones of this type, avoid the common parts, rest rooms, stairs, elevators and room angles/extremities. (Take into account the field level recommendations relative to Full DECT).
2. **Level 2**
   The coverage allows for good quality communications with the possibility of saturation during a particular peak period.
   The recommended commitment values for this level are:
   - Call establishment success rate >95%
   - Audio quality rate >95%

   Precautions:
   Clearly specify the zones of this type, avoid the common parts, rest rooms, stairs, elevators and room angles/extremities. (Take into account the field level recommendations relative to Full DECT).
3. **Level 3**
   The coverage is good but some areas are probably in a shadow zone. Therefore cut-offs and interference are to be expected.
   The recommended commitment values for this level are:
   - Call establishment success rate >90%
   - Audio quality rate >85%

   Precautions:
   Clearly specify the zones of this type, taking into account the recommendations for field level relative to DECT.
4. **Level 4**
   The coverage is not guaranteed.
   Work-around solutions are offered according to the customer's needs (case of rarely frequented zones where the accessibility can be obtained by installing one-off solutions).
   In the case where the customer has demands that exceed our own assessment, then depending on the commercial context, we must:
   - Either **sell a pre-study** that is more comprehensive, to specify the Alcatel-Lucent Enterprise level of commitment better
   - Or **present two offers** specifying the hypotheses version:
     i. What Alcatel-Lucent Enterprise feels sufficient
     ii. What would be required to meet the customer's demands

     When a results commitment is requested, we must:
     - Avoid fixing the resources (number of base stations, etc.) as a more in-depth study may enable us to reduce the number of base stations and, as a result, increase our global margin

- Increase the assessment to cover the risk relative to the number of base stations (5% if the requirements expression data are accurate and more in the case of uncertainties)

Caution:

In all cases, do not make a results commitment for a site that has not been visited.

General Rules

Traffic Calculation Rules

Even though, in most cases today, the number of base stations is linked more to coverage rather than traffic objectives, it is a good idea to make sure of the suitability of the customer's capacity, in particular in the Full DECT case.

The calculations must be carried out zone by zone.

Reminder:

A zone is a space that is homogenous regarding difficulty of coverage, traffic and the required quality level

To calculate the number of possible close base stations (or terminals) as well as the traffic when there is a reduction in the number of frequencies, refer to the document *IBS NG : Rules of installation for China and South America base stations 3AK 29000 1555 UUZZA*.

With **5 US frequencies**, the maximum number of close IBS NG **US** base stations is between 3 and 5 which limits simultaneous communications to a number between 10 and 20, while with 10 frequencies, the maximum number of close IBS NG EU base stations is between 6 and 9 which limits the simultaneous communications to a number between 25 and 40

With 5 frequencies rather than 10, the traffic reduction factor is in the order of 2.

User DECT Traffic

User traffic has two components `ti = tci + tsi`:

- The tci traffic due to the user's communications
- The tsi signalling traffic exchanged with the Alcatel-Lucent OmniPCX Office Communication Server for certain telephone features

Three cases can arise when **determining the tci traffic**:

- The customer indicates the DECT traffic of the different users - in this case, use these values.
- The customer indicates the telephone traffic of the different users without making any distinction between DECT and wired and often uses an average value: in this case take 100% for the users who just have DECT and only 50% for the others.
- The customer does not indicate any values - in this case, take 0.12 Erl for users just having DECT and only 0.06 Erl for the others who have, for example, a wired terminal.

Determining the tsi traffic

We recommend using:

- tsi=0.5 x tci for sets using the manager/secretary, supervisor, multi MCDU or multi-key MCDU functions and
- tsi=0 for the others

DECT Traffic of Users in a Zone

The calculation is done per user type (same traffic and same DECT terminal)

Tu =# **ni** x **ti**

ni is the number of users of the same type.

ti is the average traffic per user of this type expressed in Erlangs.

Traffic Capacity Calculation

The total load of the terminals is higher than the DECT traffic of the zone users. You must take into account the visitors' traffic and the load due to DECT mechanisms (Handover).

By default, and without more accurate information, visitors' traffic is estimated to be 10% of the DECT traffic of the sets in the zone. The load due to the DECT mechanisms is equal to 20% of the users' DECT traffic (those in the zone + visitors).

The total load for a zone is: T = Tu x 1.10 x 1.20

Number of Terminals

This is the number of terminals to be offered to the customer to meet their needs in terms of traffic. The calculation method is given for the IBS.

This calculated number can still be increased in the case of a Full DECT installation according to the customers' requirements.

The number of terminals finally determined for the traffic aspect must be compared with the number of terminals determined by the coverage requirements.

The higher number will be used for the proposal to the customer.

Calculation of the IBS Number

All the terminals see 6 channels.

The table below gives the admissible load per base station with a blockage rate of 1%:

This load is a function of the minimum number of base stations seen by a terminal at any place in the zone.

In rows: number of channels.

In columns: number of visible base stations.

	1	2	3	4
6 channels	**C** 6.1=1.9	**C** 6.2=2.8	**C** 6.3=3.3	**C** 6.4=3.7

The calculation of the number of base stations for the traffic requirement is then: **N** = **T** / **C** 6.b

“Full DECT” Installation

Full DECT installation with running cost optimization, the number of base stations proposed and costed must be equal to the number of base stations calculated, increased by 30%.

This is used to guarantee for the customer that, after commissioning or any subsequent office moving, there will be no more than 5% of the cells to restart.

Restarting a cell consists in passing it from 1 to 2 base stations because the station traffic serviced is higher than the average.

Conversely, if after moving, this is not the case, the zone must be brought back to 1 single base station.

In fact, in the case of a Full DECT installation, with running cost optimization, 95% of the base stations sold will be installed on commissioning and the remaining 5% will be used to handle the case of excess traffic cells.

Full DECT installation with investment cost optimization, the number of base stations proposed and costed must be equal to the number of base stations calculated.

Subsequently, the customer must adapt the coverage to the noted traffic disparities, which will be translated by moving or even adding base stations.

Coverage Performance Principles

Base Station Positioning Methods

Base Station Distribution

The **general rule is to distribute the base stations over the whole site or zone** to put the mobile handset in a context in which it will see several base stations in the different directions. This is used to guarantee the fact that it will see some base stations better than others.

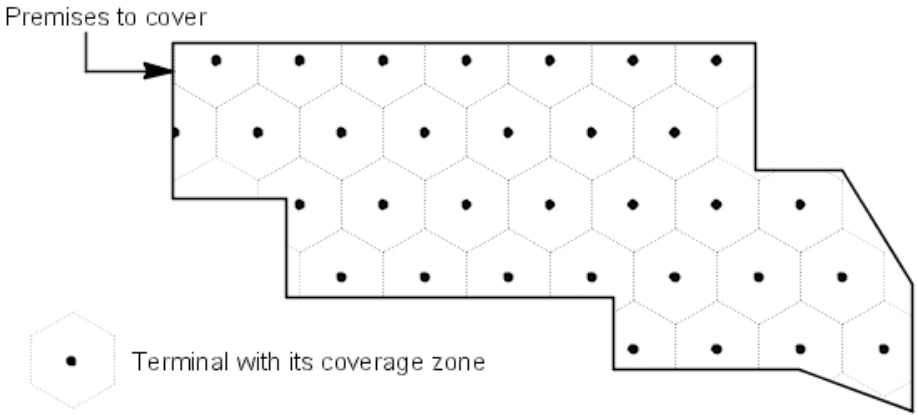
For some traffic extension or local traffic cases, one-off doubling of the base stations will be authorized by waiving this rule.

If the traffic is predominant as regards the coverage difficulty, base station meshing will be weaker, thereby allowing each mobile handset to see a maximum number of base stations within the predefined field level limits.

Measurement and Scheduling Principle

The first phase is carried out on a two dimensional horizontal surface; the aim is to obtain a radio level that is better than the coverage ceiling defined according to the type of set and the category of the coverage type. This level is used to retain a margin as regards the mobile handset sensitivity (-89 to-91 dBm) to have greater protection against fading effects (fluctuation in the order of 20 /30 dB). **The measurements obtained must be stable for a minimum of 5 seconds; if this stability cannot be obtained, the lowest level must be used as a basis.**

It can be assumed that base station distribution will be done as per a network of hexagonal cells as shown in the schematic below.



The above method assumes:

- that the antenna systems used initially are omni directional type. The use of specific antenna systems can be used in special cases that will be dealt with in the antennas chapter, either for quality reasons or to optimize the number of base stations.
- that the base stations on the adjacent floors have no influence.

Initially, when the traffic requirement is not high, the planning can be done without taking into account any inter-floor mutual assistance. Taking this into account can be done in the second phase, allowing optimization of the number of base stations for the coverage.

This optimization phase will comply with the following process:

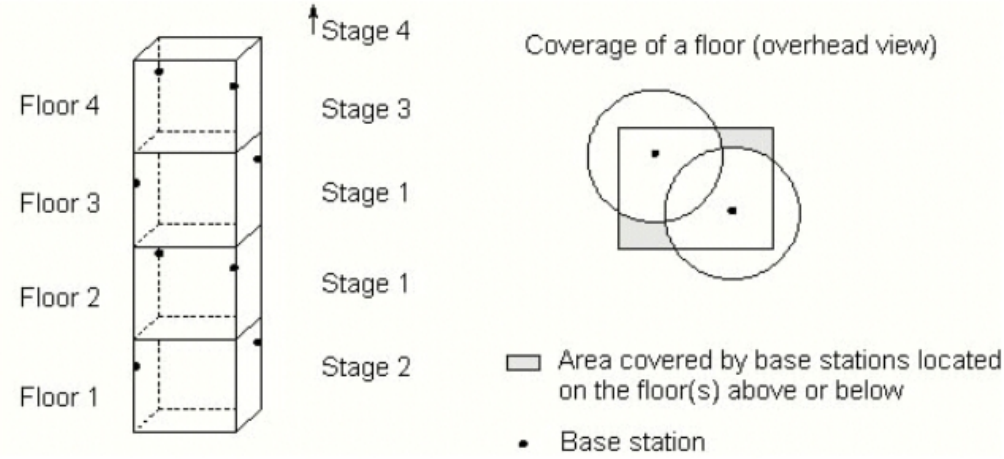
- Measurement of the level on the adjacent floors, bearing in mind that this is not always homogenous. (Use the least good cases for planning).
- Proceed with base station position interleaving between the floors if the level is sufficient to have mutual assistance (-60 to -70 dBm depending on the type of coverage retained)
- Check the efficiency of the mutual assistance between the floors.

  This position interleaving can be a rule to be applied generally.

  The best way to continue is to start the study with floor 2, position the radio base stations to obtain floor 2 coverage in line with the previous recommendations, repeat the operation on floor 1 and 3 off-setting the base stations, confirm the final coverage level obtained on floor 2 and then repeat the same base station positions on the even and odd numbered floors.

  If the upper floors do not have the same layout as floors 2 and 3, they must also be analyzed by repeating the different stages.

  The number of base stations on the first and last floors must be confirmed as they will not have the same mutual assistance capacity.



US Coverage

US IBS NG base stations work in odd mode (using odd timeslots) **or in even mode** (using even timeslots) **according to the RPN value** (Odd or even).

For regulations reasons (FCC Part 15 Subpart D Section 15.323 c5) **two US base stations**

at least (One working in **odd** mode and one working in **even** mode) **must be installed and operational for each US deployment**.

Remark:

It is recommended to alternate odd and even base stations in the hexagonal cells of the networks. Except for the US region, all other regions (EU, CH and SA) currently work with IBS NG base stations in odd mode.

RPN stands for Radio fixed Part Number.

Antennas

One of the parameters for optimal coverage of a specified zone is, apart from the position of the base station, the type of antenna emission.

Types of Antennas that can be Used

Two types of antenna can be used: Omni directional and directional.

Directive antennas can be used when:

- the complexity of the coverage forces us to use only a very small part of the theoretical zone obtained by omni directional antennas and, as a result, to multiply their number significantly.
- the zone to cover is very long as regards its width (tunnel, ship, long corridor, etc.)
- zone separation is necessary, for example: to limit the Campus effect risks

If a site has very high traffic with a requirement for high frequency re-use, spray type antenna systems must be used.

The table below details the main antennas used at present, selected as per the Alcatel-Lucent OmniPCX Office Communication Server operating manual.

Type	**Opening angles**	**Uses**	**Recommended positioning**
Omni 2 dBi 4151448	V=80° H=360°	Large hall(s) with little traffic, open space(s), ordinary offices	Clear space that is as visible as possible, away from obstacles (>3m), in the centre of the area to cover and 20 cm from the ceiling
Omni 7.5 dBi 3953630 MA43103	V=17° H=360°	Large outside area such as a car park, not recommended for indoor use.	Clear space, away from obstacles, not too high (<5m) because the vertical opening is limited.
Directional 8 dBi Suhner with left and right circular polarization 4149117 G / 4149070 D	V=70° H=70°	Indoors in rectangular corridor and metallic environments (such as a hangar).	In all types of space: Ceiling, wall, poles, etc. Can be tilted to direct the energy to the required area.

Note 1:

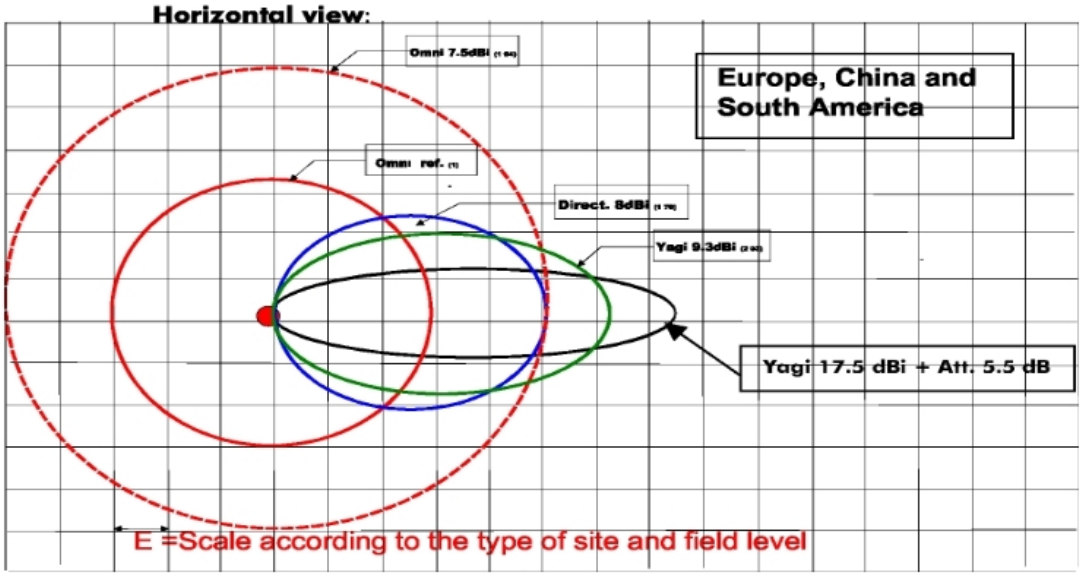
For Europe, China and South America zone, the antenna gain must be <= 12 dBi.

Note 2:
For the US zone, if the antenna gain exceeds 3 dBi by n dB, the peak emitted power must be reduced by the same number n dB.

E.g.: For an antenna gain of 8 dBi, the transmitted power must be reduced by at least 5 dB by adding a 5 dB attenuator in series with the antenna for example.

The difference in antenna coverage is shown in the schematics below:

Antenna coverage for EUROPE, CHINA and SOUTH AMERICA



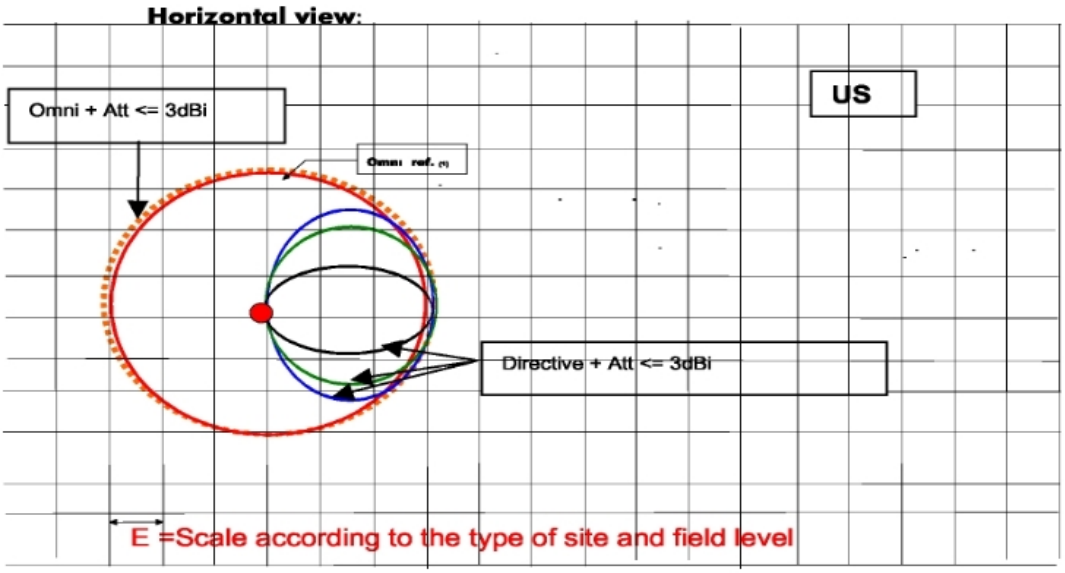
Europe, China and South America	For a field level -60 dBm	For a field level -70 dBm
Outdoors clear space	E =40m=> **r=120m**/standard ant.	E =130m =>**r=120m**/standard ant.
Indoors clear space	E =25m=> **r=75m**/standard ant.	E =70m=>**r=200m**/standard ant.
Indoors office space	E =16m=> **r=50m**/standard ant.	E =40m=>**r=125m**/standard ant.
Difficult site (Plant, etc.)	E =10m=> **r=30m**/standard ant.	E =70m=>**r=68m**/standard ant.

Note: tolerance is ~20%

Figure 5.6 : Horizontal view

These elements may be used to check the number of base stations obtained according to the measurements by providing an order of scale.

Antenna coverage for the US



Note 3:

Directive antennas for the US are not used to increase the range but to reduce the reception of reflected waves (multi-trajectory in difficult environments).

US	**For a field level of -60 dBm**	**For a field level of -70 dBm**
Outdoors clear space	E =27m => **r=85m**/standard ant.	E =90m => **r=275m**/standard ant.
Indoors clear space	E =17m => **r=50m**/standard ant.	E =48m => **r=140m**/standard ant.
Indoors office space	E =11m => **r=35m**/standard ant.	E =27m => **r=85m**/standard ant.
Difficult site (Plant, etc.)	E =7m => **r=20m**/standard ant.	E =16m => **r=47m**/standard ant.

Note 4:

Tolerance is -20%.

These elements may be used to check the number of base stations obtained according to the measurements by providing an order of scale.

Note 5:

For the US zone, $E_{\_US} = E_{\_EU}$ x 69% since $P_{\_us} = P_{\_EU}$ -4dB.

Given this reduction in power, **the number of base stations per m^2** , without considering the traffic (just considering the geographic coverage), **is, theoretically, to be multiplied by about 2** (or 2.0± 0.5) **for the US zone** as regards the number of base stations that would be obtained in the Europe, China and South America zones with the same audio quality.

- **With a reduction in the emitted power of 4 dB, the coverage is reduced by a factor of about 2** (or 2.0±0.5).

- **With 5 frequencies instead of 10, the traffic reduction factor is in the order of 2.**
- **A low traffic US coverage requires about twice (0.5 min.) more base stations than a low traffic Europe coverage.**
- **A high traffic US coverage required about 4 times (3 min.) as many base stations as a high traffic Europe coverage.**

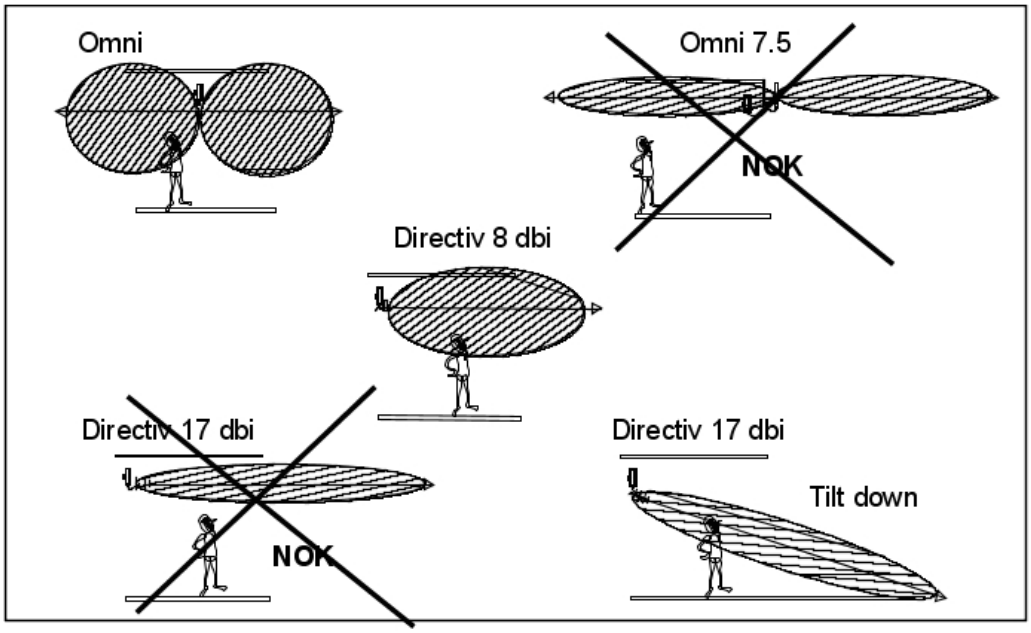


Figure 5.8 : Vertical view of the coverage zone of different antenna (See Tech Comm.: TC0213)

Case of Sites with Large Metallic Structures

In the case of industrial sites where reflection and multi-trajectory phenomena may cause much interference, it is recommended to use circular polarization antennas and to study more particularly the use of directive antennas.

DECT Rules as Regards a WLAN

The DECT network may be disrupted by a WLAN. This disruption will be a function of the WLAN emission level and the type of antenna used by the 2 networks (Omni directional or directional antennas).

To avoid interaction between networks, you must comply with the distances between the base station antennas.

For the WLANs, there are several levels of emitted power which, for the sake of simplicity, are divided into 2 sub-groups:

- NTP_WLAN network <=20 dBm and >10 dBm
- NTP WLAN network <=10 dBm

The minimum distances to be respected with the DECT bases with omni directional antennas having a gain of **2 dBi** are as follows:

NTP_WLAN network <=20 dBm and >10 dBm:	**Minimum distance = 2.5 metres**
NTP_WLAN network <=10 dBm:	**Minimum distance = 1 metre**

In the case of the terminals, the problems are the same.

For other antenna types, refer to the tables below:

table 5.11 : 10 dBm < NTP WLAN <= 20 dBm

	DECT Omni directional antenna G<=2 dBi	**DECT Directive antenna G=12 dBi**
WLAN Omni directional antenna G<=2 dBi	d>= 2.5 metres	d>= 7 metres
WLAN Omni directional antenna G<=6 dBi	d>=3.5 metres	d>= 11 metres
WLAN Directive antenna G<=12 dBi	d>= 7 metres	d>= 22 metres
WLAN Directive antenna G<=21 dBi	d>=20 metres	d>= 65 metres

table 5.12 : NTP WLAN <= 10 dBm

	DECT Omni directional antenna G<=2 dBi	**DECT Directive antenna G=12 dBi**
WLAN Omni directional antenna G<=2 dBi	d>=1 metre	d>= 2.5 metres
WLAN Omni directional antenna G<=6 dBi	d>=1.5 metres	d>= 3.5 metres
WLAN Directive antenna G<=12 dBi	d>=2.5 metres	d>= 7 metres
WLAN Directive antenna G<=21 dBi	d>=6.5 metres	d>= 20 metres

Note:

Given its spectrum spread, the WLAN is not disrupted much by the DECT network.

Elements to Size

Elements to be dimensioned	Rules
Total number of sets	The total number of sets is made up of resident sets and visitor sets from other customer nodes (calculation of the shells for incoming roaming and calculation of total traffic on the node).
Location zone	The location zone is used to situate the position of a set. This favours set paging. In the case of a company with high internal and external incoming call traffic (>1000 calls per hour, example Call Centre) thus generating high demand for paging, it is recommended to divide the default zone defined by the system into several location zones (multi zones function). ***Caution:*** ***in a multi zone case, the set that is located at the edge of the zones will undertake successive locations. This means that the overlap limit area of the 2 zones must be selected so that it is an area with a low density of permanent users (e.g.: transit area, corridor, etc.).***
Adding DECT sets and bases	Be careful in the case of extensions: the sizing calculation must be done again in order to guarantee and maintain the initial quality.

Recommendations Relative to the Wiring

The characteristics of the cables and their references are detailed in the product operational guide. (Tech com: TC0128).

However, some important precautions need to be taken into account:

- When there is a risk regarding the coverage (partial preliminary coverage study measurements), we recommend leaving a margin of several metres in the cable lengths as this allows the position of the base stations to be changed slightly.
- When traffic distribution is not fully known or when the customer wants a Full DECT network, doubling the cables for each risk base station provides an added security.
- When customers want to use their own cables, you must qualify these cables by carrying out specific measurements at the extremities covering attenuation, crosstalk and propagation times; the measurement limits are detailed in the table below:

Characteristics: for an IBS connected on a UA coupler	**Values**	**Comments**
Impedance at 682 kHz	85 Ohm < < 135 Ohm	Impedance variation on the line < 15%

Characteristics: for an IBS connected on a UA coupler	Values	Comments
Crosstalk at 682 kHz	> 44 dB	
Attenuation at 682 kHz	< 25 dB	
Propagation time	< 7 µs	
DC loop resistance	< 155 Ohms	Limit relative to the line current. For example, for information: • in 0.4 mm about 500 m • in 0.5 mm about 800 m • in 0.6 mm about 1200 m These distances are dependent on the characteristics of the cables used.

Specific Rules for Difficult Sites

The purpose of this section is to propose a particular process for these sites.

Recommended Stages

In the case of industrial sites with large dense metallic structures or clean room type sites, a specific study must be carried out.

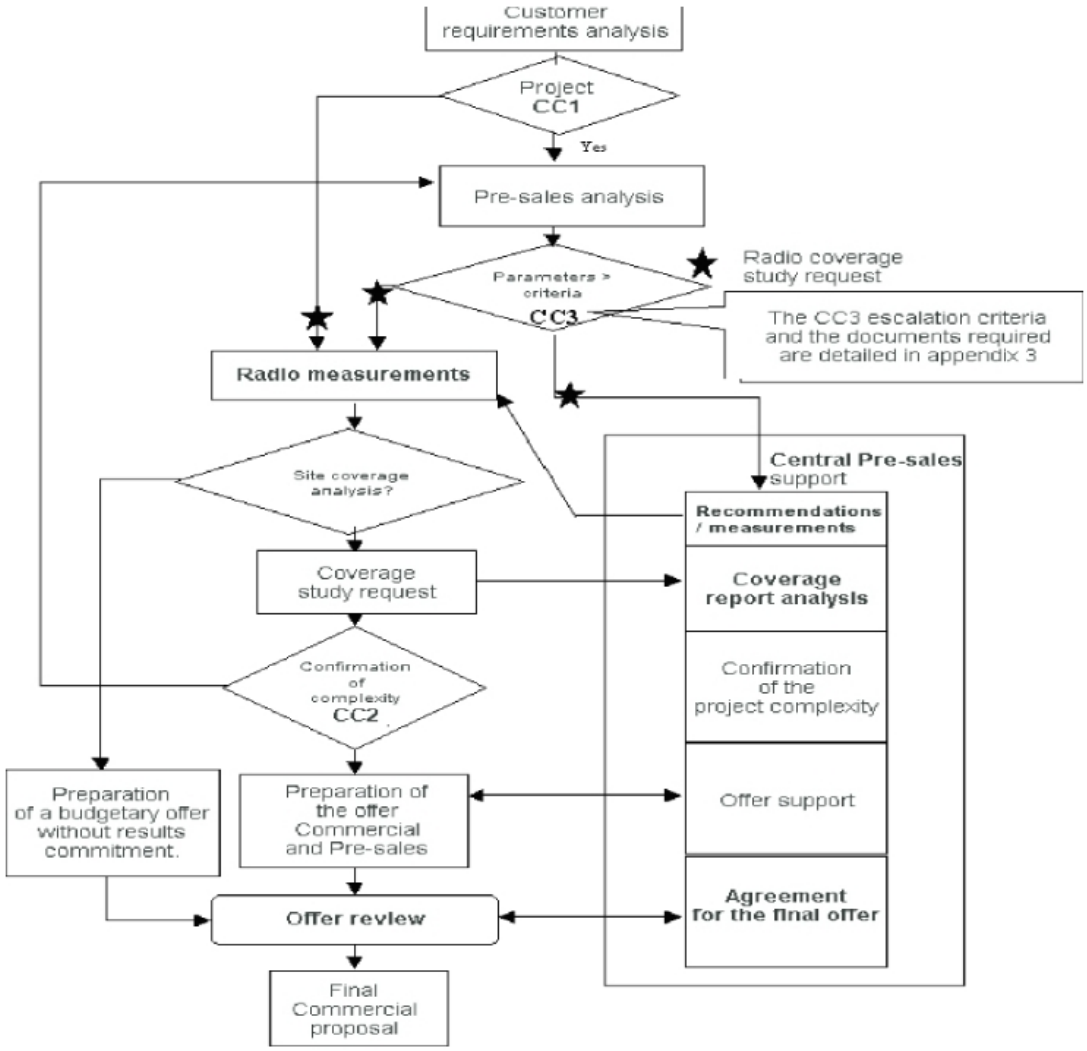
The procedure to follow is to propose a temporary installation followed by additional measurements and then an adjustment phase. This stage may result in us changing antenna type(s), modifying the positions of the base stations and, finally, adjusting the number of base stations.

Recommendations Concerning the Commitments

The commitment on this type of tricky project must be limited:

- Either to an offer with just a commitment on the means with no guarantee on the result(s) and providing customer support to improve the quality
- Or to making a quality level 3 offer with an additional services offer to evolve the quality subsequently.
- For sites with a zone presenting Clean Room type effects, there is no satisfactory solution at the DECT level.

APPENDIX 1: Generic Procedure for DECT offers



APPENDIX 2: DECT Radio Coverage Study Request

The following form is mandatory before the delivery of services and must be completed with the customer. The following form is mandatory before the implementation of the study and must be completed with the customer.

Data must be filled by the sales manager globally for the project (1).

ALCATEL: Sales manager/ Vendeur : Entity / Agence : Telephone:
Date : Signature:

CUSTOMER INFORMATION:

Company name / NOM de la société : .....
Address: .....
Manager: ..... Company activity / Secteur d'activité : .....
Telephone: .....

PABX CONFIGURATION INFORMATION:

PABX Replacement /Remplacement Yes /No Expansion/ Adjonction Yes /No

Request For Quotation / Appel d'offre : Yes /No RFQ attached to this demand A.O. joint à la demande Yes /No

Type of PABX:
Current/ Actuel :..... PABX FULL DECT : Yes /No
Future: ..... Number of wired sets / Nombre de postes filaires : .....
Network PABX Building number
Multisite : ..... / Réseau PABX: .....Campus: ...../Nb bâtiments :..
Notification server :..... Group/Supervision: .....

Zone designation: ..... ***Data for each zone***

Quality of Service Level :	1	2	3	4

MOBILE INFORMATION	Quantity	Expansion	Mobile only/ Mobile seul	Tandem with wired set / mobile + fixe	Resident DECT set / DECT fixe	High traffic zones / Zones à fort trafic	
4072							
4074							
4036 (4097)							
Reflexe 100-200							
Others / autres							

SITE

Offices/ Bureaux : ..... Warehouses/ Entrepôts : ..... Workshops/Ateliers : .....
Plant / Usine : ..... Explosion environment : ..... Clean rooms / Salles blanches :.....
Others/autres : .....
Number of floors/Nbre de niveaux :.....Number of underground levels/Nbre de sous-sols :.....
Coverage/Couverture
Indoor/ Intérieure : ..... Outdoor/ Extérieure : ..... Surface (m²) :.....

Building / Bâtiment	Concrete/Béton	Metal /Métal	Glass / Verre	Stone / Pierre	Plaster/Placo	Open space/ Paysager
Structure						
Wall / cloison						

Others/ autres : ..... Future expansion: .....
Floor plan availability / Disponibilité plans : Yes /No Where / où :.....

Site constraints / Contraintes sites :

Safety plan/plan de prévention :	Checked access / Accès réglementés : .....

(1) Offer date / Date de remise de l'offre :	Commissioning date/ Date de mise en service : .....

APPENDIX 3: Criteria for Central Pre-sales Support Escalation

Criteria:

- **Full DECT**
- **Traffic per user greater than 0.25 Erl**
- **Difficult coverage for industrial, plant, white room, ship, etc. type sites. Multi pari, multi crystal system, with Campus risks.**
- **System with new functions, such as: group call, etc.**

Documents required for escalation:

- **The "DECT radio coverage study request" completed for each zone.**
- **The description of the site with the plans/drawings of the different floors (associated measurements)**
- **The identification on the plans of the specific places (associated measurements) (tunnel, restaurant, white room, Faraday cage, etc.)**
- **The radio measurements report and the coverage study Data regarding the existing traffic (Erl and number of calls)**

5.1.1.3 4070IO/EO Base stations

5.1.1.3.1 Installation procedure

The Alcatel-Lucent 4070 IO base station is designed for internal installation in the building, whereas the Alcatel-Lucent 4070 EO base station is designed for external installation.

Attaching a4070 Base Station

Attaching a 4070 IO Base Station

The 4070 IO base station is supplied with an attachment kit comprising:

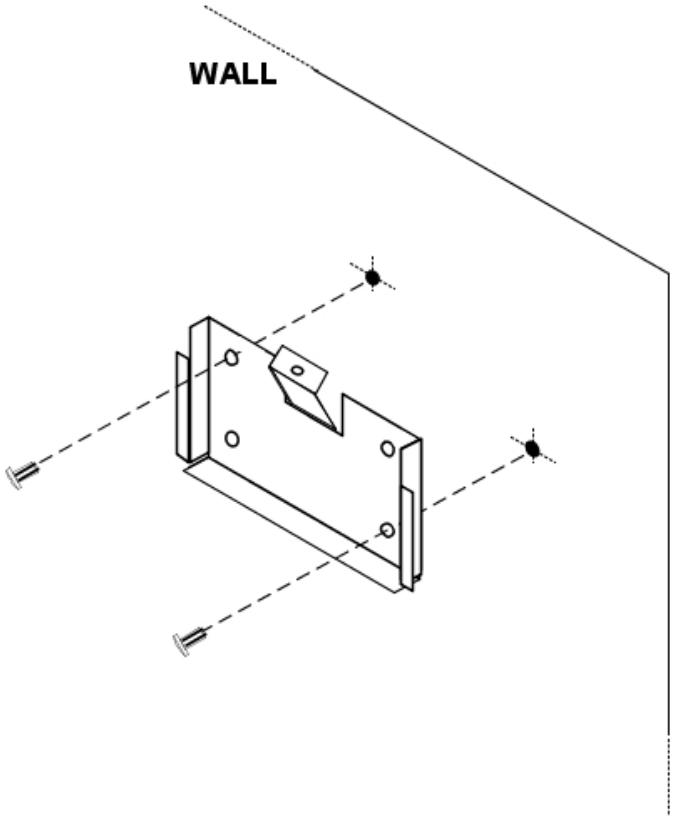
- a metal attachment bracket,
- 2 screws (Ø3.5 x 25 mm) and 2 dowels (Ø6 x 30 mm).

There are two methods of fixing the base station to a wall (in the vertical position):

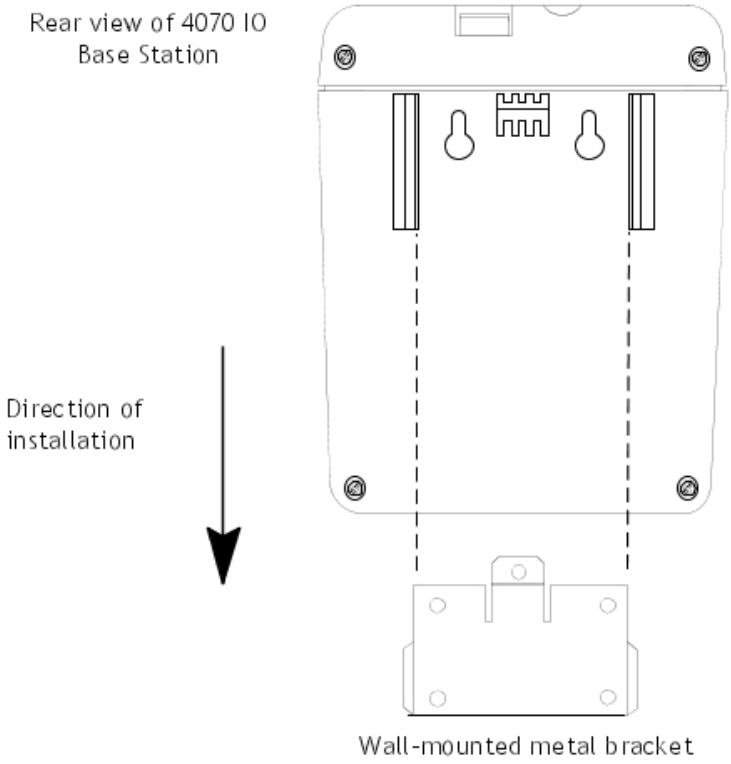
1. by mounting the base station on a metal bracket,
2. directly on the wall, by means of the two slots provided in the base station.

Mounting a 4070 IO Base Station on a Metal Bracket

The metal bracket is used as a template to locate the position of the drill holes on the wall. Drill the holes and install the dowels. Put the metal bracket in position and screw it into place as follows:



Once this has been done, slide the 4070 IO base station into the slots provided on the bracket as shown below:

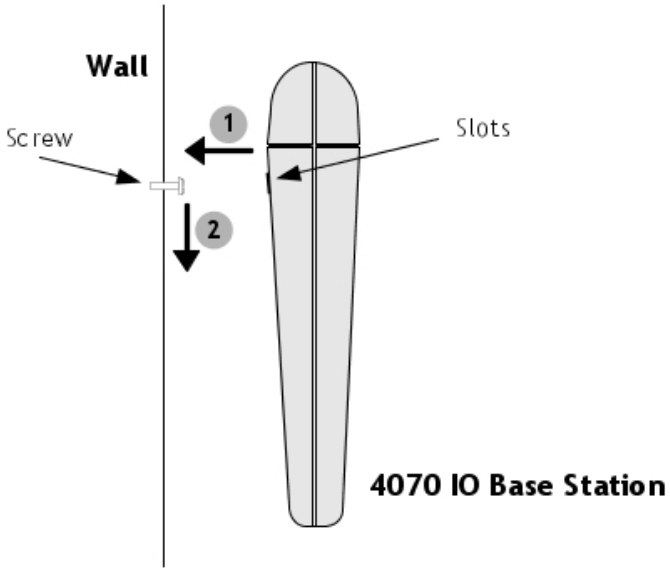


Remark:

The base station must be installed with the LED at the top.

Attaching a 4070 IO Base Station Directly on the Wall

Locate the position of the drill holes on the wall (distance between the two holes: 55.2 +/- 2 mm), then drill the holes and insert the dowels. Tighten the screws leaving sufficient space between the screw head and the wall. Position the base station slots at the same height as the screw heads (in 1) then move the station down to lock it in position 2 .



Attaching a 4070 EO Base Station

Wall and Mast Mounting Kit

Wall Attachment

The 4070 EO Base Station can be mounted on a wall:

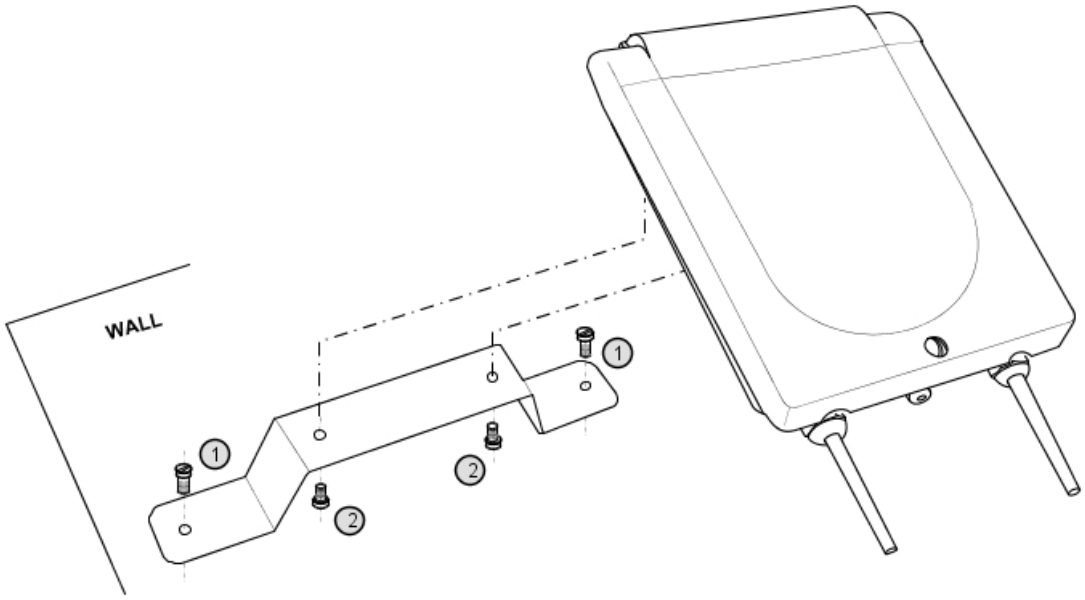


Figure 5.14 : Wall Attachment for a 4070 EO Base Station

1. Attach the wall support to the wall with two screws (not provided)
2. Attach the 4070 EO Base Station to the support with the two screws provided

Mast Attachment

The 4070 EO Base Station can be mounted on a mast:

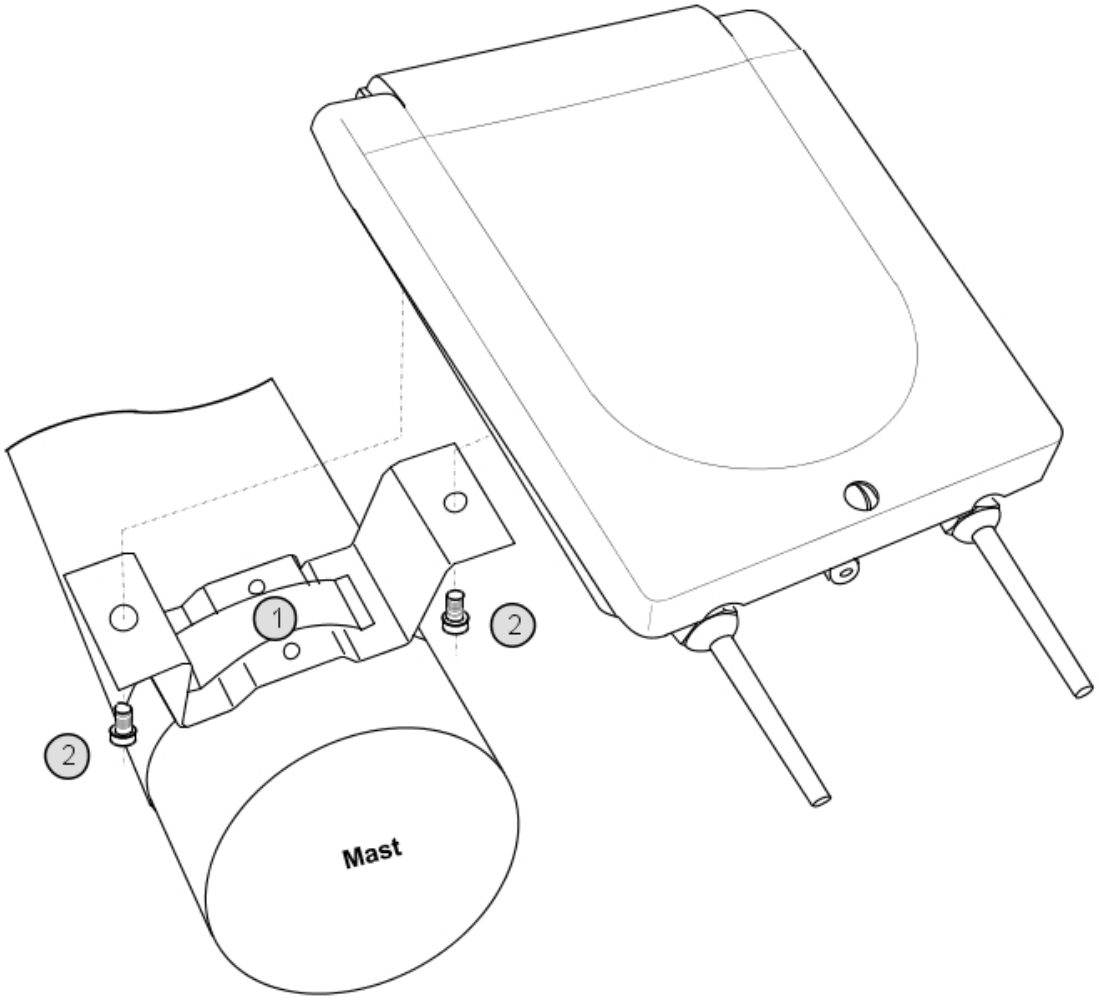


Figure 5.15 : Mast Attachment for a 4070 EO Base Station

1. Attach the mast support to the mast with a pipe-collar (not provided)

2. Attach the 4070 EO Base Station to the support with the two screws provided

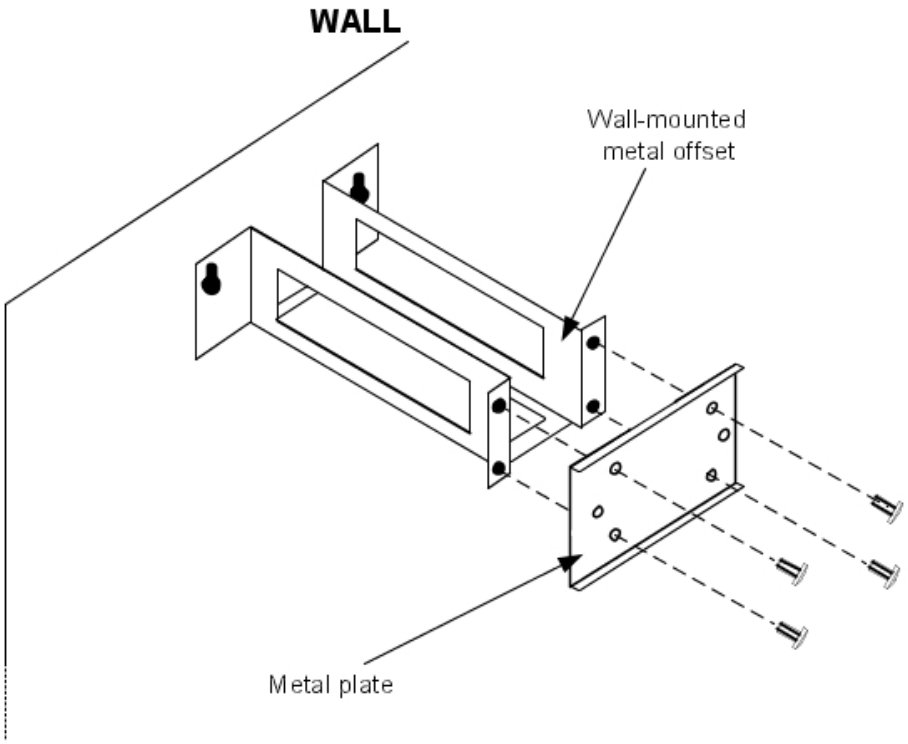
Wall Offset Mounting Kit

This kit is not included in standard delivery of the 4070 EO Base Station. It must be ordered separately.

The base station is mounted as follows:

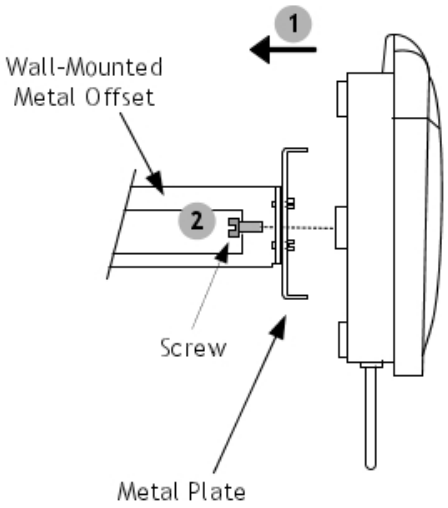
1. Position the metal plate on the offset and attach it with the screws:

   Remark 1:
   screws to be used: Ø3.5 x 25 mm.



2. When the metal plate has been mounted on the offset, position the base station on the metal plate (in 1) then attach it with the screws (in 2) as follows:

Remark 2:
use the 2 hex head screws provided with the kit.



Connection

A base station may be connected to 1 or 2 UA links (UAI boards) and allows 3 or 6 simultaneous connections with DECT/GAP terminals.

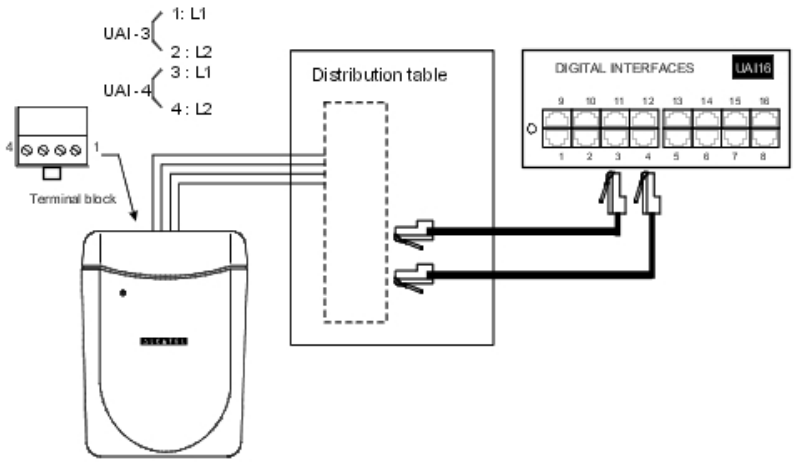
The need for three or six communication channels depends on the number of wireless sets and on the DECT traffic to be managed.

If there is a two-cable connection:

- use two neighbouring interfaces of the UAI board
- use the odd interface for the master link and the other for the slave link.

Both cables should be the same length. The first interface of the system's UAI16 board should not be used since the attendant station uses that interface.

Wiring



Internal Power Supply

- The power outlet adapter serves as a sectioning device
- The surface socket must be installed as close to the base as possible and must be easily accessible.

Configuration

Note:

Differences between 4070 and 4070 NG base stations: *on DECT 4070 base stations, the change of antenna occurred when the error rate was in excess of a specific limit. On DECT 4070 NG bases, in addition to the change of antenna described above, there is a fast antenna change call "Fast antenna diversity"; this change occurs automatically as soon as the mobile sets receiving levels become too weak.*

- Define the length of the line: because the connection distances between the modules and the base stations (1200m max.) differ, you must compensate by making the propagation length more or less identical. The following choices are available:

- short line: 0 to 400 m (default value)
- medium line: 400 to 800 m
- long line: 800 to 1,200 m

By OMC, select: **Users/Base stations List** -> **Users/Base stations List** -> **IBS Master** -> **Details** -> **Line Length**.

This programming operation is necessary to install the base station. If modified during use, the base station will be reset (regardless of any call in progress).
In the case of a mixed environment (4070 and 4070 NG bases), the installer may change the antenna diversity on several base stations at the same time.

- Define the number of antennas used: it may be necessary to cancel antenna diversity for specific needs.

By OMC, select: **Users/Base stations List** -> **Users/Base stations List** -> **IBS Master** -> **Details** -> **Antenna Diversity** -> No Diversity = 1 antenna (4070 and 4070 NG bases); Slow Diversity = 2 antennas (4070 and 4070 NG bases); Fast Diversity = 2 antennas (4070 NG bases only).

In the event of modification during use, the base station will be reset (regardless of any call in progress).

- Define the DECT frequencies used: A 4070 IO/EO base station can operate with 1, 2, 4, 5, 8 or 10 frequencies. When booted, all 10 frequencies are available (configuration varies according to the system's software version).
  Configuration before R2.0

By OMC, select: **System Miscellaneous -> Memory Read/Write -> Debug Labels -> "Dect_Freq"** -> enter the 2-byte value corresponding to the mask for the desired frequencies.

The default value of the mask is 03FF (all 10 frequencies used); this value must only be modified under particular installation conditions, normally outside Europe.

PROGRAMMING				EFFECT ON SYSTEM			
Value of mask ("Dect_Freq" address)		Chosen frequencies		Mask validated by the system		Validated frequencies	
Hex	Binary	Number	Range	Hex	Binary	Number	Range
03FF	0000 0011 1111 1111	10	1 - 10		0000 0011 1111 1111	10	1 - 10
003F	0000 0000 0011 1111	6	1 - 6		0000 0000 0000 1111	4	1 - 4
0282	0000 0010 1000 0010	3	2, 8, 10		0000 0000 1000 0010	2	2, 8
0000	0000 0000 0000 0000	0	none		0000 0011 1111 1111	10	1 - 10
003C	0000 0000 0011 1100	4	3 - 6		0000 0000 0011 1100	4	3 - 6

Configuration using R2.0 (the labelled address "Dect_Freq" is no longer operational).

By OMC, select: **System Miscellaneous -> DECT Frequency Plan** -> select the desired frequencies (frequencies between 1880 and 1898 MHz are suggested with 2 MHz increments).

Perform a warm reset of the system, or reboot each base station individually.

Installing the Base Stations

To install the base stations, follow the steps below:

- position the base stations (depending upon the result of the coverage studies)
- connect the base stations
- power down the system
- by OMC:
  - if necessary, modify the numbering plan and the account codes table
  - provide a name for each station installed
  - if necessary, modify the value associated with the "Line length" parameter
  - create the DECT accesses then declare the type of station (DECT UA) or use automatic registration (DECT GAP)
  - the default value being the same for all the systems, modify the PCX ARI value by configuring it with the ARI from the manufacturer
  - complete the system settings (trunk groups, call restriction, etc).

5.1.1.4 Configuring the system

5.1.1.4.1 Configuration procedure

Configuring the system's DECT/PWT mobile functionality consists of programming the ARI number and the GAP authentication code (if necessary). Both of these parameters must be completed before registering a set on the system.

Before starting the DECT/PWT configuration, the dialing plan must be defined and the hardware configuration (installing interface boards, recognizing sets, etc) completed.

ARI NUMBER

The ARI (Access Right Identifier) number identifies the system uniquely to mobiles. It contains 11 octal digits (base 8). This number, assigned to an ETSI base by the installer, must be entered on installing the system.

It is structured as follows:

- the ARC (Access Right Code) specifies the usage environment (private, public, etc); in the case of Alcatel-Lucent OmniPCX Office Communication Server, a type-B ARI is assigned by the DECT/PWT protocol (ARC = 1, non modifiable)
- the EIC (Equipment Installer Code) is the number assigned by ETSI to each maker or distributor offering DECT/PWT systems
- the FPN/S (Fixed Part Number/Subnumber) is a number entered by the installer: each system installed by the same installer must have a different number.

- To enter the system ARI number with OMC (Expert View):

Select: **System Miscellaneous**-> **DECT/PWT/ARI/GAP**-> enter the ARI number (the system deduces the EIC, FPN and FPS fields automatically).

- To enter the system ARI number with MMC Station:

Select **DECTor PWT** -> **ARI** -> enter the ARI number and validate by clicking **OK**

Important:

The ARI number must be modified by the installer (following the above rules) before registering any DECT/PWT sets.

GAP AUTHENTICATION

This service secures data exchange between the system and the DECT GAP handsets.

An authentication code can be sent by the mobile to the system during the registration procedure. This code is then compared with the one configured in the system. If it matches, the registration of the set can continue; if not, it is stopped.

- To define an authentication code with OMC (Expert View):

Select: **System Miscellaneous**-> **DECT ARI/GAP Authentication**-> check **? Activate GAP Authentication** -> enter a code of between 4 and 8 digits in **Authentication code**

- To define an authentication code with MMC Station:

Select **DECT** -> **AuthCd** -> enter a code of between 4 and 8 digits and validate by clicking **OK**
Select **DECT** -> **Authen** -> activate or deactivate with **Choice** and validate by clicking **OK**

REGISTERING A GAP HANDSET

DECT sets are identified by their IPUI N (International Portable User Identity type N). Each handset has a different IPUI N number, used when the set is declared to the system.

In the case of a DECT GAP handset, the IPUI N and ARI parameters are exchanged automatically during the registration procedure. It is through these parameters that the system recognizes the handset, and vice versa.

Procedure with OMC

Select: **Users/Base stations List**-> **Users/Base stations List**-> **Add** -> add the required number of DECT accesses by selecting **DECT handsets** and the number of devices, then validate by clicking **OK**

Select **Users/Base stations List** -> **Users/Base stations List** -> **GAP Reg.** -> The GAP registration procedure is under way when the **Register GAP Handsets** window appears.

On the mobile

Launch the registration procedure on the handset (refer to the accompanying documentation).

As soon as the mobile's IPUI number appears, select an unassigned number mobile and click **Assign**. The IPUI number, preceded by the mobile number, then appears in the **Assigned Handsets** window

Procedure with MMC Station.

Select **DECT** -> **Add** -> **GAP** -> The message "In Progress…" is displayed; the registration procedure is under way.
Launch the registration procedure on the handset (refer to the accompanying documentation).
When the mobile's IPUI number appears, validate by clicking **OK**.
The mobile is registered and a number is automatically assigned to it.

Basic GAP and Advanced GAP

In certain instances, the handset shown in the Unassigned IPUIs window may be a GAP type set; if so, you can select the preferred: Basic or Advanced.

Select the IPUI number and click **Modify Mode**.

5.1.2 PWT Overview

5.1.2.1 Basic description

5.1.2.1.1 PWT

PWT (Personal Wireless Telecommunications) is the US DECT protocol that uses the frequency band 1910Mhz-1930Mhz.

DECT and PWT frequencies are supported by different IBS (Intelligent Base Stations).

The PWT IBS can be used without any specific licence.

Hardware aspects

DECT IBS and PWT IBS cannot run together on the same PCX.

As soon as the first IBS is detected, the system becomes DECT or PWT.

The next IBS must be of the same protocol (DECT or PWT) as the first one.

To switch from a DECT system to a PWT system, and vice versa, unplug all IBSs, do a warm system restart and plug in the IBSs.

Software aspects

The IBS (DECT or PWT) software is downloadable from the PCX.

When an IBS is started and if the version of the software in the IBS (DECT or PWT) is newer than the version embedded in the PCX, the PCX downloads the software from the IBS.

The PCX embeds only one IBS software version, assumed to be the latest one.

The PCX embeds the following software variants:

- IBS 1G,
- IBS NG (compatible with hardware 2 chips or oldest hardware, also compatible with normal DECT frequencies and shifted frequencies),
- IBS PWT

  Note:
  IBS PWT has software version 001.00X (001.002 being the latest version).

DECT/PWT terminals are not downloaded by the PCX. They have to be downloaded manually using special chargers.

5.1.2.1.2 DECT/PWT frequencies for US installations

Now DECT and PWT can be used in US installations, but they cannot be used simultaneously.

The DECT/PWT frequencies screens have been modified for US installations to show what type of IBS the system uses.

The following two figures show the frequencies for DECT IBS and PWT IBS.

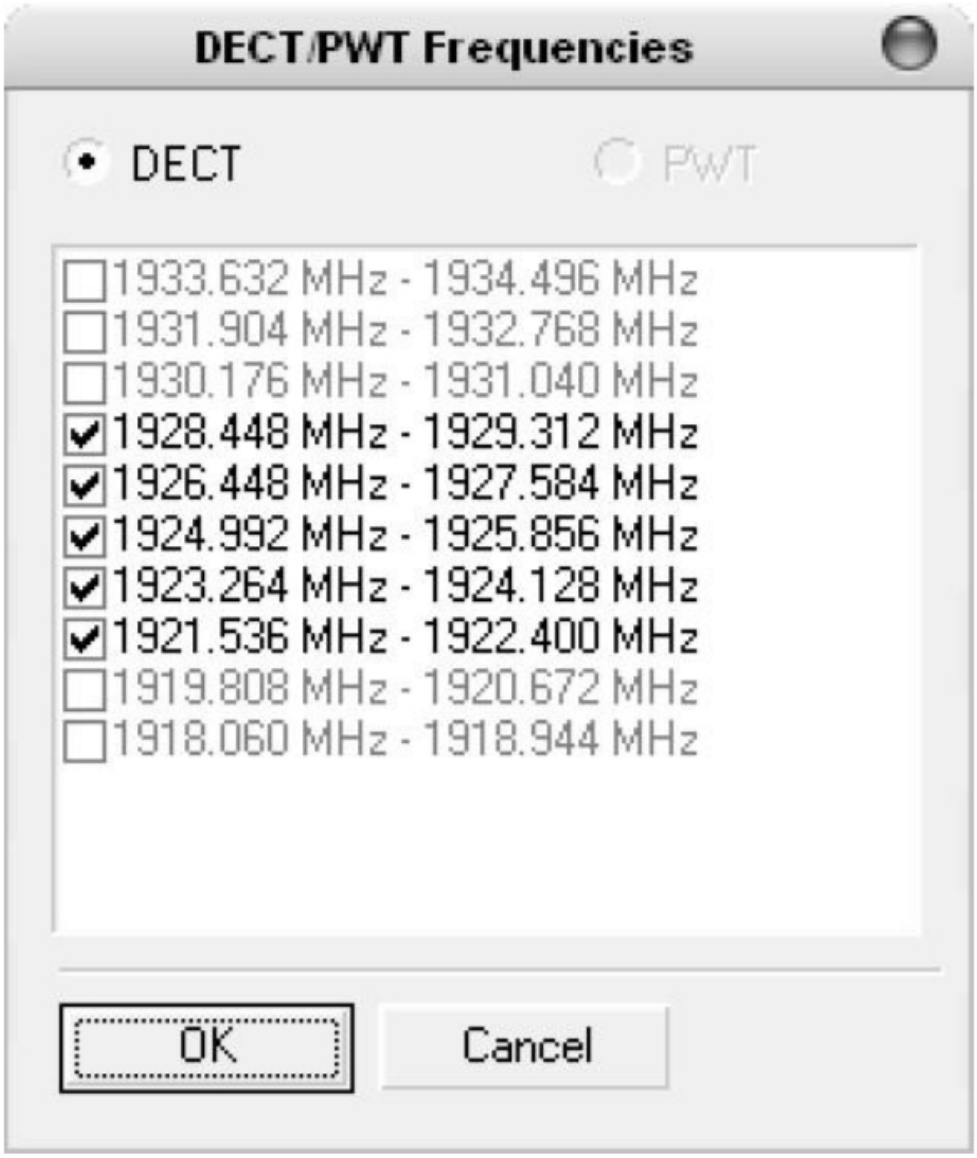


Figure 5.20 : DECT Frequencies

Note:
For DECT IBS, only 5 frequencies can be modified.

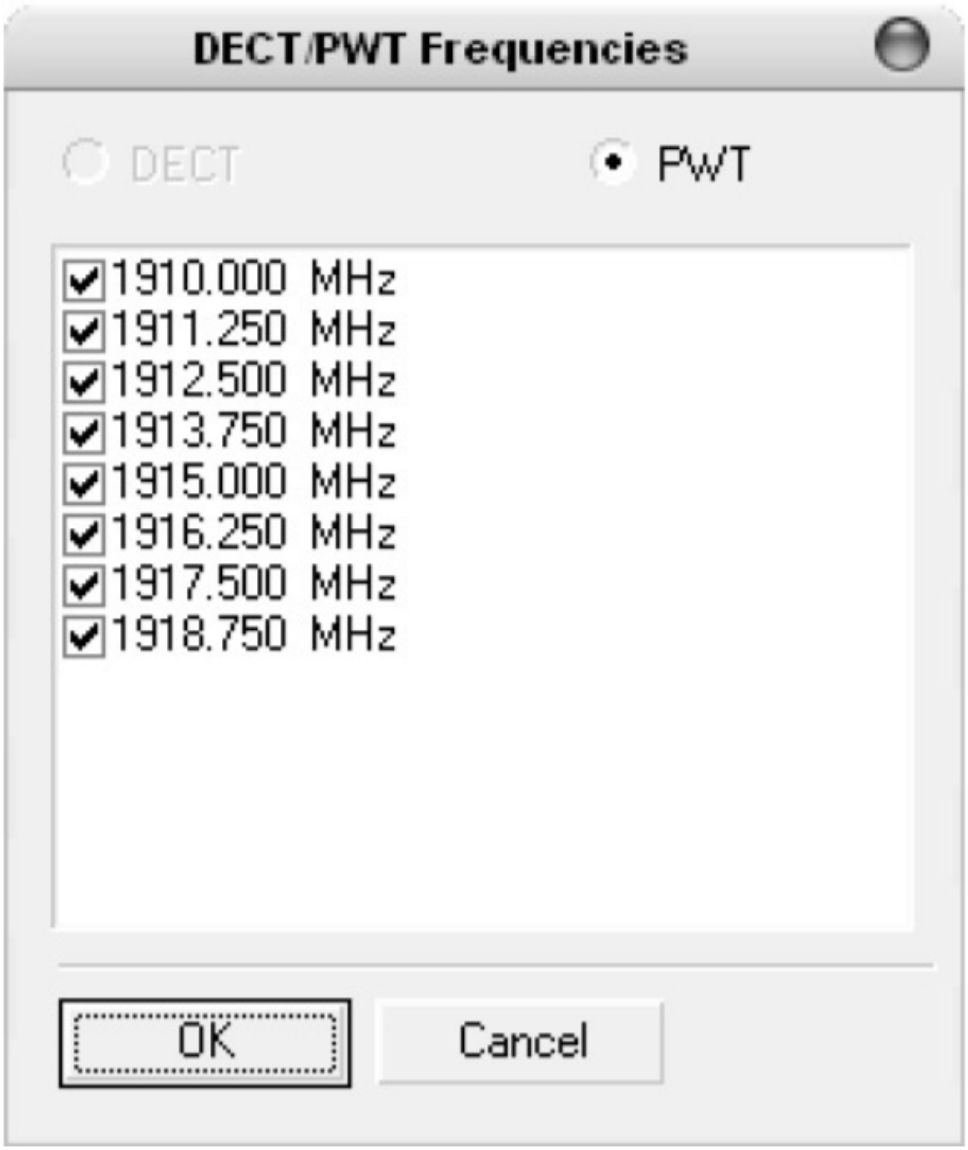


Figure 5.21 : PWT Frequencies

5.1.3 Mobile Reflexes Handset

5.1.3.1 Registering the handset

5.1.3.1.1 Operation

In new sets, the battery included is factory pre-charged. When the terminal is brought into service, the residual charge level is usually enough to power the registration stage.

Fit the battery into the handset and check that the level of charge is adequate (full or half-charge icon); if not, put it on charge.

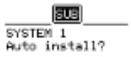
Start the registration procedure on the PCX.

When the system is ready, continue with the handset.

Step A

Turn on the handset by a long press on and observe the screen display.

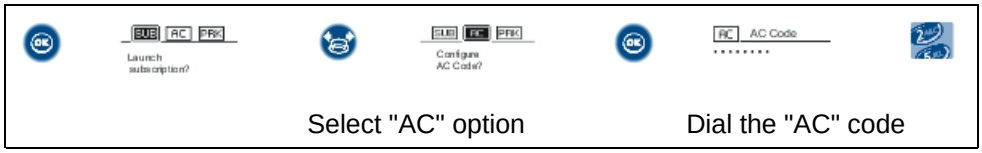
- If the set is new (never been assigned) and has enough battery charge, the display shows "SYSTEM 1 Auto install ?" ; go to **Step B**.



- If the set does not display "SYSTEM 1 Auto install ?", it is already assigned on another system; go to **Step C**.

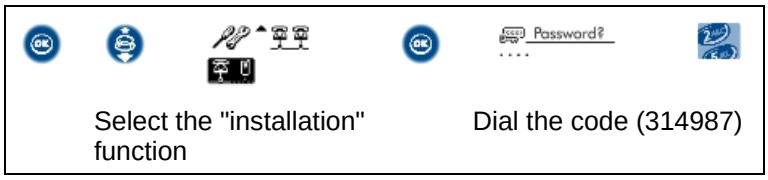
Step B

- If the installation doesn't use the authentication function (AC code), go directly to **Step D** for the simplified procedure.
- If the system uses an authentication code, configure the AC code as described below, and move on to **Step D** to complete the association process.

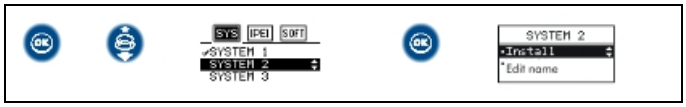


Select "AC" option — Dial the "AC" code

Step C



Select the "installation" function — Dial the code (314987)



Select a free system	Select the "Install" function and proceed with step B

Step D

Launch the registration procedure.

Launch the association process

After registration, the set switches automatically to the main language of the PCX.

5.1.3.2 Uninstalling the handset

5.1.3.2.1 Operation

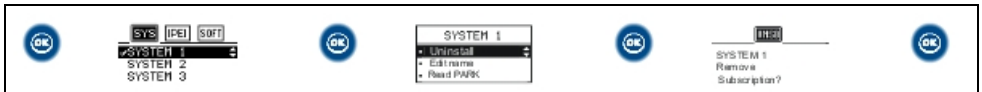
It may be necessary to uninstall a handset when it is no longer used on the system or when the terminal is replaced. The operation must be performed simultaneously on the system and on the terminal.

IMPORTANT

We recommend performing the operation on the terminal (as described below) before deleting it from the system. If this sequence is reversed, it is still possible to delete data from the terminal, but this has to be done outside the radio coverage area.

Select the "installation" function

Dial the code (314987)



Select the system to be uninstalled

Validate the "Uninstall" option

Confirm the uninstall operation

5.1.3.3 Services provided

5.1.3.3.1 Basic terminal functions (accessible in GAP or AGAP mode)

- Lock / unlock keypad (long press on)
- Activate/deactivate keypad beep, key beep, radio beep, vibrator * back lighting **
- Quick switching from ringer to vibrator * (long press on)
- 3-level reception volume adjustment with storage of the most recent setting
- Registration possible on 5 different GAP systems
- Special radio test function (see "Radio Test Mode ")

* Mobile Reflexes 100

** Mobile Reflexes 200/200 Ex

5.1.3.3.2 Functions specific to simplified GAP mode

In GAP mode, the following functions should be available (unless inhibited by system constraints):

- Manual language selection for the local menu
- Choice of ringing tunes
- Personal speed dial
- Local redial
- DTMF end-to-end signaling
- Calibrated loop

5.1.3.3.3 Functions specific to AGAP advanced mode

Outline of the main functions available, built into the PCX:

- Diversion and cancel diversion
- Audio and text message consultation
- Dial by name / collective speed dial
- Personal speed dial (system numbers)
- Automatic language configuration
- Choice of ringing tunes
- Interactive features in conversation

5.1.3.4 Maintenance

5.1.3.4.1 Reading the handset software version number

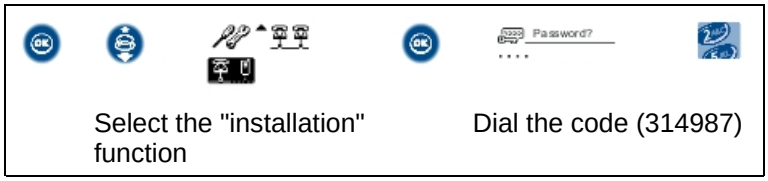
Select the "installation" function

Dial the code (314987)

Read version n#

Note: each terminal model has its own identification prefix: 70 xxxx for Mobile Reflexes 100 models and 60 xxxx for the Mobile Reflexes 200 models.

5.1.3.4.2 Reading the handset IPEI number (handset ID)



5.1.3.4.3 Resetting the EEPROM

This function restores the terminal to its factory settings, i.e. associated with no system and containing no saved data.

- Turn the handset off and on again, simultaneously pressing On-hook, Off-hook and **i**.
- Select **EEPROM Reset** and validate.

5.1.3.4.4 Quitting battery security mode

The set can activate automatic security mode on the battery in the event of a short circuit, a critically flat battery (after several weeks without charging) or an excessive charge voltage. Some of these incidents may arise when the handset suffers a violent impact.

When security mode is activated, the mobile is powered down and will not come back on.

To deactivate security mode:

- remove the battery and replace it in the mobile
- place the handset (turned off) on the charger
- press the handset "on" key without removing it from the charger.

5.1.3.5 Radio Test Mode

5.1.3.5.1 Operation

RADIO TEST MODE

Activating radio test mode

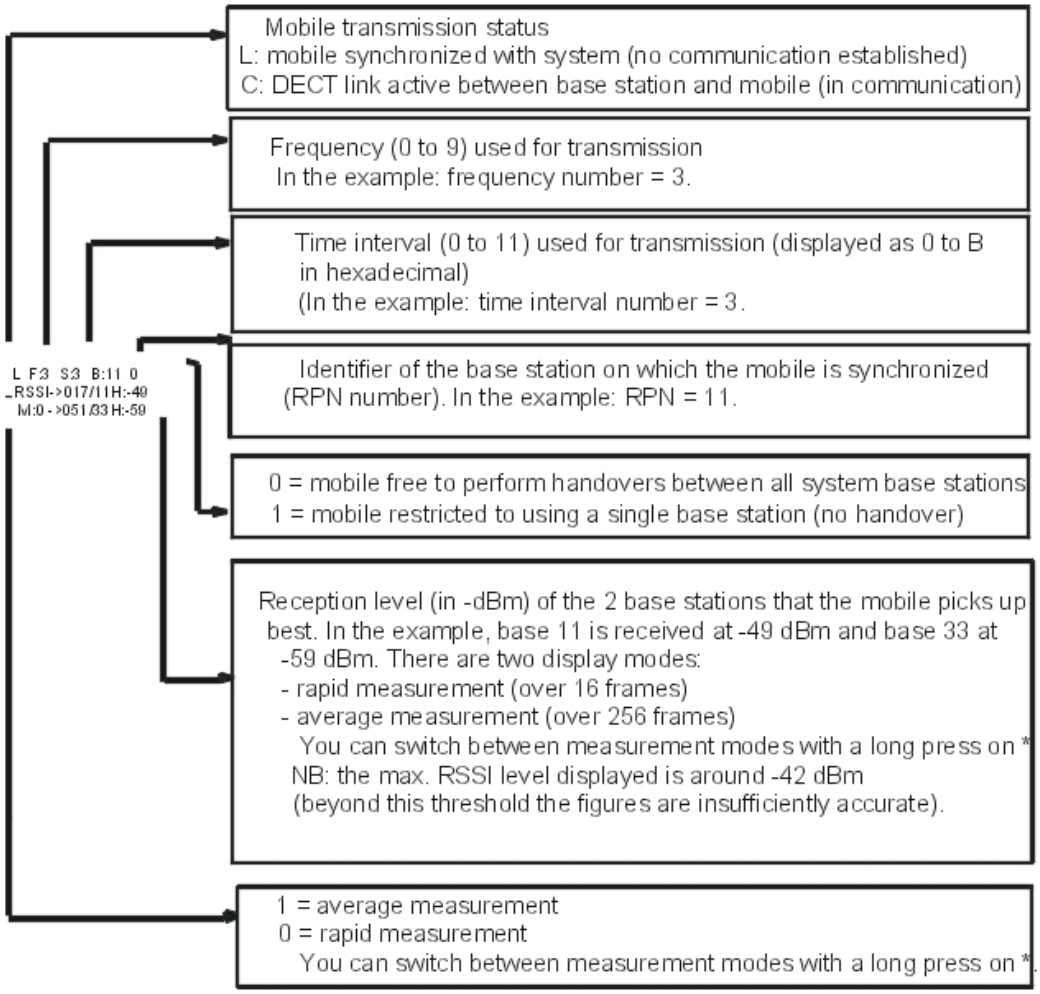
To activate radio test mode:

- turn off the mobile by a long press on
- turn it back on by pressing simultaneously on , and
- when the display comes on, do a long press on

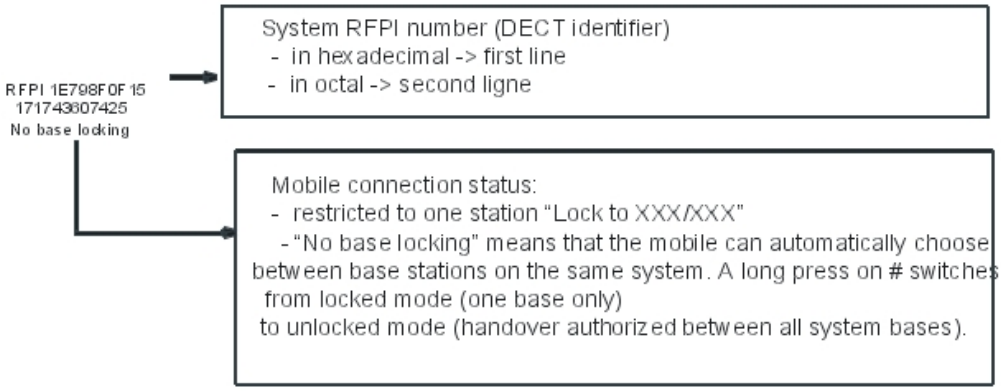
The screen displays the state and reception level measurements.

Description of radio test mode functions

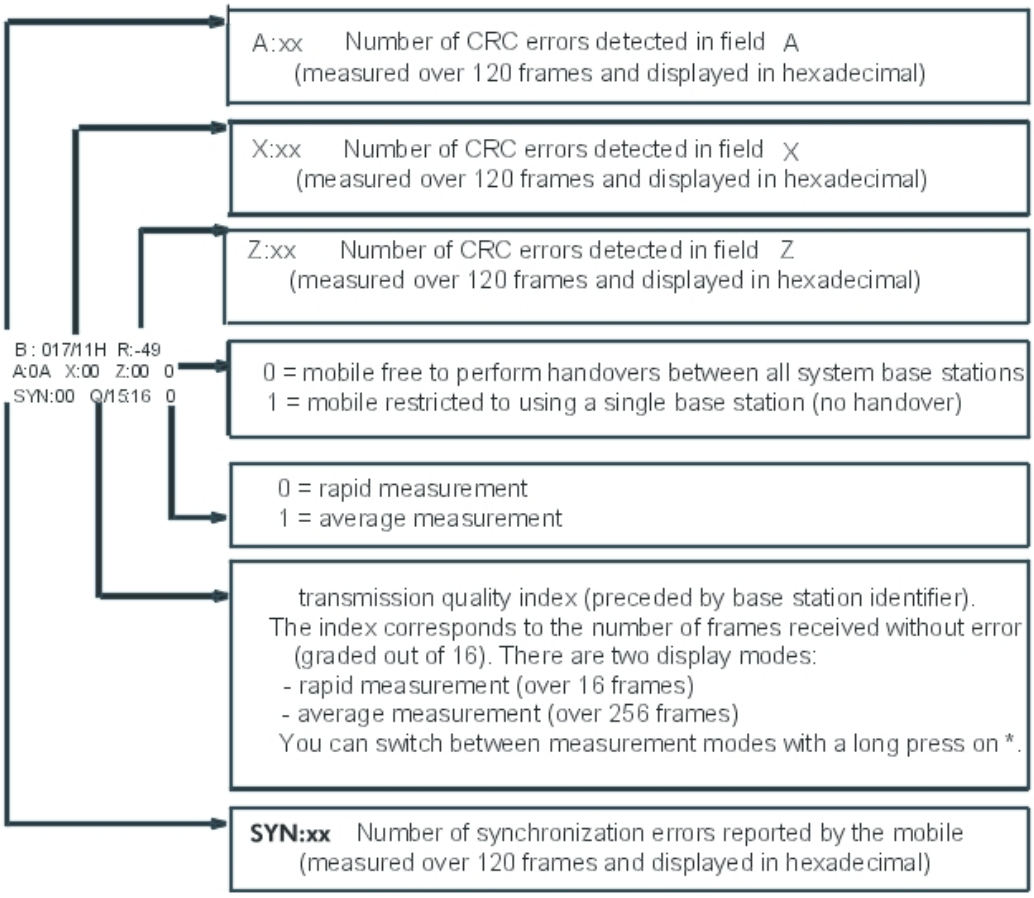
STATE / RSSI (state / reception level)



IDENTITY (system RFPI number) / CONNECTION STATUS



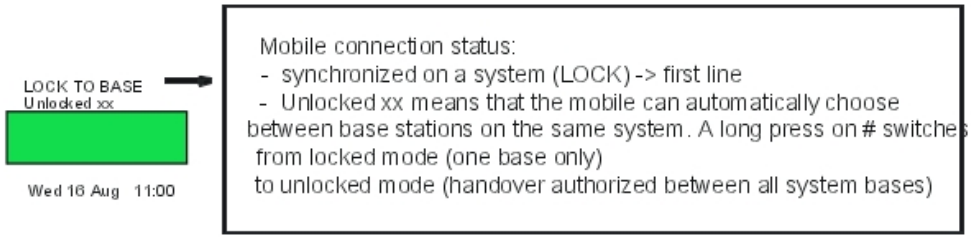
QUALITY (reception quality)



Note: the quality index gives an objective picture of the communication quality in order to determine the practical range limits (depending on the distance from the handset and the nature of the environment).

In practice, you have to select this function (preferably the averaged measurement), set up a call, and observe the index value (Q): at a given location, the quality can be considered good if the value displayed is equal to or greater than 12 on a stable basis.

CONNECTION STATUS (synchronization)



This function makes it easier to determine the coverage area of a base station.

5.1.4 Reflexes DECT Sets

5.1.4.1 Installing a set

5.1.4.1.1 Installation procedure

The registration of a DECT Reflexes set (with the 4097 CBL option) is performed by radio data exchange with the system. Before attempting the association, it is therefore important to check that the DECT bases are operational and that the sets are located in an area with adequate coverage.

In order to limit traffic during installation of the sets, it is advisable to register the DECT Reflexes sets in sequence, one after the other.

Note:

The DECT-GAP authentication procedure (described in file 3) is not available with DECT Reflexes sets.

REGISTRATION PROCEDURE FOR A NEW SET

New sets are delivered from the factory without any registration data; they are brought into service using a simplified procedure.

After adding a DECT set, go into GAP registration (MMC-Station or MMC-OMC) and initialize the association procedure up to "Subscription running".

Then switch on the set's power supply, connecting the transformer block to the power outlet and check the red LED at the back of the set: the LED should send a short series of "long ON/short OFF" flashes, then go out as soon as the set is synchronized with a base station.

At this point, the registration request is performed automatically by the set. The terminal identifier appears on the system's MMC and the attendant only needs to validate the directory number and confirm the registration.

Note: after the registration phase, if the directory number of a DECT Reflexes set has to be changed, its power supply block must be disconnected, then reconnected, after the modification has been made in the system.

REGISTRATION PROCEDURE FOR A PREVIOUSLY REGISTERED SET

If, during a registration attempt, the red LED flashes "short ON/ long OFF", this means that the set contains configuration data. To delete the data, proceed as follows:

- disconnect/reconnect the power supply;
- 2-3 seconds after switching on the power supply again, enter the following sequence of digits on the keyboard: ***#*86734#*#** (which corresponds to the alphabet code *#*UNREG#*# using the number keys); the first character must be entered within 10 seconds;
- again disconnect/reconnect the power supply; automatic registration as described in the paragraph above is initialized.

General conditions of installation

- **location:** This office set must be located in an environment with limited risk of electro-magnetic disturbance and which allows for good quality radio transmission. For

example, avoid placing the set near items such as dense metal structures, television, fluorescent strips, halogen lamps, PC monitors, etc.

- **PCX limits:** a DECT Reflexes set is considered both as a Reflexes line set and a DECT terminal. The installation must include a Reflexes corded set in order to perform the Operator function.
- **radio operation**: the DECT Reflexes set operates in dynamic DECT link mode (just like a conventional DECT mobile) or static mode (just like a corded set). The communication channel is set up with the base station each time there is a need to exchange data with the PCX. At the end of an exchange, when the set is in stand-by mode, the radio link and communication channel resources are released and made available to the base station.
- **coverage study**: This is performed in the conventional way, just as for a system equipped with DECT mobile terminals. Apart from the specific use of the terminal as a static office set, it is recommended that a sufficient radio level be maintained in order to guarantee excellent communication quality.
- **limits for standard traffic needs**: the maximum number of DECT Reflexes terminals that can operate in the same zone is the following:
  - for an area covered by one radio base station (NOTE 1)
  - 4070IO/EO base station with 3 channels: 4 sets
  - 4070IO/EO base station with 6 channels: 12 sets
  - for an area covered by a group of co-located base stations (NOTE 2)
  - cluster of two 4070IO/EO base stations with 6 channels: 30 sets
  - cluster of three 4070IO/EO base stations with 6 channels: 50 sets

Note:

1. irrespective of the model of the DECT set (any type of 4074, or DECT Reflexes)

2. The topology of co-located base stations is a specific solution that makes it possible to increase traffic capacity in an area: this specific area is identically covered by the various base stations that make up the cluster. To set up a base station cluster it is necessary to make sure that the DECT sets are compatible with this topology, which requires an overflow function not available on some DECT set models.

Remarks:

- Operating and programming limits at system level **(inherent in the dynamic DECT link operating mode of DECT Reflexes sets).**
- Avoid allocating DECT Reflexes sets to hunting groups; however, if the use of this type of set is inevitable, limit their number to 4 per group.
- Number of DECT Reflexes sets in manager-secretary configurations: 4 manager sets and 4 assistant sets.
- Do not use DECT Reflexes sets as call monitoring sets (selective or general) or to monitor resources.
- Programming the RSP keys is impossible on DECT Reflexes sets.
- Status signaling (free or busy) for sets tracked on RSL keys is unavailable except for sets allocated to manager-assistant configurations.
- Background music is not available on DECT Reflexes sets.
- After a time change made by MMC or after reception of the time sent by the public exchange, it is possible that this modification will not be taken into account immediately by

all the DECT Reflexes sets; in this case, a simple user action (going off-hook, making a call, etc.) is enough to reset the time synchronization on the display.

5.1.4.2 Moving a set

5.1.4.2.1 Detailed description

To move a DECT Reflexes set, it is necessary to disconnect the mains power supply block before installing it in another place.

Reconnect the set for normal use (the set's number and programming will be kept).

Make sure the terminal is relocated in a zone with an adequate radio reception level, one that can cope with the traffic requirements.

5.1.4.3 Supervision

5.1.4.3.1 Overview

DECT MODULE 4097 CBL INDICATOR LED

The red indicator LED at the back of the DECT Reflexes terminal shows the operational status of the module at any given moment:

LED constantly lit (ON)	4097 CBL module defect
LED unlit (OFF)	The module power supply is switched off or the module is correctly synchronized with a base station
Flashing long ON / short OFF	The module is not registered with the system and is searching for radio synchronization
Flashing short ON / long OFF	The registered module is searching for radio synchronization

5.1.5 DECT Traffic Counters

5.1.5.1 Overview

The Alcatel-Lucent OmniPCX Office Communication Server PCX manages a set of DECT traffic counters. These specific counters are mainly used to ascertain that there are enough DECT /PWT devices in an installation (correct quantity and location given the traffic to be handled, number of calls per handset, etc.). They can also be used during active maintenance, for example to track any link loss problems with a radio base station or handset.

DECT/PWT counters are read with OMC, using the labeled addresses (this displays the content of a specific memory area in table format).

The address **System Miscellaneous -> Memory Read/Write -> Other Labels -> DectCntOn** activates or deactivates the traffic counters when using the system:
- 01: active counters (CAUTION: incrementing the counters may have an impact on the response time of an already heavily loaded system)
- 00: inactive counters (default value)

5.1.5.1.1 GENERAL OPERATION

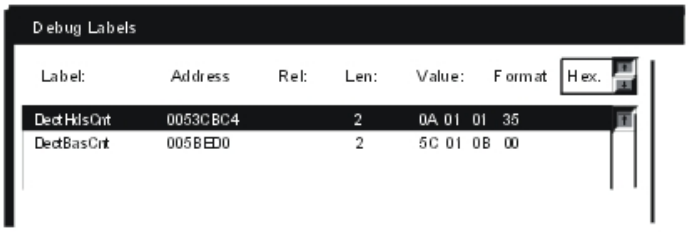
To measure the DECT/PWT traffic, 7 counters are associated with each active DECT base station (connected and in service) and another 6 are associated with each DECT/PWT

handset. Each of these counters gives specific traffic data. When there is a cold system reset, the content of the counters is automatically reset to zero.

The counters associated with the radio base stations (" **base station counters**") and those associated with the handsets (" **handset counters**") are placed in two separate tables.

The start address of each of these tables varies from one system to another, depending on the software version. This address must therefore be read beforehand by the usual means:" **Memory Read/Write -> Debug Labels**":

- the start address of the base station counters is given by the label **DectBasCnt** (005BED0 in the next example).
- the start address of the handset counters is given by the label **DectHdsCnt** (0053CBC4 in the next example).



Remarks:

- In OMC, the content of a traffic counter is always a hexadecimal (base 16) value encoded over several consecutive addresses. To obtain the corresponding decimal value, the values displayed must be converted manually (see following examples).
- On the first initialization, during the installation startup, all the addresses corresponding to the DECT/PWT counters contain the value zero (00 hex.). Only the addresses **"position"** and **"device"** contain a fixed value other than zero at this stage.
  All counters are automatically reset to zero when there is a cold system reset. It is however possible to reset one or more base station or handset counters manually, by assigning the value 00 to the corresponding addresses.

5.1.6 DECT Traffic

5.1.6.1 Base Station Counters

5.1.6.1.1 Detailed description

Start address given by content of pointer DectBasCnt

Byte nbr		Content
1		board position
2		device
3	a	nbr calls nb = (b x 256) + a
4	b	
5	a	nbr simult calls nb = (b x 256) + a
6	b	
7	a	nbr saturations nb = (b x 256) + a
8	b	
9	a	saturation time (ms) nb = ((((d x 256) + c) x 256) + b) x 256) + a
10	b	
11	c	
12	d	
13	a	nbr inter handovers nb = (b x 256) + a
14	b	
15	a	nbr intra handovers nb = (b x 256) + a
16	b	
17	a	nbr links lost nb = (b x 256) + a
18	b	
19		position next board
		device

DESCRIPTION OF FIELDS

Board position:

The first byte indicates the position as follows:

- the first figure of the byte + 1 indicates the Xth board of UA type (AMIX-1, MIX or UAI).
- the second figure + 1 indicates the physical position of the board.

A Rack 3, by way of example:

- Slot 1 = UAI16: the master link of the base station is connected to port 15.
- Slot 2 = MIX484: the master link of the base station is connected to port 1
- Slot 3 = SLI4: no DECT base station.
- Slot 4 = UAI16: the master link of the base station is connected to port 5.

3 base stations will therefore be detected in the labeled addresses:

- 0e for the 1st base station with 0 + 1 = 1 (1st UA board in the system) and e + 1 = 15 (port 15 on the board).
- 10 for the 2nd base station with 1 + 1 = 2 (2nd UA board in the system) and 0 + 1 = 1 (port

1 on the board).

- 24 for the 3rd base station with 2 + 1 = 3 (3rd UA board in the system) and 4 + 1 = 5 (port 5 on the board).

Device:

Base index in hexadecimal on the board.

N# of calls:

The cumulative total of calls achieving connected status on the base station in question.

N# of simultaneous calls:

The maximum number of simultaneous communications recorded on the base station.

N# of saturations: total (sat1 + sat2)

sat1 = number of times all the channels in the base station were in simultaneous use.

sat2 = number of times all the available channels were in simultaneous use.

Saturation time:

The cumulative time (in ms) for sat1 saturations.

N# of inter handovers:

The cumulative total of handovers between the base station and another base station.

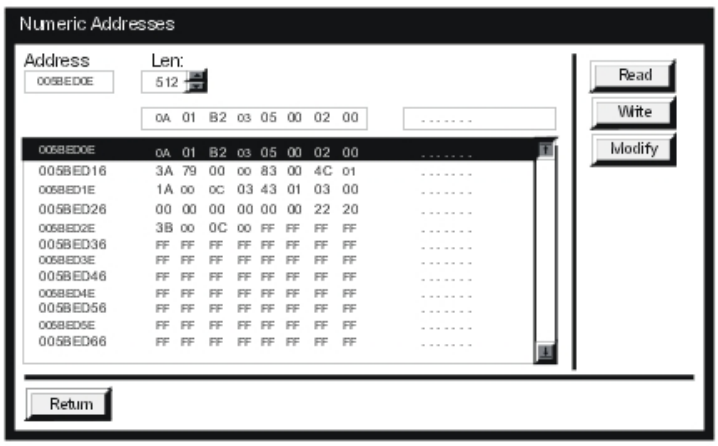
N# of intra handovers:

The cumulative total of intra handovers performed on the base station.

N# of links lost:

The total number of radio links cut off accidentally.

Example: How to read the base station counter table



For the minimum length of the memory area to belisted, assume 18 bytes per base station, hence: (minimum valueto be entered in "**Length**" field) = 18 x total numberof base stations.

In the example, the results recorded for the first base station are as follows:

- board position 0Ahex (10 dec); slot number 6 (main module)

- device : 01 hex (1 dec); first device on the UAI board
- n# of calls : 03 B2 hex (946 dec)
- n# of simult calls : 00 05 hex (5 dec)
- n# of saturations : 00 02 hex (2 dec)
- saturation time : 00 00 79 3A hex (31.034 seconds)
- n# of inter handovers: 00 83 hex (131 dec)
- n# of intra handovers 01 4C hex (332 dec)
- n# of links lost : 00 1A hex (26 dec)

5.1.6.2 Handset Counters

5.1.6.2.1 Detailed description

Start address given by content of pointer DectHdsCnt

Byte nbr		Content
1		position (fixed value = 5C h)
2		device
3	a	nbr links nb = (b x 256) + a
4	b	
5	a	nbr calls nb = (b x 256) + a
6	b	
7	a	nbr coms lost nb = (b x 256) + a
8	b	
9	a	nbr links lost nb = (b x 256) + a
10	b	
11	a	nbr inter handovers nb = (b x 256) + a
12	b	
13	a	nbr intra handovers nb = (b x 256) + a
14	b	
15		position
16		device

DESCRIPTION OF FIELDS

Position:

The virtual slot: its valueis always 5C (92 in decimal).

Device:

The handset index (in order of creation).

N# of links:

The cumulative total of radio links established by the handset.

N# of calls:

The cumulative total of calls achieving connected status on the handset in question.

N# of coms lost:

The number of communications cut off in conversation (lost signal).

N# of links lost:

The total number of radio links cut off accidentally.

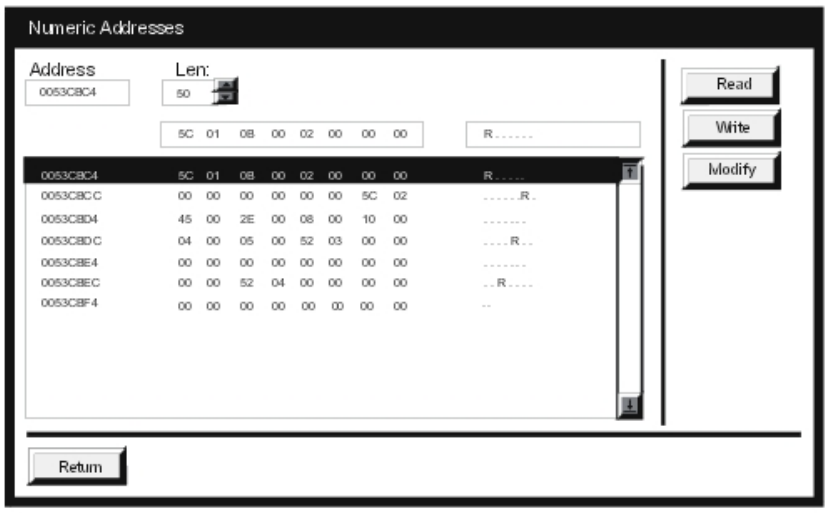
N# of inter handovers:

The cumulative total of handovers performed by the handset between two base stations.

N# of intra handovers:

The cumulative total of handovers performed by the handset on the same base station.

Example: How to read thehandset counters table



For the minimum length of the memory area to belisted, assume 14 bytes per handset, hence: (minimum value to beentered in **"Length"** field) = 14 x total number ofhandsets.

First handset : position : 5C h (92 dec)

device : 01 h (1 dec). See Subscriber menu in OMC to read the corresponding directory number.

n# of links : 00 0B h (11 dec)

n# of calls : 00 02 h (2 dec)

n# of coms lost : 00 00 h

n# of links lost : 00 00 h

n# of inter handovers: 00 00 h

n# of intra handovers 00 00 h

Second handset : position : 5C h (92 dec)

device : 02 h (2 dec)

n# of links : 00 45 h (69 dec)

n# of calls : 00 2E h (46 dec)

n# of coms lost : 00 08 h (8 dec)

n# of links lost : 00 10 h (16 dec)

n# of inter handovers : 00 04 h (4 dec)

n# of intra handovers 00 05 h (5 dec)

5.2 Voice over Wireless LAN

5.2.1 WLAN Overview and Configuration

5.2.1.1 Overview

Voice over Wireless LAN (VoWLAN) enables the convergence of wireless voice and data applications over a wireless broadband (802.11) network. The Alcatel-Lucent offer provides the components needed to establish voice communication using the Wireless Local Area Network (WLAN) infrastructure. All the features and functionality of the PCX are available on wireless handsets.

5.2.1.1.1 VoWLAN Architecture

The VoWLAN is implemented using the following components:

- **Mobile handsets**: The Alcatel-Lucent Mobile IP Touch 300/600 and Alcatel-Lucent IP Touch 310/610 WLAN Handsets are the mobile handset models available for establishing and receiving calls. They operate using the Alcatel-Lucent New Office Environment (NOE) VoIP protocol.
- **Access Points (AP)**: Access Points operate with Alcatel-Lucent WLAN Switches to provide network access for wireless clients. They act as wireless (radio) interfaces for the mobile handsets. APs must be positioned in all areas where wireless handsets are used. The number and placement of APs affects the coverage area and capacity of the wireless system. Alcatel-Lucent APs support Institute of Electrical and Electronics Engineers (IEEE) 802.11a/b/g standards for wireless systems.

  The Alcatel-Lucent IP Touch 310/610 WLAN Handsets cannot roam from one subnet to another. If routers and multiple subnets are in use, the handsets must only use APs attached to a single subnet, or be powered off and back on to switch to a different subnet.
- **WLAN Switch**: The Alcatel-Lucent OmniAccess Wireless Switch (AOS-W) acts as a wireless IP switch to provide the connection between the wired LAN and the APs.

  All Alcatel-Lucent APs are connected either directly or remotely through an IP network to a WLAN Switch. The WLAN Switch bridges wireless client traffic to and from traditional wired networks and performs high-speed Layer-2 or Layer-3 packet forwarding between Ethernet ports. While the APs provide radio services only, the WLAN Switch performs upper-layer media access control (MAC) processing, such as encryption and authentication, as well as centralized configuration and management of SSIDs and RF characteristics for the APs. This allows you to deploy APs with little or no physical change to an existing wired

infrastructure.

- **SpectraLink Voice Priority (SVP)**: SVP is a proprietary Quality of Service (QoS) mechanism that is implemented in the handsets and APs to enhance voice quality over the wireless network. SVP gives preference to voice packets over data packets on the wireless medium, increasing the probability that all voice packets are transmitted efficiently and with minimum delay. SVP is fully compatible with the IEEE 802.11 standards.

  Call Admission Control (CAC) limits the maximum number of simultaneous calls per AP. This feature guarantees good audio quality for simultaneous voice over WLAN communications in the AP.

  For installations using Alcatel-Lucent Mobile IP Touch 300/600, an **SVP Server** is required to implement SVP.

- **Security**: Security mechanisms prevent intruders external to the PCX from using WLAN services and reaching the Intranet site. The handsets support Wired Equivalent Privacy (WEP) as defined by the 802.11 specification with both 40-bit and 128-bit encryption. The handsets also support Wi-Fi Protected Access (WPA and WPA2) Pre-Shared Key (PSK).

- **DHCP server**: An internal or external DHCP server can be used to assign IP addresses.

- **TFTP server**: An internal or external TFTP server must be available on the network to load the appropriate software into the handsets.

- **Call Server**: The Call Server manages the voice signalling between wireless handsets and other sets on the Call Server, call recovery, and other telephony features.

  In addition to call management, the Call Server provides one or more configuration files via TFTP to the IP Touch WLAN Handsets at power-on. The location of the configuration files can be given to the handsets via DHCP or through static configuration using the handset's Administration menu as TFTP1 IP (primary) and TFTP2 IP (redundant).

Topologies with an SVP Server

Because of the need for centralized Call Admission Control (CAC) management in the SVP Server, any system with Alcatel-Lucent Mobile IP Touch 300/600 configured on the Call Server, must include an SVP Server. The following figure shows the voice communication flow over the VoWLAN components in a configuration with an SVP Server.

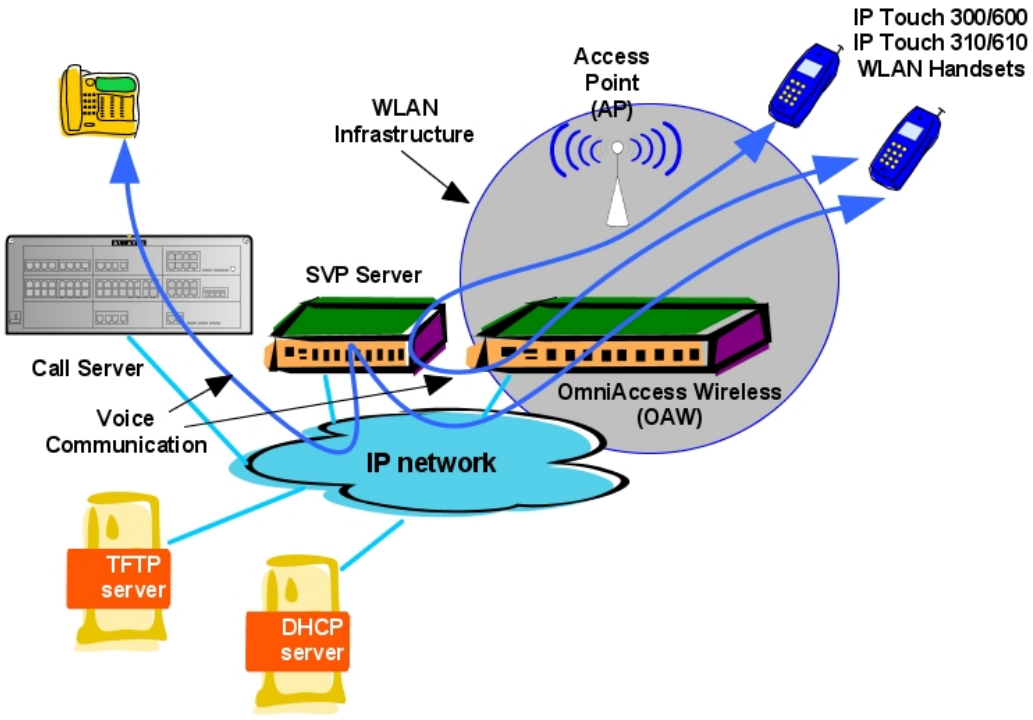


Figure 5.31 : VoWLAN voice communication flow with SVP Server

In architectures with an SVP Server, the "Cascading SVP Server" feature allows for SVP Servers to be added to increase the user capacity of the system.

Note:

The SVP Server, all WLAN handsets, and all APs must be on the same subnet.

Topologies without an SVP Server

Starting with AOS-W Release 3.1, the 310/610 handsets and the WLAN Switch support Wi-Fi MultiMedia (WMM), U-APSD, and Tspec for QoS. Therefore, the SVP Server is not needed to support the QoS.

Note:

For more information on the availability of this feature, see the AOS-W R3.1 Release Notes.

The following figure shows the voice communication flow over the VoWLAN components in a configuration using only Alcatel-Lucent IP Touch 310/610 WLAN Handsets.

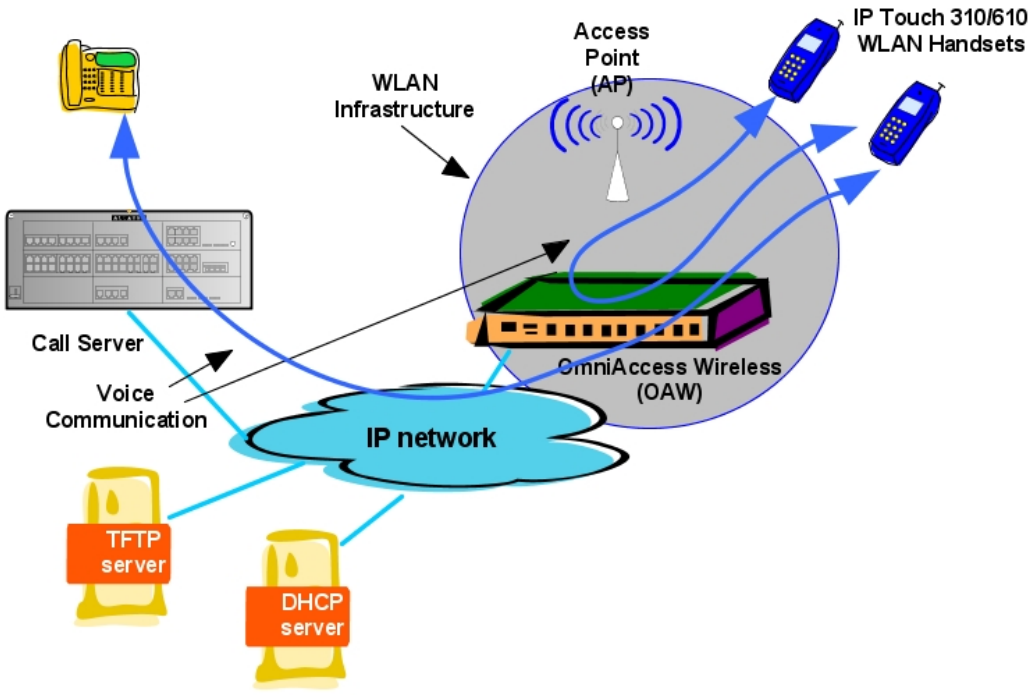


Figure 5.32 : VoWLAN voice communication flow without SVP Server

Topologies without an SVP Server have the following advantages:

- The SVP Server is a weak point because it does not support redundancy. Since the AOS-W in overlay mode supports failover, removal of the SVP Server improves the global reliability of the system.
- System administration is simplified since there is no more SVP Server administration, and there is no need to add cascaded SVP Servers for scalability.
- Deployment is easier without the SVP Server since 310/610 handsets are not required to be in the same subnet and can move between Virtual LANs and subnets on the network.
- Audio quality is improved without SVP Server delay.
- Handsets use standard QoS.
- In-call battery life is improved using U-APSD mode.

Topologies without an SVP Server have the disadvantage that existing Alcatel-Lucent Mobile IP Touch 300/600 can no longer be used and must be replaced by Alcatel-Lucent IP Touch 310/610 WLAN Handsets.

5.2.1.1.2 VoWLAN deployment overview and additional information

First, define the security mechanisms needed for your WLAN: the minimum authentication and encryption needed, VLAN, and user roles. For more information on VoWLAN security, see module Voice over Wireless LAN - Security .

Next, define the radio coverage and network capacity needed for you WLAN to determine the

number and placement of APs. For more information on determining the number and placement of APs, see:

- module Voice over Wireless LAN - Engineering Rules Overview
- module Voice over Wireless LAN - AP Placement Guidelines
- module IP Touch 310/610 WLAN Handset - Survey Mode
- module Mobile IP Touch 300/600 - Survey Mode

Run the Initial Setup of the WLAN Switch and deploy the APs. Configure the security and QoS mechanisms in the WLAN Switch. For more information on configuring the WLAN Switch:

- For AOS-W Release 3.1 and later, see module Voice over Wireless LAN - WLAN Switch Configuration with AOS-W R3.1 and Later

  For detailed information on the Initial Setup and Configuration of the WLAN Switch, see the AOS-W Quick Start Guide and the AOS-W User Guide, both located on the Business Partner Web site at http://www.businesspartner.alcatel-lucent.com.

  For information on migrating to AOS-W R3.1 from prior releases, see module Voice over Wireless LAN - AOS-W R3.1 Migration .
- For AOS-W releases prior to 3.1, see module Voice over Wireless LAN - WLAN Switch Configuration with AOS-W R2.5.x and Earlier

Configure the WLAN voice clients:

- For more information on the description, configuration and maintenance of Alcatel-Lucent IP Touch 310/610 WLAN Handsets, see:
  - module IP Touch 310/610 WLAN Handset - Description
  - module IP Touch 310/610 WLAN Handset - Configuration
  - module IP Touch 310/610 WLAN Handset - Handset Administration Tool
  - module IP Touch 310/610 WLAN Handset - Maintenance
- For more information on the description, configuration and maintenance of Alcatel-Lucent Mobile IP Touch 300/600, see:
  - module Mobile IP Touch 300/600 - Description
  - module Mobile IP Touch 300/600 - Configuration
  - module Mobile IP Touch 300/600 - Maintenance

If the network includes clients needing an SVP Server, install and configure the SVP Server. For more information, see:

- module SVP Server - Detailed description
- module SVP Server - Installation procedure
- module SVP Server - Configuration procedure

For configuration and release compatibility information specific to the PCX, see module Voice over Wireless LAN - Configuring OmniPCX Office .

5.2.1.2 Security

Security mechanisms prevent intruders external to the system from using Voice over Wireless LAN (VoWLAN) services and reaching the intranet site. You have a wide variety of options for authentication, encryption, access management, and user rights when you configure the Alcatel-Lucent OmniAccess Wireless Switch (AOS-W) and IP Touch WLAN Handsets. However, you must configure the following basic elements:

- A Service Set IDentifier (SSID) that uniquely identifies the voice WLAN
- Layer-2 authentication to protect against unauthorized access to the WLAN
- Layer-2 encryption to ensure the privacy and confidentiality of the data transmitted to and from the network
- A Virtual Local Area Network (VLAN) for the authenticated client, and starting with AOS-W R3.1, a user role

The following sections describe security mechanisms available on the WLAN.

5.2.1.2.1 SSID Control

You configure a service set identifier (SSID) on the Access Point (AP), which corresponds to a specific voice WLAN. You configure each WLAN handset with the same SSID. The handsets use the SSID to establish a wireless connection by associating with an AP. This process is called association, and uses either passive or active scanning:

- In passive scanning, the APs send out beacons that contain the SSID of the specific WLAN. The handset passively scans the radio channels for beacons and selects an AP. The handset keeps on scanning even after association is made, in order to support roaming.
- In active scanning, the handsets send out probe requests containing the SSID. Only the APs with the correct SSID respond.

5.2.1.2.2 MAC Filtering

You can configure APs to allow or deny association of a handset based on the handset's MAC address. With this method, only handsets with MAC addresses recognized by the AP can connect.

5.2.1.2.3 WEP

When you enable WEP (Wired Equivalent Privacy) mode in the IP Touch WLAN handset, a secret key is shared between the WLAN Switch and the handset. The key is 40 or 128 bits long (128 bits recommended). The key is used for authentication and encryption.

Authentication

When authentication is enabled, the shared key is checked. The WLAN Switch challenges the handset. The handset must encode the challenge with the shared key and return the result to the WLAN Switch. The WLAN Switch checks the result and authorizes or bars connection accordingly.

When authentication is disabled, the shared key is not controlled. This mode is called Open System Authentication.

Open System Authentication is recommended. The WLAN Switch sends a challenge to the handset in both unencrypted and encrypted messages. An intruder can intercept messages and the key can be broken. As the key is the same for data encryption, WEP authentication can be seen as a disadvantage.

Data Encryption

When encryption is enabled, data exchanged between the AP and the handset is encrypted according to the standard RC4 algorithm. The encryption uses the shared key.

5.2.1.2.4 WPA/PSK

As of AOS-W R1.1, the WPA/PSK (Wi-Fi Protected Access/Pre Shared Key) is introduced to improve intrusion security.

When WPA/PSK mode is enabled, a secret passphrase (password with several words) is shared between the WLAN Switch and the handsets.

Communications between the WLAN Switch and a handset are authenticated and encrypted with a temporary key.

This temporary key is built from:

- The shared passphrase
- The MAC address of the handset
- 2 random texts

The temporary key is changed at regular intervals and is deleted at the end of the session.

The encryption is performed according to the RC4 standard.

Packets are numbered to avoid additional malicious data.

Data completeness is checked according to the Message Integrity Check standard.

5.2.1.2.5 WPA2/PSK

As of AOS-W R2.0, WPA2/PSK security protocol can be used.

WPA2/PSK provides the same features as the WPA/PSK security protocol, but the WPA2/PSK security protocol uses the AES (Advanced Encryption Standard) encryption algorithm, more robust than the RC4 (Rivest encryption Ciphers 4) encryption algorithm (used in WPA/PSK).

5.2.1.2.6 VLANs

VLANs are used to segregate communication into different security classes, and to isolate voice communication from data communication. Each authenticated client is placed into a VLAN, which determines the client's DHCP server, IP address, and Layer-2 connection. While you could place all authenticated wireless clients into a single VLAN, the WLAN Switch allows you to group wireless clients into separate VLANs. This enables you to differentiate groups of wireless clients and their access to network resources. For example, you can place authorized employee clients into one VLAN and itinerant clients, such as contractors or guests, into a separate VLAN. You create the VLANs for wireless clients only on the WLAN Switch. You do not need to create the VLANs anywhere else on your network.

5.2.1.2.7 ACL

The ACL (Access Control List) service filters IP addresses according to filtering rules. A filtering rule defines the source IP address, authorized destination IP address and the protocols allowed.

Typically, the system administrator allows for voice communication between the handsets and the SVP Server, and between the handsets and the TFTP server.

The ACL filtering rules are defined for one VLAN. The system administrator can define different rules for voice communications and for data communications.

5.2.1.2.8 User Roles

Starting with AOS-W R3.1, every WLAN client is associated with a user role, which determines what a client is allowed to do, where and when it can operate, how often it must

re-authenticate, and which bandwidth contracts are applicable. The WLAN security level for the IP Touch WLAN handsets (WEP, WPA/PSK, WPA2/PSK) is the same as for configurations using previous versions of AOS-W.

A policy identifies a set of rules that applies to traffic that passes through the WLAN Switch. A policy can consist of firewall rules that permit or deny traffic, quality of service (QoS) actions such as setting a data packet to high priority, or administrative actions such as logging.

Whenever you create a user role, you specify one or more policies for the role.

Note:

User roles and policies require the installation of a Policy Enforcement Firewall licence in the WLAN Switch.

Prior to AOS-W R3.1 in topologies with an SVP Server, the WLAN system offered strong VoWLAN security by filtering Spectralink Radio Protocol (SRP) in the WLAN Switch for the defined voice SSID. SRP encapsulates the Alcatel-Lucent New Office Environment (NOE) protocol.

In topologies without an SVP server, SRP is replaced by the NOE Aware feature implemented in the WLAN Switch. The NOE Aware feature supports:

- a NOE Firewall for security purposes
- NOE Aware monitoring/scanning, allowing simultaneous air monitoring (ARM) and NOE voice traffic

5.2.1.2.9 Blacklist

When a client is blacklisted, the client is not allowed to associate with any AP in the network for a specified amount of time. A blacklisted client is defined by its MAC address. If a client is connected to the network when it is blacklisted, a deauthentication message is sent to force the client to disconnect. While blacklisted, the client cannot associate with another SSID in the network.

The system administrator can remove a client from the blacklist.

5.2.1.3 Engineering Rules Overview

This chapter is intended to help determine the number of Access Points (APs) to deploy depending on customer's needs and building types. A critical objective is to maintain voice quality, reliability, and functionality for wireless users similar to what they expect from their wired business telephones. The required number and placement of APs in a given environment is driven by several factors. This chapter discusses radio standard, coverage area, and network capacity. Where to place APs is driven by AP type, power output, and the physical environment. For more information about AP placement, see module Voice over Wireless LAN - AP Placement Guidelines .

The goal of this document is to help define customer requirements in order to optimize the Alcatel-Lucent offer and identify possible commercial or technical risks. Alcatel-Lucent recommends performing a site survey of the deployment site to optimize the installation.

5.2.1.3.1 Determining Deployment Requirements

Radio standard

To provide reliable service, wireless networks should be engineered to deliver adequate signal strength in all areas where the wireless telephones will be used. The required minimum signal strength for Alcatel-Lucent IP Touch WLAN handsets depends on the 802.11 frequency band

and modulation used, and the data rates enabled on the AP. Recommended signal strength characteristics are summarized in the following table.

802.11 Radio Standard	Enabled Data Rates (Mb/s)	Recomended Minimum Signal Strength
802.11b	11, 5.5, 2. 1	-70dBm
	11 only	-60dBm
802.11g	54, 48, 36, 24, 18, 12, 9, 6, 11, 5.5, 2, 1	-60dBm
	54 only	-45dBm
802.11a	54, 48, 36, 24, 18, 12, 9, 6	-60dBm
	54 only	-45dBm

The pros and cons to be considered in the deployment of each frequency band are summarized in the following table.

Radio Standard	Pros	Cons
802.11a/b/g	Highest capacity option: voice and data use separated bands. Highest performance option (54 Mbps for data).	Increase in the Access Point and clients wireless adaptors cost.
802.11 b/g only	Supports legacy clients Lowest cost Alcatel-Lucent Access Point.	802.11g networks that also support 802.11b-only clients must run in protected mode to enable backward compatibility, which reduces overall throughput. When Alcatel-Lucent IP Touch 310/610 WLAN Handsets are installed on a mixed 802.11b/g network which is running in protected mode, the handsets must be set to 802.11b mode. Does not support 802.11a-only clients.
802.11a only	High performance. High Capacity. Up to 23 channels available, which provides for the potential for higher AP density.	Does not support legacy clients (Alcatel-Lucent Mobile IP Touch 300/600). Higher radio frequency signals used by 802.11a band do not propagate as well through air or obstacles. More APs are required to provide the same level of coverage as 802.11b/g.

Coverage Area Requirements

For voice applications, customers typically want seamless, full radio frequency coverage.

An enterprise Wi-Fi network laid out for data applications may not provide adequate coverage for a wireless telephony application. Such networks may be designed to only cover areas where data terminals are used and may not include coverage in other areas such as stairwells, break rooms or building entrances – all places where telephone conversations are likely to

occur.

The overall quality of coverage is also more important with telephony applications. In areas of poor wireless coverage, the performance of data applications may be acceptable due to retransmission of data packets, but for real-time voice quality this will not be acceptable.

Another factor to consider when determining the coverage area is the device usage. Telephone users tend to walk as they talk, while data users are usually stationary or periodically nomadic. Wireless telephones are typically held very close to the user's body, introducing additional radio signal attenuation. The wireless LAN layout should account for some reduction of radio signal propagation.

Coverage holes are areas where clients cannot receive a signal from the wireless network. When deploying wireless networks, there is a trade-off between the cost of the initial network deployment and the percentage of coverage hole areas. An acceptable percentage of coverage holes is determined by the customer (typically 0-10%). Areas such as stairways, bathrooms, lifts, cafeterias, and basements may require special consideration and additional APs.

Building Type

Identifying the building type and its RF characteristics is critical in determining how many APs will be needed. The following table shows some basic building types that are common in the enterprise market. If the building does not fall into one of these categories then some amount of professional assistance may be needed.

Building Type	**Description**
Typical Office Space	This is the most common enterprise building. This type of building consists of large open cubicle areas with walled offices and conference rooms.
Drywall Office Space	This type of building consists of mostly offices with dry wall characteristics.
Brick/Concrete Walled Office Space	This type of building consists of concrete or brick walls for both exterior and for interior office space. Old buildings found on college campuses are good examples of this type of building.
Hospital	-
Warehouse/ Manufacturing with no obstacles, or metallic separations	This type of building consists of large areas with high ceilings
difficult environment	There are some buildings such as sports arenas, stock exchanges, warehouses or manufacturing plants with large metallic parts, clean rooms that do not fit into one of the typical categories. **No tests have been carried out in these environments yet**. These buildings typically require some special consideration or professional service.

Homogeneity

Building Homogeneity

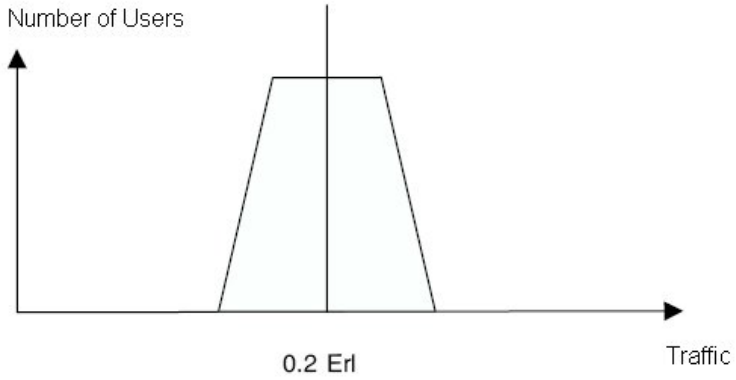
If the building does not have similar radio frequency (RF) characteristics throughout the coverage area, the coverage area needs to be divided into areas with similar characteristics and the design process repeated for each area.

User distribution

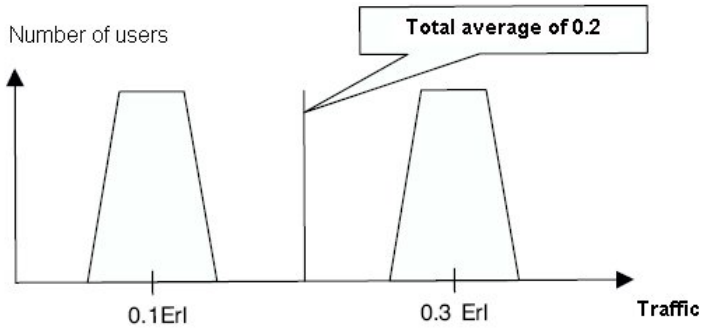
Determine if the distribution of the users is homogeneous in terms of mobility and traffic (voice versus data). Depending on the type of activities, there may be a need to define different geographic zones taking into account user diversity.

One example of very different distribution is shown in the next two figures:

- Homogeneous distribution
  Population of users well distributed with a majority centred on the mean value.



- Non homogeneous distribution
  Company made of different departments with various needs in terms of traffic. Two cases can be seen:
- Different kinds of users in the same area
- Different kinds of users in separated areas
  In each of these cases, the capacity is variable, so the number of necessary APs is different.



Classification into Zones

A zone is an area in which the customer's objectives in terms of percentage of coverage holes, traffic distribution (voice and data) and radio coverage are homogeneous. Each site should be divided into zones and the design process repeated for each zone to get an optimized result.

Network capacity

Although coverage area is the primary factor, network capacity requirements factor into the number of APs required. Data traffic is very bursty and sporadic, but data applications can tolerate network congestion with reduced throughput and slower response times. On the other hand, voice traffic requires that the bandwidth be constant and consistent for every phone call, and cannot tolerate unpredictable delays. Voice traffic can be predicted using probabilistic usage models, allowing a network to be designed with high confidence in meeting anticipated voice capacity requirements.

Beyond the normal IP telephony design guidelines, there are several additional considerations that need to be addressed for Wi-Fi telephony with Alcatel-Lucent IP Touch WLAN Handsets.

Access Point Bandwidth Considerations for Voice Application

There are several factors that determine the AP bandwidth use during a telephone call. The first is the VoIP protocol and its characteristics. The type of codec used combined with the packet rate will determine the size of the voice packets, along with any additional overhead information required for the protocol.

The payload information makes up a little more than half of a typical voice packet, with 802.11 and IP protocol overhead filling the rest. The 802.11 protocols include timing gaps for collision avoidance, which means bandwidth utilization is more accurately quantified as a percentage rather than actual data throughput.

The percentage of bandwidth used increases for lower data rates, but it is not a linear function because of the bandwidth consumed by the timing gaps and overhead. For example, a call using standard 64kb/s voice encoding (G.711) uses about 4.5% of the AP bandwidth at 11 Mb/s, and about 12% at 2 Mb/s. In this example, four simultaneous calls on an AP would consume about 18% of the available bandwidth at 11 Mb/s or about 48% at 2 Mb/s.

The maximum number of simultaneous telephone calls an AP can support is determined by dividing the total available bandwidth by the percentage of bandwidth used for each individual call. Approximately 20-40% of the AP bandwidth is reserved for channel negotiation and association algorithms, so 60-80% of the total available bandwidth should be used for calculating the maximum call capacity per AP.

As a general rule based on lab tests and experience, wireless LAN designs for **Alcatel-Lucent IP Touch WLAN handsets should consider no more than 12 simultaneous calls per AP at 11 Mb/s.**

To allow for bandwidth to be available for data traffic, Alcatel-Lucent provides the ability to limit the number of calls per access point within the SVP Server. The "Calls per Access Point" setting will limit the number of active wireless telephone calls on each AP. Wireless Telephones are free to associate with other APs within range that have not reached the set maximum number of calls. Alcatel-Lucent recommends this setting be equal to or below the maximum number of calls discussed in the previous paragraph.

In topologies without an SVP Server, Call Addmission Control (CAC) can be configured on the WLAN Switch to prevent any single AP from becoming congested with voice calls.

Push to Talk

The Alcatel-Lucent Mobile IP Touch 600 and Alcatel-Lucent IP Touch 610 WLAN Handset offer Push-to-talk (PTT) functionality. Because the PTT mode uses IP multicasting, all APs on the subnet will transmit a PTT broadcast. This can be limited to only the APs that are handling one or more PTT-enabled handsets by enabling the Internet Group Management Protocol (IGMP) on the wired infrastructure network.

Telephone Usage

Because the data rate and the packet rate are constant, Wi-Fi telephony calls may be modelled in a manner very similar to circuit-switched calls. Telephone users (whether wired or wireless) generally tend to make calls at random times and of random durations. Because of this, mathematical models can be applied to calculate the probability of calls being blocked based on the number of call resources available. Telephone usage is measured in units of Erlangs. One Erlang is equivalent to the traffic generated by a single telephone call that lasts for one hour. A typical office telephone user will generate 0.10 to 0.2 Erlangs of usage, which equates to six to twelve minutes on the telephone during a one-hour period. Heavy telephone users may generate 0.20 to 0.30 Erlangs, or 12 to 18 minutes of phone usage in an hour.

The following ranges can help to estimate network size when the actual voice traffic levels are unknown.

- Very heavy traffic: call centre, telesales, stock exchanges (>0.3Erl)
- Heavy traffic: sales, purchasing (0.3Erl>>0.2Erl)
- Moderate traffic : technical, accounting, business (0.2Erl>>0.1Erl)
- Light traffic: warehouse, manufacturing, labs (<0.1Erl)

Note 1:
If different kinds of users share the same geographical area, traffic analysis is based on the aggregate traffic for all users. So, users with higher or lower usage are averaged out. Another point to take into account is to determine if users will have only a wireless phone or if they will keep a wired line, which means that the wireless phone traffic is lower.

The traffic engineering decision is a trade-off between additional call resources and an increased probability of call blocking. Call blocking is the failure of calls due to an insufficient number of call resources being available. Typical systems are designed to a blocking level (or grade of service) of 0.1% to 2% at the busiest times. Traffic model equations use the aggregate traffic load, number of users, and number of call resources to determine the blocking probability. The blocking probability can also be used along with the aggregate traffic load to determine the number of call resources required. Traffic model equations and calculators are available at www.erlang.com.

The following table shows maximum users per AP, based on the AP's ability to handle simultaneous calls:

User calling intensity	light	moderate	heavy	Very heavy	light	moderate	heavy	Very heavy
Erlangs per user	0,1	0,15	0,2	0,3	0,1	0,15	0,2	0,3
Max active calls per AP	Users supported per AP (1% blocking)				Users supported per AP (0,1% blocking)			
1	1	1	1	1	1	1	1	1
2	2	2	2	2	2	2	2	2

3	4	3	3	3	3	3	3	3
4	8	6	4	4	4	4	4	4
5	13	9	7	5	7	5	5	5
6	19	13	10	6	11	7	6	6
7	25	17	13	8	15	10	7	7
8	31	21	16	10	20	13	10	8
9	37	25	19	12	25	17	12	9
10	44	30	22	14	30	20	15	10
11	51	34	26	17	36	24	18	12
12	58	39	29	19	42	28	21	14

Consider a system with APs that can support six active telephone calls. If a blocking probability of 1% or less is desired, each AP can support about 13 moderate wireless telephones users. If the AP coverage can support 12 simultaneous calls per AP, each AP can support about 39 moderate users, if users use a wired line for 50% of their calls and their wireless telephone for the other 50% then each AP can support 78 moderate users.

Note 2:

These calculations give the number of APs needed to cover capacity for voice applications only.

5.2.1.3.2 Determining the Number of APs

Depending on the customer's deployment requirements, there are three strategies for designing and deploying an Alcatel-Lucent wireless network. The following table provides guidelines for choosing the appropriate strategy.

Deployment Option	**Deployment Requirements**
Professional Site Survey	This option should be considered when: • Deployments require full coverage with close to 0% coverage holes. • The RF characteristics of the building vary throughout the coverage area. • The building type is classified as difficult environment as defined in part 4.2.3 of this document • The cost or logistics of running Ethernet cables is prohibitive.
RF Prediction with minimal Site Survey	This option should be considered when: • The RF characteristics of the building vary throughout the coverage area. • The building type is not typical (e.g. Arena, Convention Centre, Stock Exchange). • A Professional Site Survey is too costly, and a graphical coverage plot is desired before deployment.

Basic Guidelines with minimal Site Survey	This option is suitable when: • The RF Characteristics are homogenous throughout the coverage area. • The building type can be easily classified.

Professional Site Survey

Generally, the professional site survey involves temporarily placing one or more APs and then measuring the resulting coverage(s). Based on the results of these measurements, APs are relocated and/or reoriented to achieve complete coverage of the target space without unnecessary coverage overlap or coverage holes between APs. This approach is appropriate given the following deployment requirements:

• Full Coverage with 0% coverage holes

• The RF characteristics of the building vary throughout the coverage area

• The building is classified as difficult environment

During the professional site survey, one or two APs are placed at or near one end of a building. Their coverage is measured and the APs are relocated and reoriented as necessary to ensure that this end of the building is completely covered. When measurements confirm that this is true, a second or third AP is added so its coverage area somewhat overlaps the coverage area of the first AP(s). (Generally, 10 to 15 percent coverage overlap is considered appropriate). Its coverage is measured to ensure that its overlap with the first AP(s) is appropriate and to determine the coverage in the rest of the building. This process continues, adding a third or fourth AP and so on. This process continues until all areas of the building are covered.

The professional site survey allows the designer to provide full seamless coverage.

Other variables designers may include are static transmit power level, geometric pattern used for AP placement, and the antenna type (omnidirectional, wide beam directional, or narrow-beam directional). Some designers like to have the flexibility to select antenna types most suited to specific buildings. Designers may differ in the criteria they use to determine coverage area. Some prefer to use signal strength (RSSI), some prefer signal-to-noise ratio (SNR), and others prefer to use some indication of throughput, such as packet retry rate.

These measurements are normally made using site survey software provided by a wireless LAN manufacturer, running on a PC or PDA such as the Alcatel-Lucent Site Survey tool. They may also be made using one of the handheld measurement tools currently available, such as Air Magnet or Berkeley Varitronics. The measurement tools are usually selected on their ability to measure the desired variable, RSSI, SNR, or packet retry rates.

RF Prediction with Minimal Site Survey

RF prediction consists of importing the floor plans of the coverage area into a Computer Aided Design system in which a user can place APs, draw in the walls of the building and assign RF characteristics to the walls. Depending on the confidence level of the estimates made for the building RF characteristics and the cost of filling in potential coverage holes after deployment, an optional site survey may be appropriate to verify assumptions.

This approach is appropriate given the following deployment requirements:

• Full Coverage with 2 to 10% coverage holes

• The RF characteristics of the building vary throughout the coverage area

• The building is classified as difficult environment

• A professional site survey is too costly, and a graphical coverage plot is desired before deployment.

Basic Guidelines with Minimal Site Survey

The Basic Guideline approach is based on empirical data from existing wireless deployments and is adequate for most deployments. This approach is based on most enterprise buildings having common RF characteristics, and that only a part of the building needs to be characterized to verify the AP coverage for the entire building. This approach leverages the algorithms built into the Alcatel-Lucent AireWave Director Software that ensure that the overlap between APs is minimized and that coverage holes are detected and eliminated before clients find them. When deploying 802.11 wireless LANs to support Voice over IP (VoIP) telephones, a few special considerations are needed in the deployment process. When deploying an 802.11 voice system with the Alcatel-Lucent IP Touch WLAN handsets, a coverage of at least –70dBm in 802.11b band is needed.

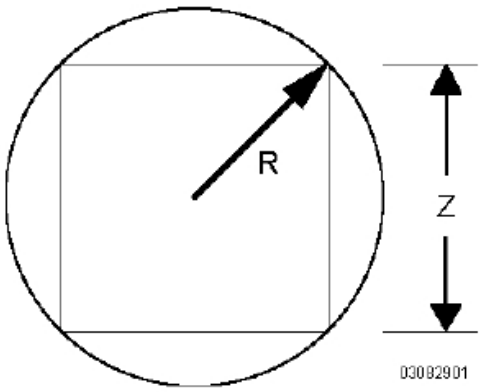
Areas such as stairways, bathrooms, cafeterias and outside areas may require special consideration and APs. These are areas that are not typically critical for data users but are critical coverage areas for voice users who want seamless coverage. Refer to the Sample Basic Guidelines Process for an example of the Basic Guidelines approach.

5.2.1.3.3 Sample Basic Guidelines Process

Use the table below to determine the coverage area of an AP based on the building type and desired average user performance.

Determine Radius and Z Factor

The Z factor represents the length of a square that corresponds to the coverage area of the AP.



The following table includes building types, and shows the coverage area measurements for a coverage at –70 dBm for the WLAN handsets and for data on 802.11a band. **These values are based on empirical data and can vary from one site to the other and depending on the WLAN card** used for data. A WLAN adaptor D-link Air Xpert DWL-AG650 802.11 triband has been used for these measurements.

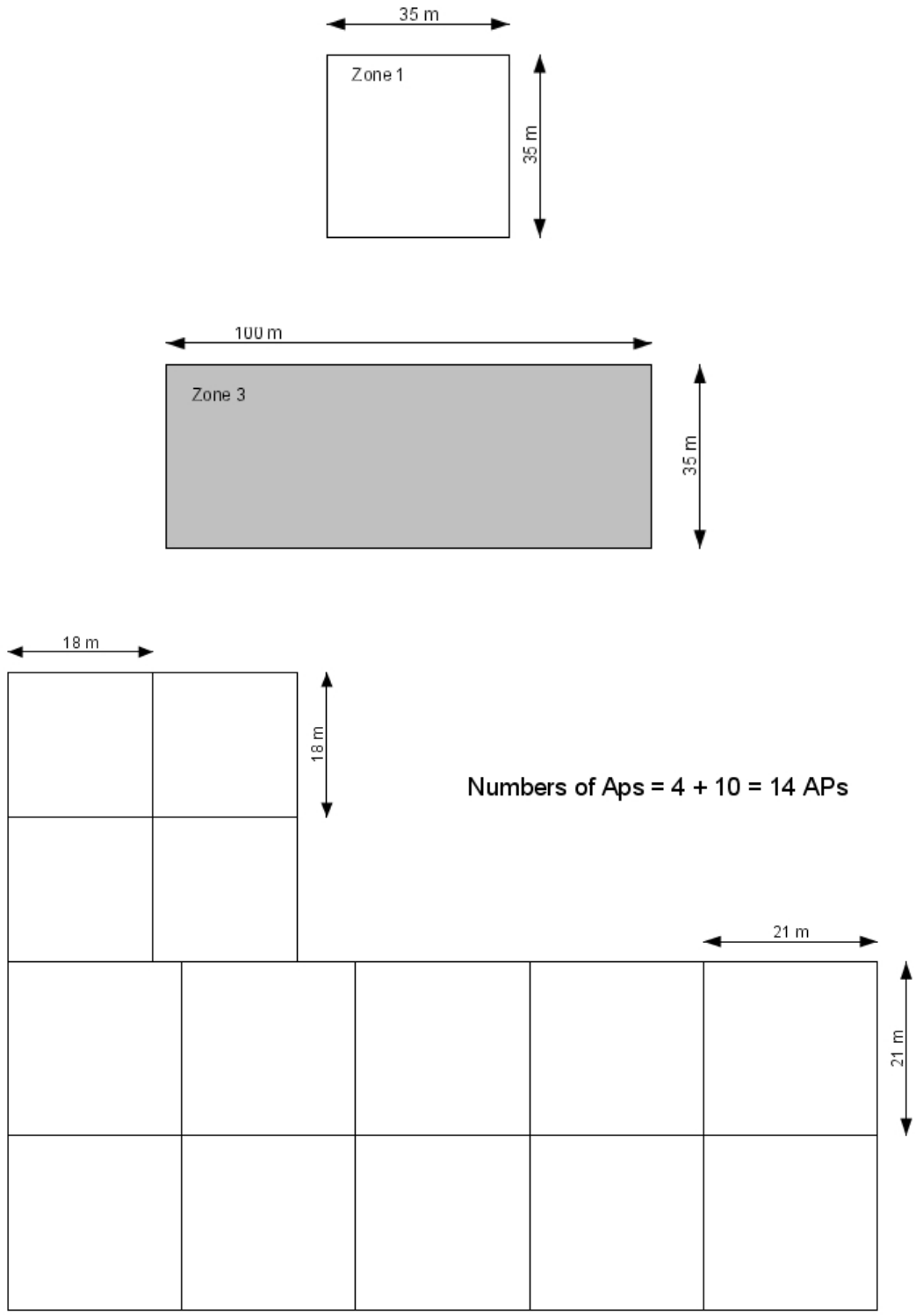
Building Type	Measurement	802.11b/g: coverage at –70dBm for the phones = -65 dBm for data (note 1)	802.11a: average user throughput of 15Mbps	802.11a: average user throughput of 18Mbps
Typical Office	A (m 2)	450	450	324
	R (m)	15	15	13
	Z (m)	21	21	18
Drywall Office Space	A (m 2)	324	324	289
	R (m)	13	13	12
	Z (m)	18	18	17
Brick Wall Office Space	A (m 2)	288	288	N/A
	R (m)	12	12	-
	Z (m)	17	17	-
Hospital	A (m 2)	324	324	289
	R (m)	13	13	12
	Z (m)	18	18	17
Warehouse/ Manufacturing with no obstacles, metallic separations	A (m 2)	450	450	324
	R (m)	15	15	13
	Z (m)	21	21	18

Note:
Measurements have been done with the Alcatel-Lucent site survey tool and a WLAN adaptor D-link Air Xpert DWL-AG650 802.11 triband, a survey at –65 dBm in 802.11b band will ensure a coverage at –70 dBm for the telephones. A margin of 5 dB is taken to account for differences in the WLAN adaptor and telephones receivers.

Determine How Many APs are Needed

In this step you define the coverage area for each floor in the building in zones and divide it into squares of areas equal to the Z factor squared corresponding to the building type (see previous table) and calculate how many APs are needed. The centre of each square indicates the approximate location of the APs.

This example is for a floor composed of a drywall office space (zone 1) and a typical office area (zone 2). The application is voice on 802.11b and data on 802.11a with an average user throughput of 15Mbps.


35 m
Zone 1
35 m
100 m
Zone 3
35 m
18 m
18 m
Numbers of Aps = 4 + 10 = 14 APs
21 m
21 m

Minimal Site Survey

For information on running site survey mode:

- For Alcatel-Lucent Mobile IP Touch 300/600, see module Mobile IP Touch 300/600 - Survey Mode
- For Alcatel-Lucent IP Touch 310/610 WLAN Handsets, see module IP Touch 310/610 WLAN Handset - Survey Mode

5.2.1.4 AP Placement Guidelines

This chapter describes where and how to place Access Points (APs).

5.2.1.4.1 Requisites

Collect building maps or floor plans of the areas to be covered, with a feet or meters scale included.

Note any deployment constraints, for example:

- If the APs are to use existing wiring, note these locations on the map.
- If there are locations where APs cannot be placed, note these locations on the map.
- All possible interferers (for example other WLAN devices, Bluetooth devices, microwave ovens) and plan AP locations accordingly (see § Interferers).

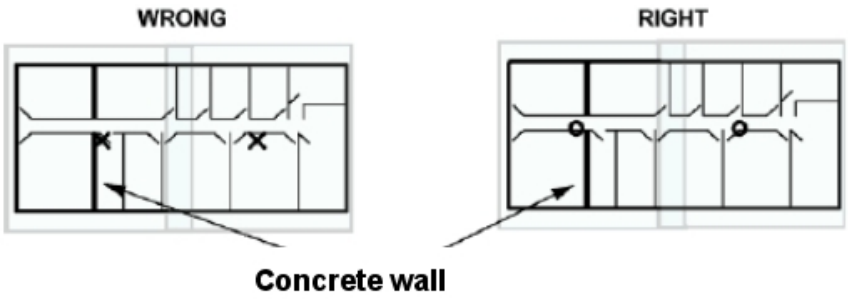
5.2.1.4.2 Access Point Placement Guidelines

General recommendations

- Position the APs above obstructions.
- Position the APs vertically near the ceiling in the centre of each coverage area, if possible. APs are designed to be installed vertically, either standing up in a plenum or hanging from a ceiling, to create the largest coverage area per AP. Hanging the AP from the ceiling provides the best coverage.
- Position APs in locations where users are expected to be. For example, large rooms are typically a better location for APs than a hallway.
- Place APs no more than 40 meters apart from each other. Placing APs further apart almost always results in poor coverage.
- Do not mount APs outside buildings.
- Do not mount APs on building perimeter walls unless the operator wants to provide coverage outside the building.
- **Important:** Do not mount AP antennas within one meter (3 feet) of any metal obstructions. The radio frequency waves from the APs are blocked and/or reflected by metal objects, such as ducts, conduit, pipes, bookcases, elevator shafts, stairwells, and walls.

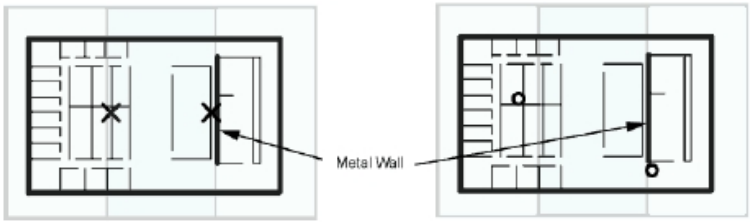
Three sample solutions to AP placement problems

In the first example, there is a large concrete wall in the middle of one coverage area.



The figure on the left shows a poor installation of two APs indicated with an X. The figure on the right shows a better solution. Both APs are mounted in hallways. The leftmost AP is moved to other side of wall to provide coverage on left side of the wall and the rightmost AP is moved slightly left to provide better coverage to overlap area.

In the second example, there is a large metal wall next to a planned location.



The figure on the left shows a poor installation of two APs indicated with an X. The figure on the right shows a better solution. The rightmost AP is moved to the hallway slightly to the right of one end of the metal wall. The leftmost AP is moved up and to the left to provide better coverage to overlap area.

In the third example, the AP needs to be mounted in a right angle corner of a hallway.

In the right angle corner of a hallway, mount the AP at a 45 degree angle to the two hallways as shown in the figure on the right. The Alcatel-Lucent AP internal antennas are not omnidirectional, and will cover a larger area if mounted this way.

Interferers

802.11b/g standards share the unlicenced Industrial, Scientific and Medical (ISM) band (2.4GHz) with a number of other wireless technologies. Bluetooth devices and microwave ovens are the most common ones and can be found on a site where WLAN will be deployed. AP placement should be chosen in order to minimize interferences on the WLAN system's performance. Interferences by WLAN on other technologies is not discussed, except cohabitation with DECT APs. For more information, see § Cohabitation with DECT APs .

Cohabitation with Bluetooth Devices

Bluetooth technology is based on frequency hopping over 79 channels in the 2400 to 2483.5MHz band.

There are 3 power classes

- Power class 1: max transmit power: +20dBm (range 100m)
  - Voice application: do not mount an Alcatel-Lucent AP within 10 meters of a power class 1 Bluetooth AP. The number of maximum simultaneous calls on WLAN AP can decrease significantly if a Bluetooth AP class 1 emits within 10 meters.
  - 802b/g data application: for maximum throughput, do not mount an Alcatel-Lucent AP within 10 meters of a power class 1 Bluetooth AP.
    802.11b/g data throughput is reduced when a user within 10 meters from a class 1 Bluetooth device in use. To ensure 80% of the maximum data throughput, users should be at least 10 meters away from a Bluetooth class 1 device.
- Power class 2: maximum transmit power: +4dBm (range 10m)
  - Voice application: do not mount an Alcatel-Lucent AP within 1 meter of a power class 2 Bluetooth AP. WLAN handset users can experience cuts in the audio when placed less than 1 meter from a Bluetooth class 2 device in use. Cuts are less than 1 second long and can appear in bursts. General audio quality is minimally impacted.
  - 802b/g Data application: for maximum throughput, do not mount an Alcatel-Lucent AP within 10 meters of a power class 2 Bluetooth AP.
    802.11b/g data throughput is reduced when a user is within 10 meters from a class 2 Bluetooth device in use. To ensure 80% of the maximum data throughput, users should be at least 3 meters away from a Bluetooth class 2 device.
- Power class 3: max transmit power: 0dBm (range 10cm)
  Not tested, interferences should be minimal on WLAN.

Cohabitation with Microwave Ovens

Microwave ovens emit signals in the ISM band. Depending on how well the oven is shielded, emissions can disturb WLAN applications. To reduce interference from microwave ovens, check the label on the microwave which should provide the central operating frequency. Most microwave ovens operate at a central frequency of 2.45 GHz, Emissions occur in a large band, so typically disturb channels 6 to 11. In this case, an AP close to a microwave oven should be set to channel 1.

Cohabitation with other WLAN APs

Adjacent APs need to use different radio channels to prevent interference between them. See § Channel and transmission power considerations .

Cohabitation with DECT APs

Place WLAN APs at least 3.5 meters from DECT APs in order not to disturb DECT communications.

5.2.1.4.3 Channel and transmission power considerations

Adjacent APs need to use different radio channels to prevent interference between them. The 802.11b/g standard used by Alcatel-Lucent IP Touch WLAN Handsets provides for three non-interfering channels: channels 1, 6, and 11. APs within range of each other should always be set to non-interfering channels to maximize the capacity and performance of the wireless

infrastructure, as shown in the diagram below.

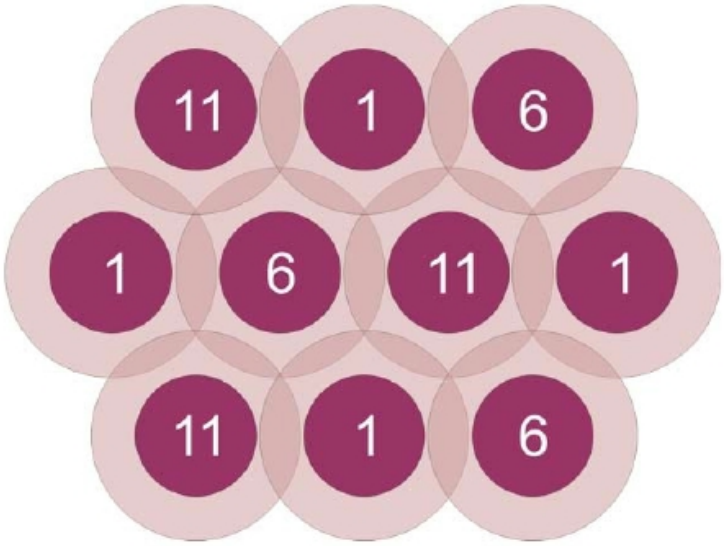


Figure 5.42 : 802.11b/g Non-interfering channels with overlaping cell coverage

If adjacent APs are set to the same channel, or use channels with overlapping frequency bands, the resulting interference will cause a significant reduction in the network performance and throughput, and will degrade overall voice quality.

In an 802.11a deployment, all 23 channels are considered non-overlapping, since there is 20MHz of separation between the centre frequencies of each channel. However, since there is some frequency overlap on adjacent 802.11a channel sidebands, there should always be at least one cell separating adjacent channels and two cells separating the same channel, as shown in the diagram below.

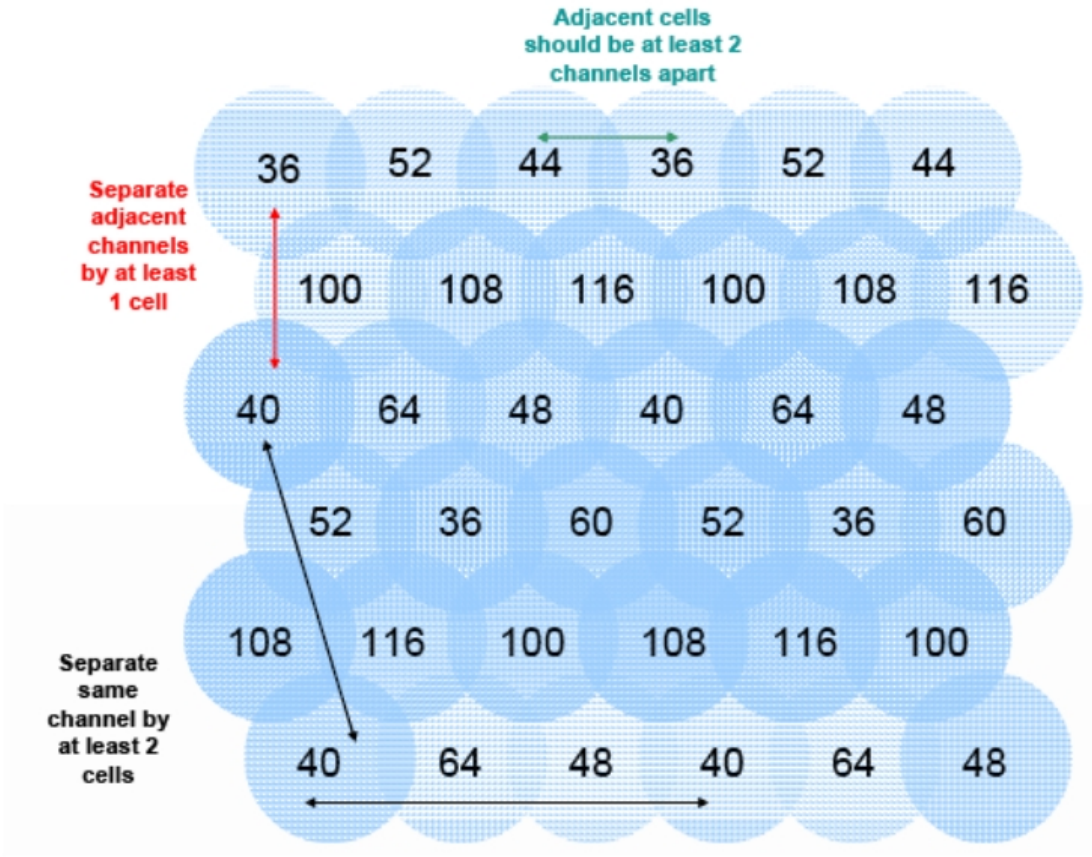


Figure 5.43 : 802.11a Non-interfering channels with overlapping cell coverage

For voice only applications: do not use the same channel for APs placed less than 3.5 meters from each other. This distance assumes that the AP's transmit power is 100mW. For an interfering AP emitting at a different power level, the rule is, the interferer has to be at such a distance that it should not been seen by the system at more than –40dBm.

For voice and data applications in 802.11b/g band: do not use the same channel for APs placed less than 12 meters from each other. This distance assumes that the AP's transmit power is 100mW. For an interfering AP emitting at a different power level, the rule is, the interferer has to be at such a distance that it should not been seen by the system at more than –47dBm.

The transmission power of APs can be increased or decreased to provide more or less AP coverage area. Generally, the transmission power setting should be the same for all APs in a facility. This minimizes the chance of higher-power APs interfering with nearby lower-power APs and provides consistent coverage.

It is recommended to set AP power output to 100 mW. If this cannot be accommodated, use a 50 mW setting or a minimum of 30 mW. With lower power output settings, special attention must be made to AP placement to ensure there are no frequency re-use issues. Regardless of the selected power level settings, all APs and handsets must be configured with the same

settings to avoid channel conflicts and unwanted cross-channel interference.

In mixed 802.11b/g environments, set the power of the 802.11b and 802.11g radios to the same setting, if they are separately configurable. For example, set both radio to 30mW to ensure identical coverage on both radios. For mixed 802.11a/b/g environments, where the AP uses all three radios types, AP placement should first be determined by modelling for the characteristics of 802.11a, since this environment will typically have the shortest range. Then, the transmission power of the 802.11b and 802.11g radios should be adjusted to provide the required coverage levels for those networks, within the already established AP locations.

Where possible, all APs should be set to the same transmission power level within a given radio type. For example, set all 802.11a radios to 50 mW and set all 802.11b and 802.11g radios to 30 mW. It is crucial to then set the transmission power of the handset to match the transmission power of the APs. This will ensure a symmetrical communication link. Mismatched transmission power outputs will result in reduced range, poor handoff, one-way audio and other QoS issues.

5.2.1.5 WLAN Switch Configuration with AOS-W R3.1 and Later

This chapter guides you in the configuration of the Alcatel-Lucent OmniAccess Wireless Switch (AOS-W) for AOS-W releases starting from Release 3.1, which support Alcatel-Lucent IP Touch 310/610 WLAN Handsets. For information on the procedure to configure the WLAN Switch for AOS-W releases prior to Release 3.1, see module Voice over Wireless LAN - WLAN Switch Configuration with AOS-W R2.5.x and Earlier . For information on migrating to AOS-W R3.1, see module Voice over Wireless LAN - AOS-W R3.1 Migration .

This chapter is intended as a high-level configuration guide. Configuration procedures are shown using the Web User Interface (WebUI). The WebUI allows you to configure and manage the WLAN Switch through a standard Web browser from a remote management console or workstation. For detailed information on the installation and configuration of the WLAN Switch, see the AOS-W Quick Start Guide and the AOS-W User Guide, both located on the Business Partner Web site at http://www.businesspartner.alcatel-lucent.com.

With the AOS-W R3.1, a new Voice Services Module licence appears and includes voice features which were present in the Policy Enforcement Firewall (PEF) licence. The Voice Services Module is necessary for topologies without an SVP Server. For more information on the Voice Services Module licence, see the AOS-W User Guide.

5.2.1.5.1 Configuration overview

This guide assumes a simple deployment scenario, shown in the following figure. The WLAN switch and the Access Points (APs) are on the same subnetwork. The APs can be physically connected directly the WLAN switch. The uplink port on the WLAN Switch is connected to a router. The router acts as the default gateway for the WLAN switch and clients. All voice clients belong to the same VLAN.

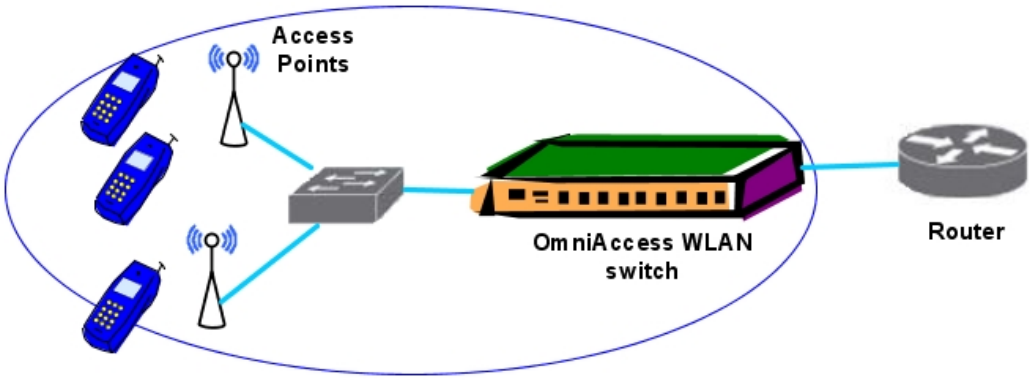


Figure 5.44 : Simple WLAN deployment scenario

The tasks to configure this scenario are as follows:

1. Run the Initial Setup
   - Set the IP address of the voice VLAN 1.
   - Set the default gateway to the IP address of the interface of the upstream router to which you will connect the WLAN Switch.
2. Connect the uplink port on the WLAN Switch to the switch or router interface. By default, all ports on the WLAN Switch are access ports and will carry traffic for a single VLAN.
3. Deploy the APs.
4. Configure user roles and policies (authentication, encryption, and QoS).
5. Configure optional voice features.

5.2.1.5.2 Setting up the WLAN switch

Run the Initial Setup to configure administrative information for the WLAN Switch. When you run the Initial Setup for the first time, you enter:

- the role (master or local) for the WLAN Switch
- passwords for administrator and configuration access
- the country code for the country in which the WLAN Switch will operate; this sets the regulatory domain for the radio frequencies that the APs use
- an IP address for the VLAN 1 interface, which you can use to access and configure the WLAN Switch remotely via an SSH or WebUI session

After you complete the Initial Setup, the WLAN Switch reboots using the new configuration. For more information about using the Initial Setup, see the AOS-W Quick Start Guide.

5.2.1.5.3 Configuring the VLAN

Configure the VLANs if the WLAN switch will use separate voice and data VLANs. You do not need to perform this step if you are using VLAN 1 to connect the WLAN Switch to the wired network.

To configure a VLAN for network connection:

1. Using the VLAN 1 IP address to start the WebUI, navigate to the **Configuration > Network > VLANs** page.
2. Click **Add** to create a new VLAN.
3. On the **Add New VLAN** screen, enter an id for the **VLAN ID** and click **Apply**.
4. Navigate to the **Configuration > Network > IP > IP Interfaces** page. Click **Edit** for the VLAN you just added. Select **Use the following IP address**. Enter the IP address and network mask of the VLAN interface. If required, you can also configure the address of the DHCP server for the VLAN by clicking **Add**.
5. Click **Apply** to apply this configuration. Clicking **Apply** saves changes to the running configuration but the changes are not retained when the WLAN Switch is rebooted.
6. At the top of the page, click **Save Configuration**. Clicking **Save Configuration** saves configuration changes so they are retained after the WLAN Switch is rebooted.

To assign and configure the trunk port:

1. Navigate to the **Configuration > Network > Ports** page on the WebUI.
2. In the **Port Selection** section, click the port that will connect the WLAN Switch to the network.
3. For **Port Mode**, select **Trunk**.
4. For **Native VLAN**, select the voice VLAN created in the last procedure from the scrolling list, then click the **<--** arrow.
5. Click **Apply**.

To configure the default gateway:

1. Navigate to the **Configuration > Network > IP > IP Routes** page.
2. In the **Default Gateway** field, enter IP gateway address for the voice VLAN.
3. Click **Apply**.

5.2.1.5.4 Connecting the WLAN Switch to the Network

Connect the ports on the WLAN Switch to the appropriately-configured ports on an L2 switch or router. Make sure that you have the correct cables and that the port LEDs indicate proper connections. Refer to the Installation Guide for the WLAN Switch for port LED and cable descriptions.

To verify that the WLAN Switch is accessible on the network, ping the VLAN IP address (either the VLAN 1 or newly created VLAN) from a workstation on the network.

5.2.1.5.5 Deploying APs

Alcatel-Lucent APs are designed to require only minimal setup to make them operational in an Alcatel-Lucent OmniAccess WIreless system. When connected to the network, each AP is assigned a valid IP address. APs are able to locate the WLAN Switch using the Alcatel-Lucent Discovery Protocol (ADP).

Note:

To use ADP, all Alcatel-Lucent APs and WLAN Switches must be connected to the same Layer-2 network. If the devices are on different networks, a Layer-3 compatible discovery mechanism, such as DNS, DHCP, or IGMP forwarding, must be used instead.

Perform a site survey to help determine the number and location of APs (see module Voice over Wireless LAN - Engineering Rules Overview). Once the APs are deployed and operational, you can configure them on the WLAN Switch.

5.2.1.5.6 Configuring User Roles

After you have installed a basic AOS-W system, the APs advertise the default SSID. Wireless users can connect to this SSID, but because you have not yet configured authentication, policies, or user roles, they will not have access to the network.

Every WLAN client is associated with a user role, which determines the client's network privileges, how often it must re-authenticate, and which bandwidth contracts are applicable. A policy is a set of rules that applies to traffic that passes through the WLAN Switch. You specify one or more policies for a user role. Finally, you can assign a user role to clients before or after they authenticate to the system.

Note:

To configure policies, you must install the Policy Enforcement Firewall licence in the WLAN Switch.

There is a predefined user role configured on the WLAN Switch called "voice" that allows Alcatel-Lucent New Office Environment (NOE) and other VoIP protocols. You can simply configure the authentication of the VoIP handsets and assign this voice role to authenticated clients.

A firewall policy identifies specific characteristics about a data packet passing through the WLAN Switch and takes some action based on that identification, for example, permitting or denying the packet, logging the packet, setting 802.1p bits, or placing the packet into a priority queue. Once a firewall policy is created, it can be applied to a user role (until the policy is applied to a user role, it does not have any effect).

When you create a user role, you specify one or more policies for the role. The following sections give examples for creating user roles and policies for Alcatel-Lucent IP Touch WLAN handsets. For examples of configuring user roles for other types of VoIP handsets (SIP, Vocera, SCCP), see the AOS-W User Guide.

A client is assigned a user role by one of several methods. A user role assigned by one method may take precedence over a user role assigned by a different method. A user role can be derived from user attributes when the client associates with an AP. An example of configuring a user-derived role is given below.

Configuring a User Role for NOE Clients

This section describes how to configure a user role "noe-phones" for handsets that use the NOE signalling protocol without an SVP server. The "noe-phones" user role consists of the predefined policy "control", which permits basic IP connection, and a user-defined policy "noe-policy". The "noe-policy" policy includes a rule that permits NOE traffic and sets the traffic to high priority.

Note:

The "noe-policy" configuration shown is an example; you can configure more restrictive rules for a policy if additional security is required.

To use the WebUI to configure an NOE user role:

1. Navigate to the **Configuration > Security > Access Control** page.
2. Select the **Policies** tab. Click **Add** to create a new policy.

3. For **Policy Name**, enter `noe-policy`.
4. Under **Rules**, click **Add**.
   a. For **Source**, select **any**.
   b. For **Destination**, select **any**.
   c. For **Service**, select **service**, then select **svc-noe**.
   d. For **Action**, select **permit**.
   e. For **Queue**, select **High**.
   f. Click **Add**.
5. Click **Apply**.
6. Select the **User Roles** tab. Click **Add** to add a user role.
   a. For **Role Name**, enter `noe-phones`.
   b. Under **Firewall Policies**, click **Add**.
   c. For **Choose from Configured Policies**, select the previously-configured **noe-policy** from the drop-down menu.
   d. Click **Done**.
   e. Under **Firewall Policies**, click **Add**.
   f. For **Choose from Configured Policies**, select **control** from the drop-down menu.
   g. Click **Done**.
7. Click **Apply**.

Configuring a user role for SVP clients

This section describes how to configure the user role “svp-phones” for SVP traffic. The user role consists of the predefined policy “control”, which permits basic IP connection, and a user-defined policy “svp-policy”. The “svp-policy” policy includes rules that permit SVP traffic and traffic to DHCP and TFTP servers. All traffic is set to high priority.

To use the WebUI to configure an SVP user role:

1. Navigate to the **Configuration > Security > Access Control** page.
2. Select the **Policies** tab. Click **Add** to create a new policy.
3. For **Policy Name**, enter `svp-policy`.
4. Under **Rules**, click **Add**.
   a. For **Source**, select **any**.
   b. For **Destination**, select **any**.
   c. For **Service**, select **service**, then select **svc-svp**.
   d. For **Action**, select **permit**.
   e. For **Queue**, select **High**.
   f. Click **Add**.
5. Under **Rules**, click **Add**.
   a. For **Source**, select **any**.
   b. For **Destination**, select **any**.
   c. For **Service**, select **service**, then select **svc-tftp**.
   d. For **Action**, select **permit**.
   e. For **Queue**, select **High**.

f. Click **Add**.

6. Under **Rules** click **Add**.
   a. For **Source**, select **any**.
   b. For **Destination**, select **alias**, then click **New**.
   - For **Destination Name**, enter `dhcp-server`.
   - Under **Type**, click **Add**.
   - Enter the IP address(es) of the DHCP server(s) in your network, then click **Add**.
   - Click **Apply** to add this alias to the **Destination** menu.
   - Select this alias from the **Destination** drop-down menu.

   c. For **Service**, select **service**, then select **svc-dhcp**.
   d. For **Action**, select **permit**.
   e. For **Queue**, select **High**.
   f. Click **Add**.
7. Under **Rules** click **Add**.
   a. For **Source**, select **any**.
   b. For **Destination**, select **alias**, then click **New**.
   - For **Destination Name**, enter `tftp-server`.
   - Under **Type**, click **Add**.
   - Enter the IP address(es) of the TFTP server(s) in your network, then click **Add**.
   - Click **Apply** to add this alias to the **Destination** menu.
   - Select this alias from the **Destination** drop-down menu.

   c. For **Service**, select service, then select **svc-tftp**.
   d. For **Action**, select **permit**.
   e. For **Queue**, select **High**.
   f. Click **Add**.
8. Click **Apply**.
9. Select the **User Roles** tab. Click **Add** to add a user role.
   a. For **Role Name**, enter `svp-phones`.
   b. Under **Firewall Policies**, click **Add**.
   c. For **Choose from Configured Policies**, select the previously-configured **svp-policy** from the drop-down menu.
   d. Click **Done**.
   e. Under **Firewall Policies**, click **Add**.
   f. For **Choose from Configured Policies**, select **control** from the drop-down menu.
   g. Click **Done**.
10. Click **Apply**.

Configuring user-derivation rules

The user role can be derived from attributes from the client's association with an AP. For VoIP phones, you can configure the devices to be placed in their user role based on the SSID or the Organizational Unit Identifier (OUI) of the client's MAC address.

Note:

User-derivation rules are executed before the client is authenticated.

To use the WebUI to derive the role based on SSID:

1. Navigate to the **Configuration > Security > Authentication > User Rules** page.
2. Click **Add** to add a new set of derivation rules. Enter a name for the set of rules, and click **Add**. The name appears in the **User Rules Summary** list.
3. In the **User Rules Summary** list, select the name of the rule set to configure rules.
4. Click **Add** to add a rule. For **Set Type**, select **Role** from the drop-down menu.
5. For **Rule Type**, select **ESSID**.
6. For **Condition**, select **equals**.
7. For **Value**, enter the SSID used for the phones.
8. For **Roles**, select the user role you previously created.
9. Click **Add**.
10. Click **Apply**.

5.2.1.5.7 Configuring the VoIP CAC Profile

VoIP call admission control prevents any single AP from becoming congested with voice calls. You configure call admission control options in the VoIP CAC profile which you apply to an AP group or a specific AP.

Note:
This feature requires installation of the Voice Services Module licence in the WLAN Switch.

To use the WebUI to configure the VoIP CAC profile:

1. Navigate to the **Configuration > AP Configuration** page. Select either **AP Group** or **AP Specific**.
   - If you select **AP Group**, click **Edit** for the AP group name for which you want to configure VoIP CAC.
   - If you select **AP Specific**, select the name of the AP for which you want to configure VoIP CAC.
2. In the **Profiles** list, select **QoS**.
3. Select **VoIP Call Admission Control** profile.
4. You can select a profile instance from the drop-down menu. Or you can modify parameters and click **Save As** to create a new VoIP CAC profile instance.
5. To enable CAC options, select **VoIP Call Admission Control** (this option is disabled by default).
6. Click **Apply**.

In the VoIP Call Admission Control (CAC) profile, you can limit the number of active voice calls allowed on an AP. This feature is disabled by default. When the disconnect extra call feature is enabled, the system monitors the number of active voice calls, and if the defined threshold is reached, any new calls are disconnected. The AP denies association requests from a device that is on call.

You enable this feature in the VoIP CAC profile. You also need to enable call admission control, which is disabled by default, in this profile.

To use the WebUI to disconnect excess calls:

1. Navigate to the **Configuration > AP Configuration** page. Select either **AP Group** or **AP Specific**.
   - If you select **AP Group**, click **Edit** for the AP group name for which you want to enable disconnect excess calls.
   - If you select **AP Specific**, select the name of the AP for which you want to enable disconnect excess calls.
2. In the **Profiles** list, select **QoS**.
3. Select **VoIP Call Admission Control** profile.
4. Select **VoIP Call Admission Control** check box.
5. Scroll down to select the **VoIP Disconnect Extra Call** check box.
6. You can optionally change the **VoIP High-capacity Threshold** value.
7. Click **Apply**.

When you enable CAC options, you should also enable VoIP-aware scanning in the Adaptive Radio Management (ARM) profile.

To use the WebUI to enable VoIP aware scanning in the ARM profile:

1. Navigate to the **Configuration > AP Configuration** page. Select either **AP Group** or **AP Specific**.
   - If you select **AP Group**, click **Edit** for the AP group name for which you want to configure IDS.
   - If you select **AP Specific**, select the name of the AP for which you want to configure IDS.
2. In the **Profiles** list, select **RF Management**.
3. Select **Adaptive Radio Management (ARM)** profile.
4. Check the **VoIP Aware Scan** option.
5. Click **Apply**.

5.2.1.5.8 Optional configurations for voice

Optionally, you can configure several other voice-related features in the WLAN Switch:

- **WiFi Multimedia (WMM)** which supports the 802.11e wireless QoS standard and works with 802.11a, b, and g physical layer standards.
- **Battery Boost** which converts all musticast traffic to unicast before delivery to the client.
- **WPA Fast Handover** which allows certain WPA clients to use a pre-authorized PMK to reduce handover interruption.

The following features require installation of the Voice Services Module licence in the WLAN Switch:

- **Dynamic WMM Queue Management**
- **TSPEC Signalling Enforcement**
- **WMM Queue Content Enforcement**
- **Voice-Aware 802.1x**

- **SIP Authentication Tracking**
- **SIP Call Setup Keepalive**
- **Mobile IP Home Agent Assignment**

For information on the configuration of these voice-related features, see the AOS-W User Guide.

5.2.1.6 WLAN Switch Configuration with AOS-W R2.5.x and Earlier

This chapter guides you in the configuration of the Alcatel-Lucent OmniAccess Wireless Switch (AOS-W) for AOS-W releases up to and including Release 2.5.x, which support Alcatel-Lucent Mobile IP Touch 300/600. For information on the procedure to configure the WLAN Switch for AOS-W Release 3.1 and later, see module Voice over Wireless LAN - WLAN Switch Configuration with AOS-W R3.1 and Later . For information on migrating to AOS-W R3.1, see module Voice over Wireless LAN - AOS-W R3.1 Migration .

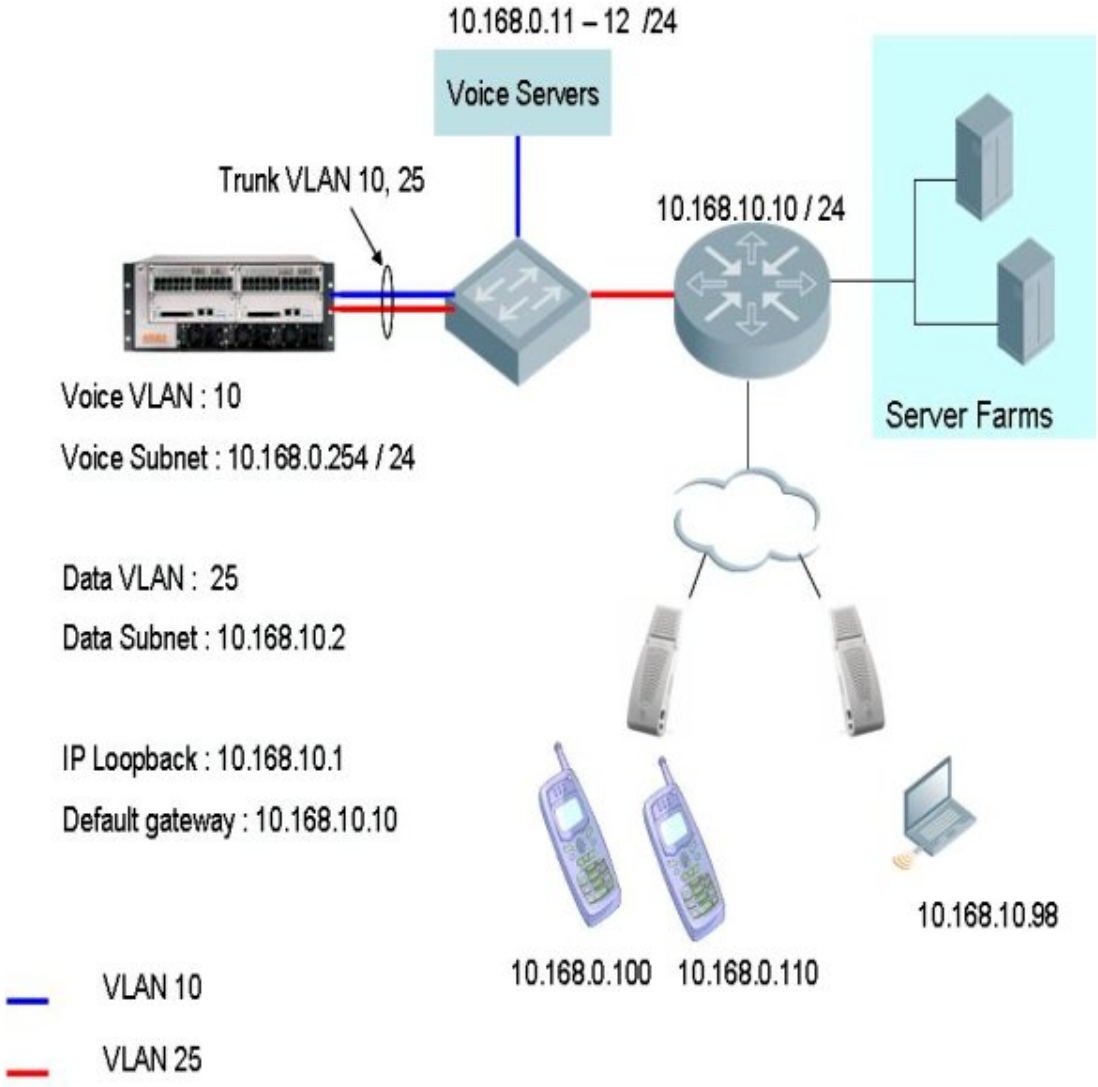
Alcatel-Lucent recommends you place the SVP Server and the handsets in the same broadcast domain.

This configuration guide assumes that the base WLAN Switch licence and the Firewall Module licence have been enabled on the WLAN Switches being used.

5.2.1.6.1 Topological Requirements

Before configuring the WLAN Switch, it is necessary to determine the topology to deploy. This section provides the reader with recommendations for a single WLAN Switch deployment scenario. It is important to remember that these recommendations are generic in nature and may have to be fine-tuned for the deployment on hand.

L2/L3 requirements



- Interfaces on the WLAN Switch

  A simple setting would be to place the voice users on one VLAN and the data users on another VLAN. Each VLAN requires a unique IP address. In addition the WLAN Switch IP address needs to be set via the loopback interface setting. The loopback address should be a routable address such that the APs can reach this address.

- Identify the ports that would be the uplink port belonging to VLAN 25. Assume that the port used in this case is Fast Ethernet 1/0 and is a trunk port with VLAN 10 and 25.

- Default route

  This will have to be configured to the next hop gateway connected to the controller.

- Physical interface

  Identify the interface connected to the routers, servers and gateways and set them as trusted.

- Connecting the APs

  The APs need an IP address to operate. They can be connected to the WLAN Switch over a L2 or L3 network. Ensure that DHCP is enabled on the subnet the APs are connected to and can ping the Alcatel Mobility Controller “switch IP address” from their current subnet.

RF Settings

Perform a site survey to help determine the number of Access Points required and the channel and power settings. Ensure that the APs can reach the Controllers loopback address from the subnet they are placed in. Once the APs get an IP address they will boot up and become operational. Refer to the Configuration / User Guides for AP configuration and deployment.

Once deployed and operational, it is necessary to configure the RF environment to support voice and data clients.

Use unique SSIDs for the voice and data network. This is because the level of encryption used for a voice network would be less secure than that used for a data network. Example settings for the RF environment:

	ESSID	**VLANID**	**Encryption**	**DTIM**	**Retry**
Voice	Voice	10	Static WEP	2	2
Data	Data	25	WPA2-AES	1	Default

- Radio Setting .11b or .11g - Most VoWLAN phones are 802.11b phones. In addition some phone equipment vendors recommend that the radio be set to an 802.11b mode and not the b/g mixed mode.
- Preamble Settings – Set the preamble on the AP to the preamble settings recommended by the voice equipment vendor. If the preamble setting required is long for the voice equipment, use the short preamble setting on the WLAN Switch as this supports both long and short preamble unless specified otherwise.
- When using a single radio AP, the radio will have to be set to operate as an 802.11b radio for both the voice and data network. When using the dual radio APs, the data devices can use the 802.11a network and share the 802.11b network with the voice devices.

Securing Access to the WLAN Switch

Configure a username and password on the WLAN Switch to ensure secure access. Refer to the User Guide for information on configuring the Management user.

Only web and SSH access to the WLAN Switch is permitted by default. Configurations at the CLI can also be done via the WLAN Switch's console.

Configuring the WLAN Switch

On power up, the user is presented with the startup wizard:

```
Enter System name : Alcatel4308
Enter VLAN 1 interface IP address [172.16.0.254]:
Enter VLAN 1 interface subnet mask [255.255.255.0]:
Enter IP Default gateway [none]:
Enter Switch Role, (master|local) [master]: master
Enter Country code (ISO-3166), <ctrl-I> for supported list: US
You have chosen Country code US for United States (yes|no)?: yes
Enter Password for admin login (up to 32 chars): admin
Re-type Password for admin login: admin
Enter Password for enable mode (up to 15 chars): enable
Re-type Password for enable mode: enable
Do you wish to shutdown all the ports (yes|no)? [no]: no

Current choices are:

System name: Alcatel4308
VLAN 1 interface IP address: 172.16.0.254
VLAN 1 interface subnet mask: 255.255.255.0
IP Default gateway: none
Switch Role: master
Country code: US
Ports shutdown: no

If you accept the changes the switch will restart!
Type <ctrl-P> to go back and change answer for any question
Do you wish to accept the changes (yes|no)yes
. . . . .

<<<<< Welcome to Alcatel Wireless Networks - Alcatel 4308>>>>>

Performing CompactFlash fast test... passed.
Reboot cause: User reboot.
Crash information available.
Restoring the database...done.
Reading configuration from default.cfg

(Alcatel)
User:
```

Login to the WLAN Switch. The default login is `admin`, the default password is `admin`.

Configure the VLAN interface, IP address and default gateway to access the WLAN Switch over the network.

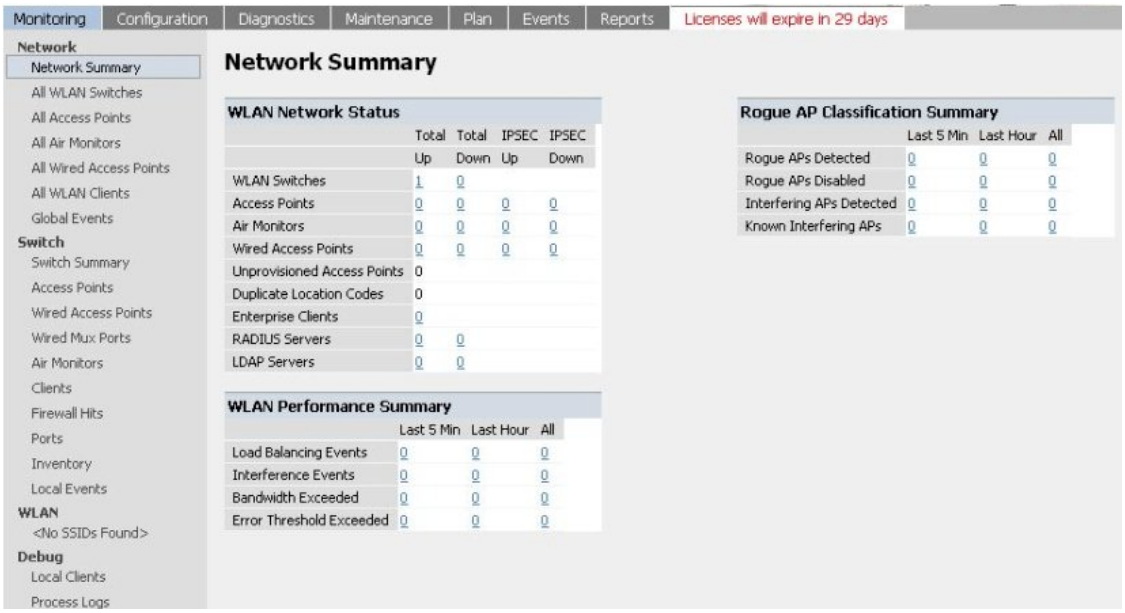
```
User: admin
Password *****
(OAW-4324) >en
Password:******
(OAW-4324) #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(OAW-4324) (config) #vlan 25

(OAW-4324) (config) #interface vlan 25
(OAW-4324) (config-subif)#ip address 10.168.10.2 255.255.255.0

(OAW-4324) (config-subif)#!

(OAW-4324) (config) #interface loopback
(OAW-4324) (config-loop)#ip address 10.168.10.1
Switch IP Address is Modified. Switch should be rebooted now
```

```
(OAW-4324) (config-loop)#!
(OAW-4324) (config) #ip default-gateway 10.168.10.10

(OAW-4324) (config) #interface fastethernet 1/0
(OAW-4324) (config-if)#trusted
(OAW-4324) (config-if)#no shutdown

(OAW-4324) (config-if)#switchport mode trunk
(OAW-4324) (config-if)#switchport trunk allowed vlan all
(OAW-4324) (config-if)#!
(OAW-4324) (config)#
```

Ping the default gateway from the WLAN Switch's console. Ping the WLAN Switch's IP address from the management station. Once the connectivity to the WLAN Switch is verified, open a web browser and enter the WLAN Switch's IP address in the navigator bar.

Use **http://<switch IP Address>** or **https://<switch IP Address>:4343**

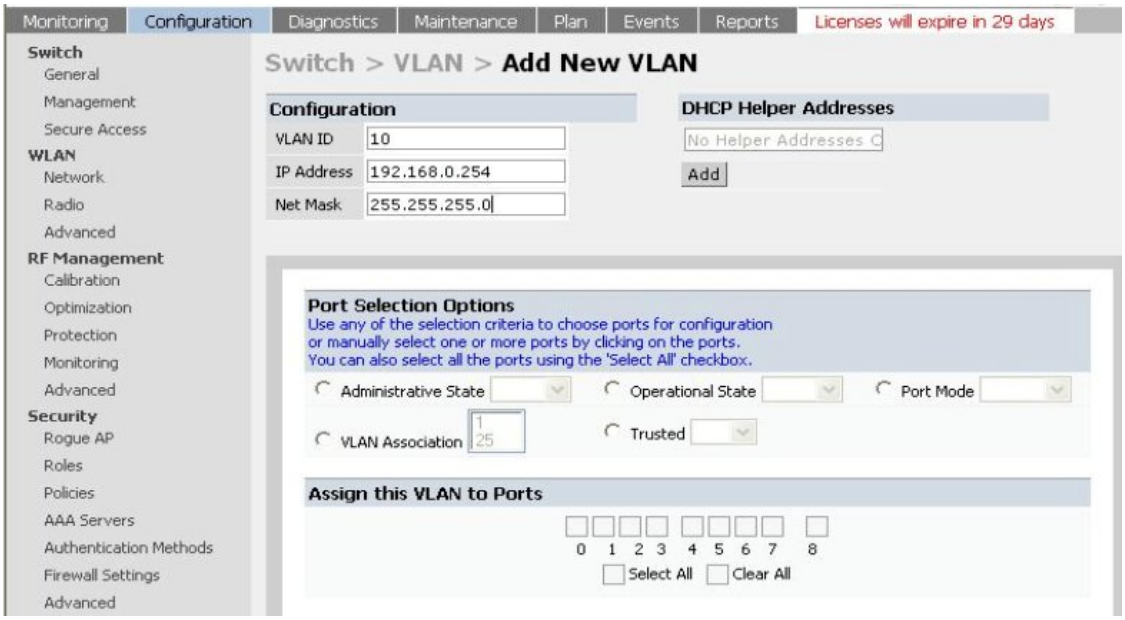
The user is prompted with the username and password configured (in the example above, the username / password configured is admin / admin). On successful login the Network Summary page opens up.



Configuring the Voice VLAN

In case the WLAN Switch is being configured to use separate voice and data VLANs, the VLANs need to be configured.

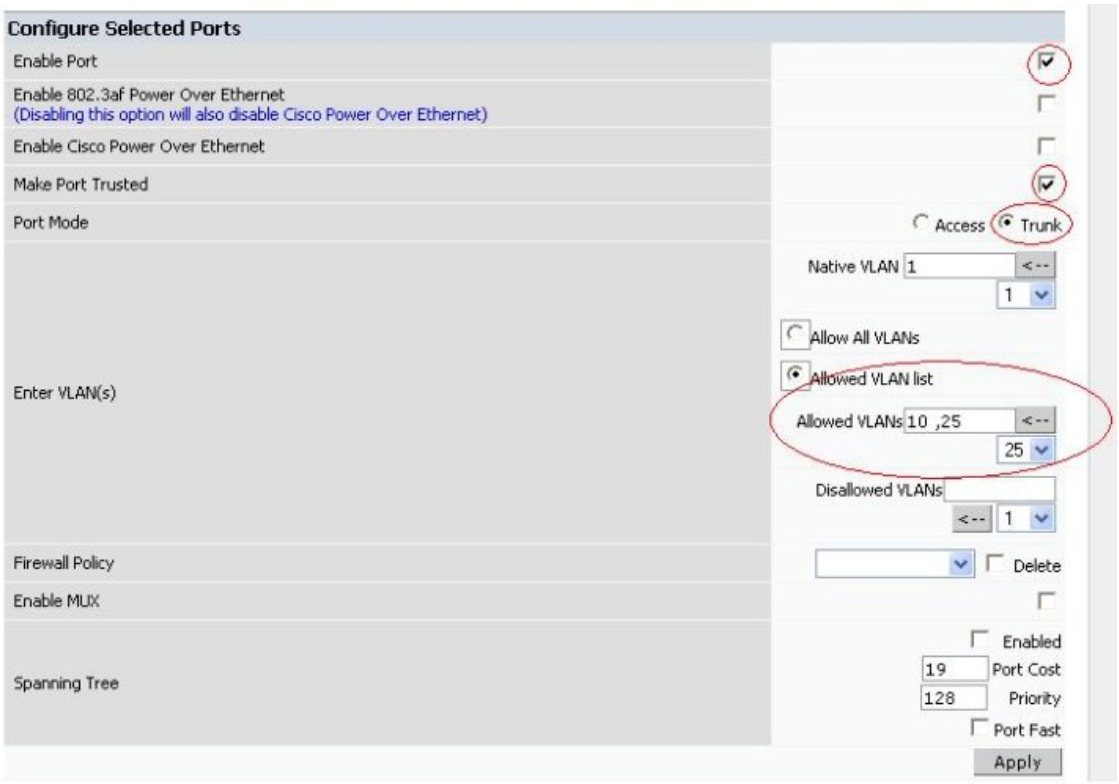
Navigate to **Configuration > Switch > General** page and select the VLAN tab. This page will display all the VLANs configured so far. To configure a new VLAN click on the Add tab and configure the VLAN. On entering the configuration, click the **APPLY** tab to apply the changes made on this page.




```
configure terminal
vlan 10
interface vlan 10
   ip address 192.168.0.254 255.255.255.0
```

Assigning Ports to a VLAN

In this example the port connecting to the L2 switch is a trunk port with both the data and voice VLAN. Navigate to the **Configuration > General > Port** page. Select the port that needs to be configured and set up as required. For configuration guidelines refer to the user guide.



Configuring the AP

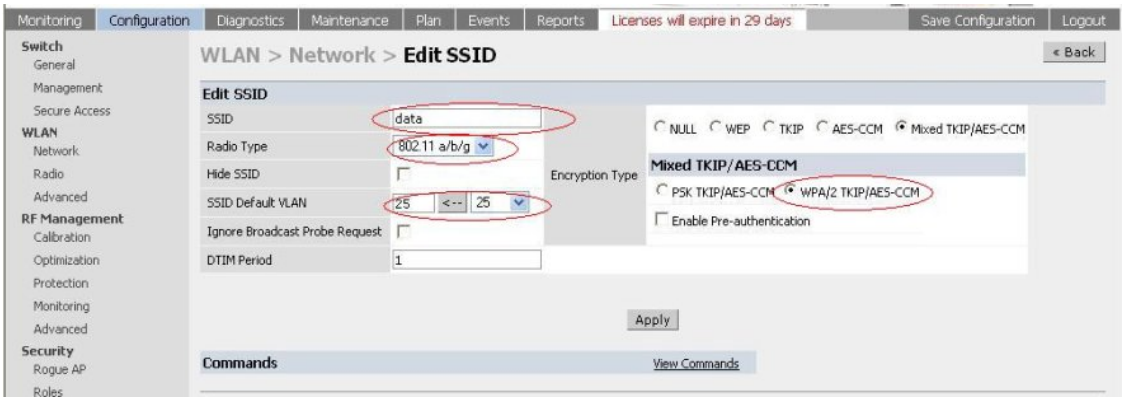
Refer to the User guide for initial configuration of the APs. Once the APs are connected they will bootstrap to the WLAN Switch. After this the APs can be seen on the WLAN Switch as “Alcatel Access Points” on the **Monitoring > Network Summary** page.

Configuring WLAN – Voice and Data

Once the AP has been configured, it is now necessary to configure the ESSID for voice and data devices. In this example, the *data* WLAN settings are:

	ESSID	**VLANID**	**Encryption**	**DTIM**	**Retry**
Data	Data	25	WPA2-AES	1	Default

Navigate to the **Configuration > WLAN > Network** page



Click the **Apply** tab to apply the changes made on this page.

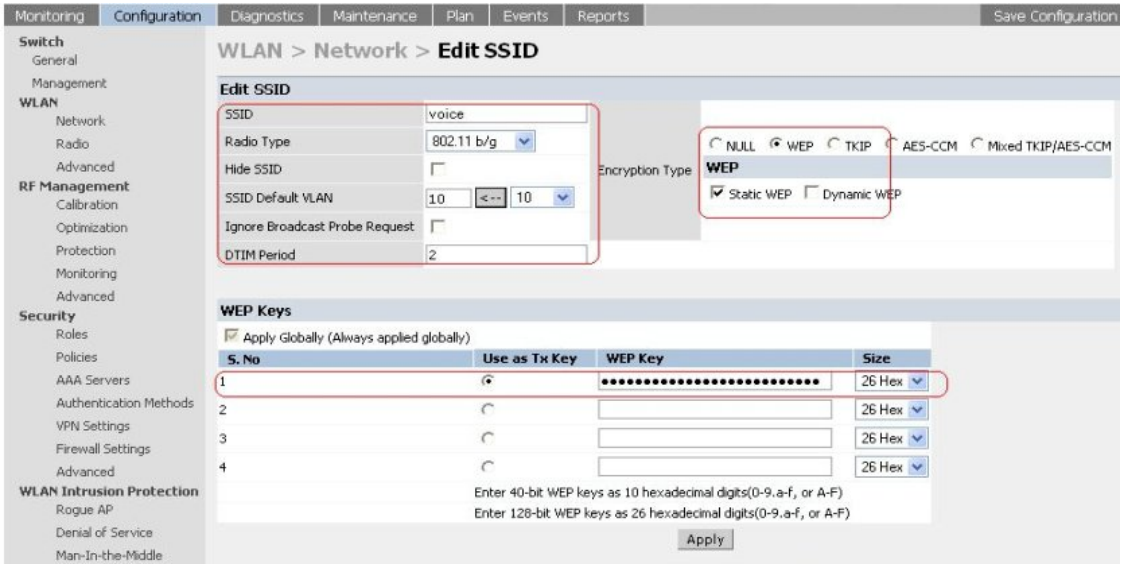
NOTE: For more options on WLAN settings read the User Guide.

Voice WLAN Settings

	ESSID	VLANID	Encryption	DTIM	Retry
Voice	Voice	10	Static WEP	2	2

To configure the voice WLAN, navigate to the **Configuration > WLAN > Network** page and click the**Add** tab.

Add the SSID, set the radio to b/g, set the dtim period to the value recommended by the voice equipment vendor. Select the encryption method as required. Click the **Apply** tab once these changes have been made.



Navigate to the **WLAN > Network > Radio** page and set the max-retries to 2 and the max-clients to the required value for the 802.11g radio (recommended value is 25).

Ensure that the rates 1,2 are selected and 5 and 11 are selected in the supported rates option.

If the voice equipment vendor requires the radio to be configured as a b-only radio, set it on the WLAN Switch using the CLI.

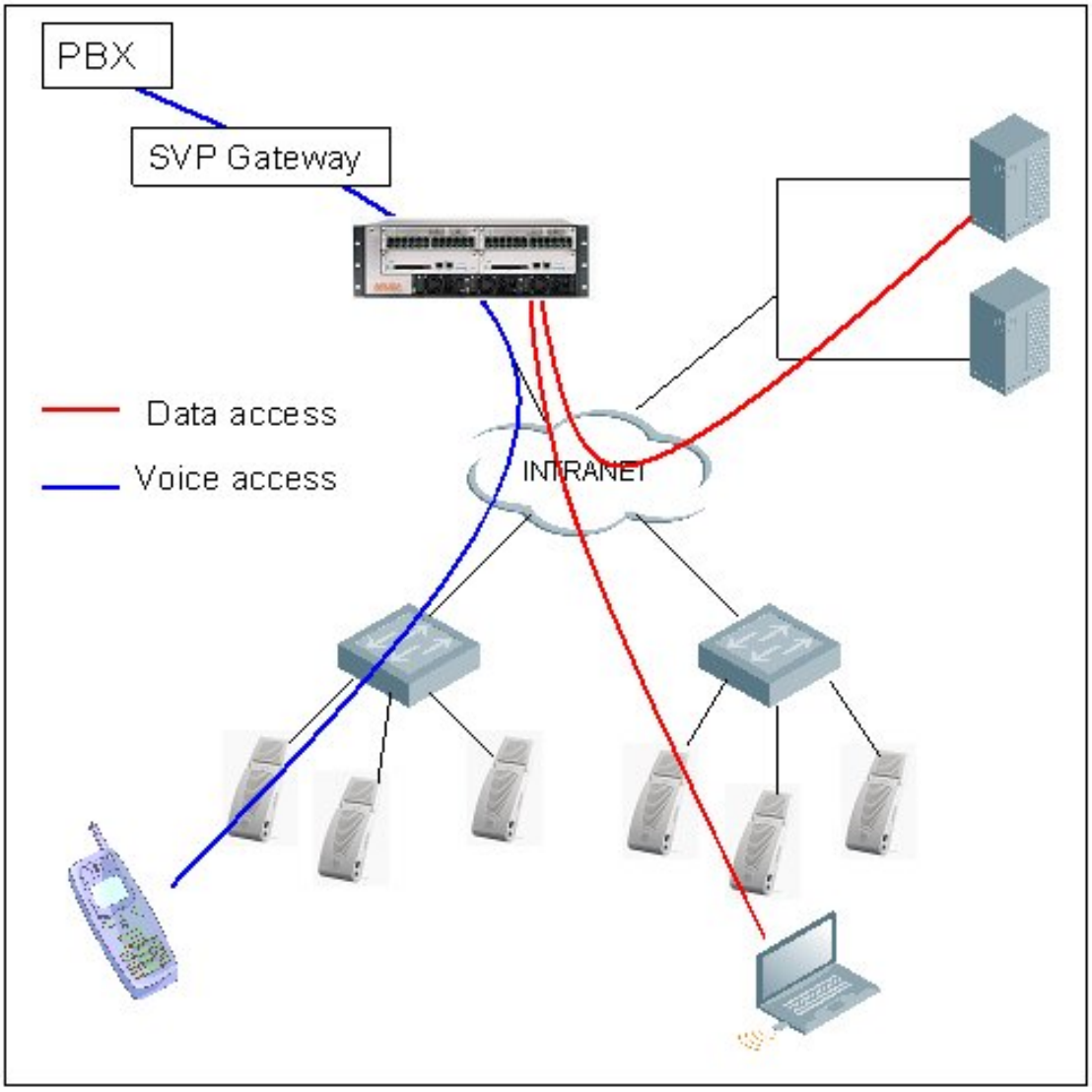
It is also recommended to enable local-probe-response. Local probe response allows APs to respond to probe requests locally from the AP and not wait for the same from the WLAN Switch. Enabling local-probe-response helps with the mobility.

```
configure terminal
ap location 0.0.0
 max-tx-fail 25
phy-type g
    bg-mode b-only
    local-probe-response enable
```

Alternatively, the same can be configured from the WLAN Switch's CLI.

```
configure terminal
ap location 0.0.0
 max-tx-fail 25
phy-type a
    essid "data"
    opmode dynamicTkip,wpa2-aes
    vlan-id 25
    max-clients 64
!
phy-type g
    max-retries 2
    max-clients 25
    short-preamble enable
    bg-mode mixed  ← set to b-only as per the phone equipment
vendor recommendations
    opmode dynamicTkip,wpa2-aes
    essid "data"
    vlan-id 25
    virtual-ap "voice" vlan-id 10 opmode staticWep deny-bcast
disable weptxkey 1 hide-ssid disable dtim-period 3
   !
```

5.2.1.6.2 Security and QoS



Once the basic infrastructure is configured, it is necessary to configure the security policies to ensure that the data network is secured from the voice network. The voice network is as secure as the voice equipment and the encryption selected. It is therefore necessary to protect the data network from the voice network and the voice devices from attacks.

In the example design, the voice and data devices are on two different VLANs. The encryption used by the phones is static WEP making it necessary to limit network access to the user devices on the phone subnet. The rights of the voice device are limited to the voice servers and traffic on limited ports. The Alcatel-Lucent system is also session aware and can follow SIP, SCCP and other voice protocols to open ports for voice traffic as and when required. The data devices with advanced encryption and authentication will be assigned advanced access rights to data servers and the data network.

Access Rights for the Phones

The voice devices (phones) should have limited access to the network. Access to only the required voice server, DHCP and TFTP servers should be permitted. In case the phones do not communicate with each other directly (no peer-to-peer communication) then user to user communication should be denied.

```
Example: For MIPT phones with WEP encryption
ACLS
Phone -> SVP_server svp_svc permit queue high
SVP_server -> Phone svp_svc permit queue high
user -> multicast address any permit queue low
User -> dhcp_server svp_dhcp permit queue low
Dhcp_server user svc_dhcp permit queue low
User -> tftp_server svp_tftp permit queue low
user -> user any deny
Add other ACLs as required to permit other traffic from the phones.
```

Create aliases for the servers

Navigate to the **Configuration > Advanced (under the Security sub-heading)** page and select the **Destination** tab. To add a new destination, click the **Add** tab.

Create a new net-destination, ex. svp-server and add the SVP servers as hosts.

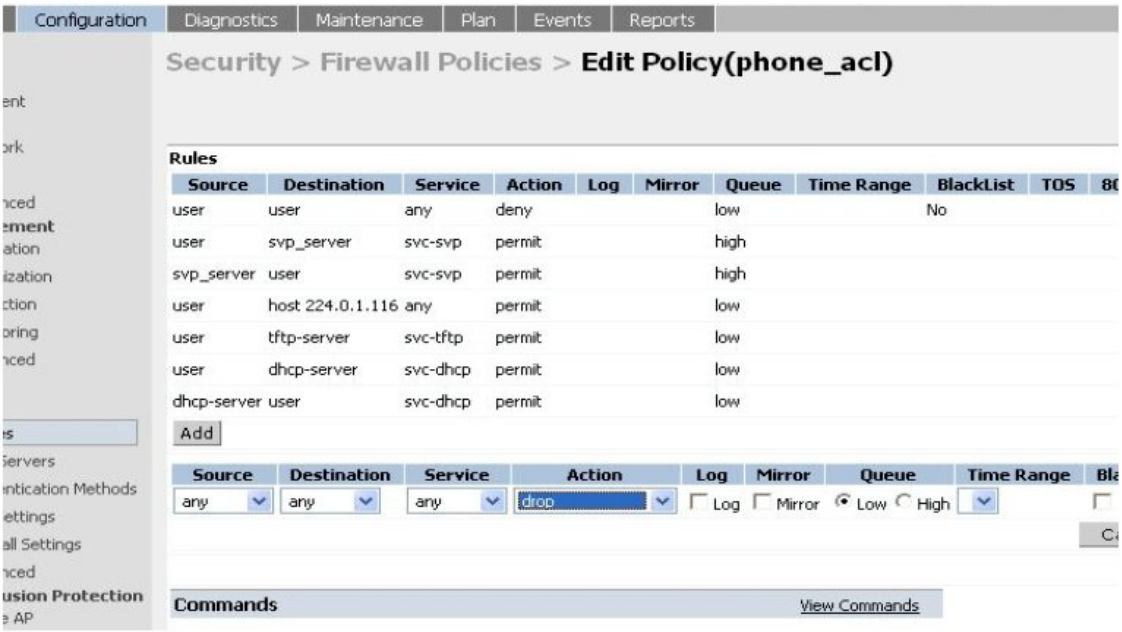
```
For more details on configuring the net-destinations refer to the User Guide.
```

Create policies for the phone user

Create the access policies that define the access rights for the phones.

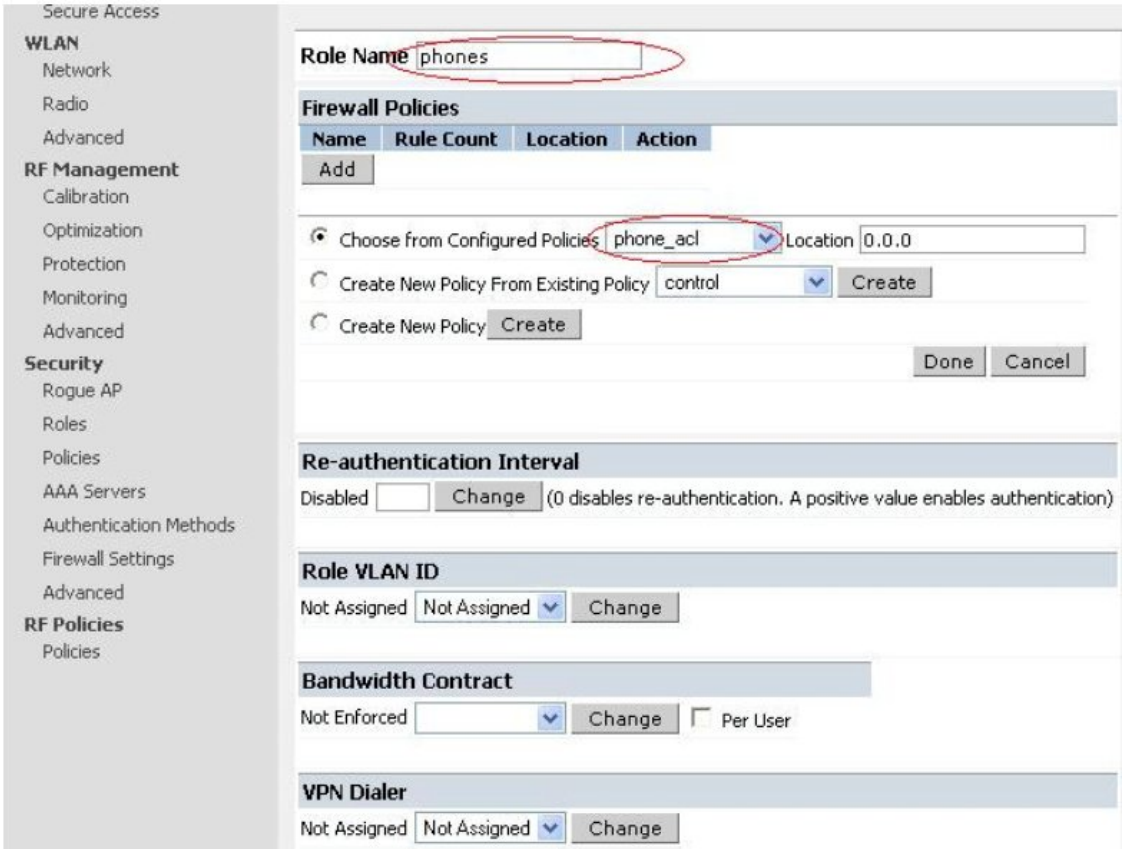
```
Example: For MIPT phones with WEP encryption
ACLS
Phone -> SVP_server svp_svc permit queue high
SVP_server -> Phone svp_svc permit queue high
user -> multicast address any permit queue low
User -> dhcp_server svp_dhcp permit queue low
User -> tftp_server svp_tftp permit queue low
user -> user any deny
Add other ACLs as required to permit other traffic from the phones.
```

Navigate to the **Configuration > Security > Firewall Policies** page. Click **Add** tab to add a new policy. Configure the policy as shown.



Assign Policies to the Role

Create a role, say phones and assign the policies to this role. This is the role that would be assigned to the phones when they are authenticated successfully.



CLI commands corresponding to this section:

```
configure terminal
netdestination tftp-server
  host 10.168.0.20
!
netdestination svp_server
  host 10.168.0.11
  host 10.168.0.12
!
netdestination dhcp-server
  host 10.168.0.21
!
ip access-list session phone_acl
  user user any deny
  user   alias svp_server svc-svp permit queue high
  alias svp_server user svc-svp permit queue high
  user   alias tftp-server svc-tftp permit
  user   alias dhcp-server svc-dhcp permit
  user host 224.0.1.116 any permit
!
user-role phones
 session-acl phone_acl
!
```

QoS

Quality of service is achieved by prioritising the voice traffic over data traffic. To prioritize the voice traffic over data traffic in the AP traffic queues, the “queue high” tag is used at the end of each ACL to prioritize the traffic matching the ACL over all other traffic. In the example shown above

```
user alias svp_server svc-svp permit queue high
```

```
alias svp_server user svc-svp permit queue high
```

The traffic that matches the above two rules is prioritised over all other traffic. In addition, a DiffServ tag or a Dot1p tag can be configured at the end of each ACL to indicate the relative priority of the traffic to the traffic to the network.

Example:

```
user alias svp_server svc-svp permit dot1p 4 queue high dot1p-priority 4 tos 4 queue high
```

```
alias svp_server user svc-svp permit queue high dot1p-priority 4 tos 4 queue high
```

By default, the packets are not tagged.

Authentication

The user equipment has to be authenticated before it is given access to the voice network. Selection of authentication method should be made based on the following criteria:

- Authentication methods supported by the device
- Roaming times published by the phone vendor for the authentication method in question

Authentication methods with acceptable (lower) roam time and authentication time should be the one selected. For phones that do not support advanced authentication methods, MAC authentication can be used.

Alcatel-Lucent can support the use of an internal database or an external Auth server for MAC authentication. Refer to the User Guide for details on Mac Authentication configuration. The phones are authenticated by their MAC addresses. On successful authentication the phones will be assigned the user-role configured, in the current example the role assigned would be phones.

Refer to the User Guide for Mac authentication.

Alternatively a group of users can also be authenticated using their OUIs. Since all phones from a single vendor would start with the same OUI, the authentication can also be configured as follows.

```
configure terminal
aaa derivation rules user
   set role condition macaddr starts-with "00:90:7a" set-value phones
!
```

Note:
Alcatel-Lucent recommends that individual phones MACs be used to authenticate the phones using MAC authentication as described in the User Guide.

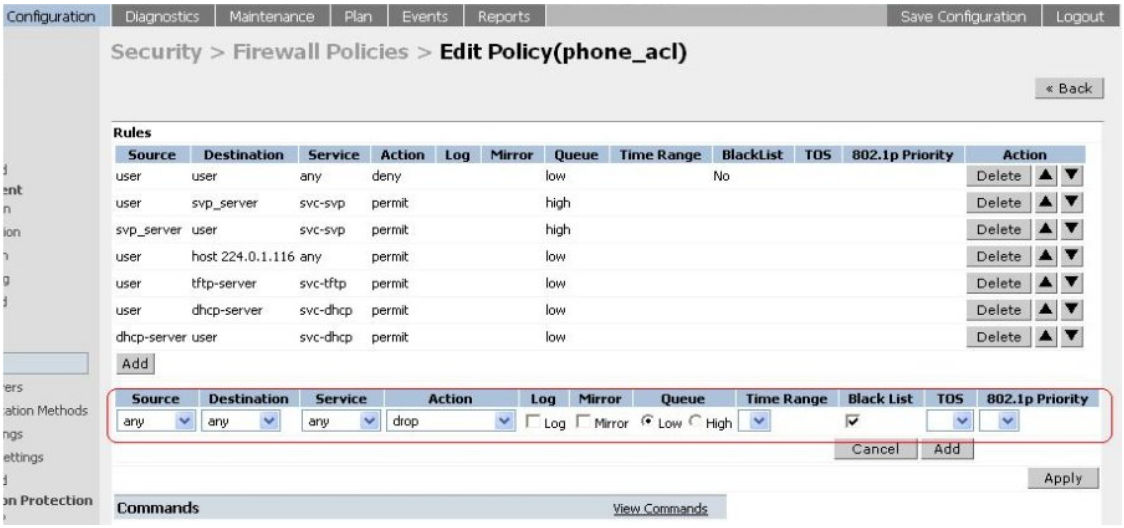
Configure the policies, roles and authentication mechanisms for the data users as described in the User guide.

Blacklisting

Another security mechanism is to blacklist policy violators. Users on the voice role trying to access the non-voice servers or using the non-SVP protocols or non-SVP ports can be blacklisted and denied access to the network. These users could be rogue data users trying to spoof the voice clients to gain access to the network.

To configure blacklisting, navigate to the voice policy configuration page (**Configuration > Policies, Edit phone_acl**) and add a last rule.

```
any any any deny blacklist
```



To take action on the blacklisted clients and to prevent them from accessing the network, enable Dos Protection. This will result in the client being de-authed if they try to access the network.

5.2.1.6.3 Miscellaneous Voice Settings

Some of the features that help data in fast-roaming need to be disabled for voice devices. Ensure that the fast-roaming and handoff assist are disabled.

```
configure terminal
wms
   station-policy handoff-assist disable
!
stm fast-roaming disable
!
```

5.2.1.6.4 RF Management and Voice

The Alcatel-Lucent WLAN system can be configured as a self healing system, it adjusts to compensate for the changes in the RF environment. To accomplish this, the APs must scan all channels to gather the channel information. When configured this way, the APs also monitor the RF environment and perform IDS operations.

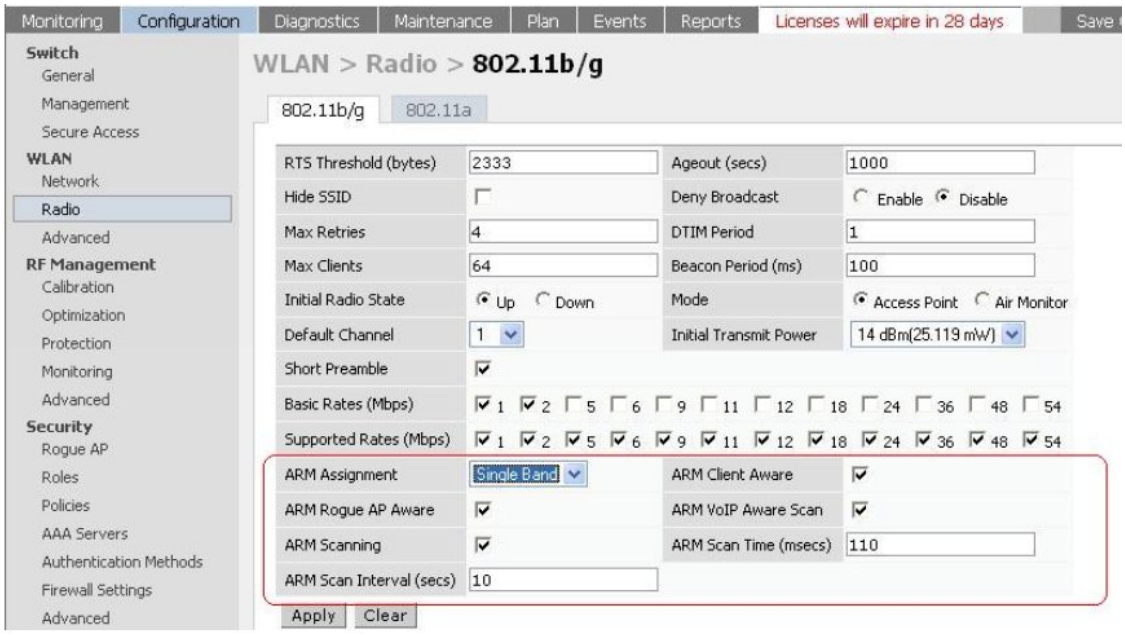
While air scanning has negligible effects on a data network, it may cause some packet loss in the voice network. Alcatel-Lucent's voice aware technology, using the session aware firewalls, allows Alcatel-Lucent's WLAN system to be call-aware. An AP will not scan the network when a phone on call is associated with it. The AP will resume scanning once all the phones associated with the AP are on-hook (off-call).

In a pure voice environment where there is at least 1 active phone (on call) associated with every AP in a given location at any given point of time, Alcatel-Lucent recommends the use of dedicated Alcatel-Lucent Air Monitors to monitor the network.

In a converged environment that does not meet the previous criteria, you can use the APs to monitor the network.

ARM is a configurable feature that can be enabled on the APs. To enable ARM, navigate to the **WLAN > Radio** page.

Select the 802.11b/g tab and enable ARM



Set the ARM assignment to Single Band to force the APs to select an 802.11b/g channel. Select the ARM Rogue AP aware to enable the AP t detect rogues, ARM scanning has to be enabled to allow the APs to scan the channel and find a cleaner channel. If ARM assignment is set, the AP will move to a cleaner channel based on its preset criteria.

Enable ARM VoIP aware scanning to improve voice qualities. This will prevent the APs from scanning other channels or moving to other channels only when the phone associated with it is on a call. When all the phones associated with the AP are off the call or on hook, the AP will presume its normal operations.

Repeat the settings on the 802.11a radio to enable ARM on 802.11a.

NOTE: For details on ARM settings, refer to the User Guide Manuals.

5.2.1.6.5 Load Balancing

The load balancing feature allows you to share Alcatel-Lucent Mobile IP Touch 300/600 and data terminals between the APs.

This feature can be enabled for data terminals. When enabled, the handset's voice quality is not affected.

Alcatel-Lucent recommends disabling this function when data terminals do not use load balancing.

5.2.1.7 Configuring OmniPCX Office

This document describes information for configuring and maintaining Voice over Wireless LAN (VoWLAN) **specific to the Alcatel-Lucent OmniPCX Office Communication Server** . For more information on the general procedure for deploying VoWLAN, see module Voice over Wireless LAN - Overview .

5.2.1.7.1 Licences

Alcatel-Lucent OmniPCX Office Communication Server 5.1 came with 3 new licences displayed in OMC under the "Software key Features" screens:

- 2 main licences: The "Mobile IP users" licence and the "Call accounting over IP" licence.
- 1 CTI licence; The "PIMphony Attendant users" licence.

The software licences are loaded during the system installation in factory and therefore should be present in the system at the customer's premises. If this is not the case, the system starts in the default mode.

Using OMC, it is possible to enter a new software licence during the system life. It is also possible to update the software licence by MMC-SET.

5.2.1.7.2 Compatibilities

The Alcatel-Lucent OmniAccess Wireless Switch (AOS-W) Release R3.1 is designed to work with Alcatel-Lucent OmniPCX Office Communication Server release R6.0.1. For AOS-W R3.1 the following compatibility rules apply:

- Only Alcatel-Lucent IP Touch 310/610 WLAN Handsets accept the Alcatel-Lucent New Office Environment (NOE) protocol (through an “IP Touch 300/600 compatible" mode). The Alcatel-Lucent IP Touch 310/610 WLAN Handsets will not support the H.323 protocol.
- The Alcatel-Lucent IP Touch 310/610 WLAN Handsets in an “IP Touch 300/600 compatible” mode are supported by Alcatel-Lucent OmniPCX Office Communication Server releases prior to R6.0.1. The PCX sees the Alcatel-Lucent Mobile IP Touch 300/600 and Alcatel-Lucent IP Touch 310/610 WLAN Handsets as having the same profile. This configuration is supported only by architectures with an SVP Server.

  Note:
  This architecture (with SVP Server) also allows for a mixed configuration, including Alcatel-Lucent Mobile IP Touch 300/600 and Alcatel-Lucent IP Touch 310/610 WLAN Handsets on the same WLAN network.
- Coexistence of Alcatel-Lucent IP Touch 310/610 WLAN Handsets without an SVP Server and other voice clients without an SVP Server (SIP phone, MPC, …), is a supported

architecture. The Call Admission Control (CAC) is managed by the OmniAccess WLAN Switch.

- Coexistence of Alcatel-Lucent Mobile IP Touch 300/600, needing an SVP Server, and other voice clients without an SVP Server (SIP phone, MPC, …), is a supported architecture. The CAC is centralized in the OmniAccess WLAN Switch. The CAC function in the SVP Server is disabled by setting the maximum calls per Access Point to a very high, unreachable value.
- When Alcatel-Lucent IP Touch 310/610 WLAN Handsets are deployed on a network with Alcatel-Lucent Mobile IP Touch 300/600, some interoperability considerations must be observed. The 310/610 handsets have 25 PTT channels available, where the 300/600 handsets enable only eight PTT channels. When PTT is activated on a network using a mix of handset versions, only the eight common channels will be available for the 300/600 handsets.

5.2.1.7.3 WLAN Switch configuration

You configure network services by defining user roles and policies on the Alcatel-Lucent OmniAccess WLAN Switch. To configure a network service for NOE handsets associated with an Alcatel-Lucent OmniPCX Office Communication Server, you must first enter the following configuration command on the WLAN Switch Command Line Interface:

```
netservice svc-noe-oxo udp 5000 alg noe
```

For more information on configuring the WLAN Switch, see module Voice over Wireless LAN - WLAN Switch Configuration with AOS-W R3.1 and Later .

5.2.1.7.4 Maintenance

Statistics

The following sections describe the WLAN statistics and how to dump them on your PC.

About statistics

Statistics are counters handled by the call server. They provide general information about the VoWLAN performance.

Statistics are created for debug purposes and are used by software technicians. Statistics are also useful to the WLAN network supervision by technical support specialists.

Statistics can be useful in case of customer complaints.

A thorough study and understanding of the statistics provided may lead to a new infrastructure deployment and configuration.

The following statistics are available for the system, the Access Points (APs) and the IP Touch WLAN handsets:

- **System statistics**
  - Last activation date
  - File generation date
  - Calls: Total number of VoWLAN calls
  - Calls cut: Total number of VoWLAN calls abnormally cut
  - Total handoffs: Number of handoffs in system
- **AP statistics**
  - Equipment: MAC address of the AP

- Calls: Total number of voice calls on the AP
- Calls cut: Total number of voice calls abnormally cut
- Simultaneous calls: Maximum number of simultaneous calls
- Saturations nb: Number of times the allowed maximum number of calls on the AP has been reached
- Emergency calls: Total number of emergency calls
- Saturation duration
- Nb handoffs: Number of handoffs

- **WLAN Handset Statistics**
  - Equipment: MAC address of the handset
  - Calls: Total number of voice calls on the handset
  - Calls cut: Total number of voice calls abnormally cut
  - Emergency calls: Total number of emergency calls
  - Nb handoffs: Number of handoffs
  - Nb reset: Total number of handset resets (including switch OFF/ON)

Note:
Statistics are saved after warm reset. They are saved/restored by datasaving. The "Reset" option in OMC creates a total reset of statistics.

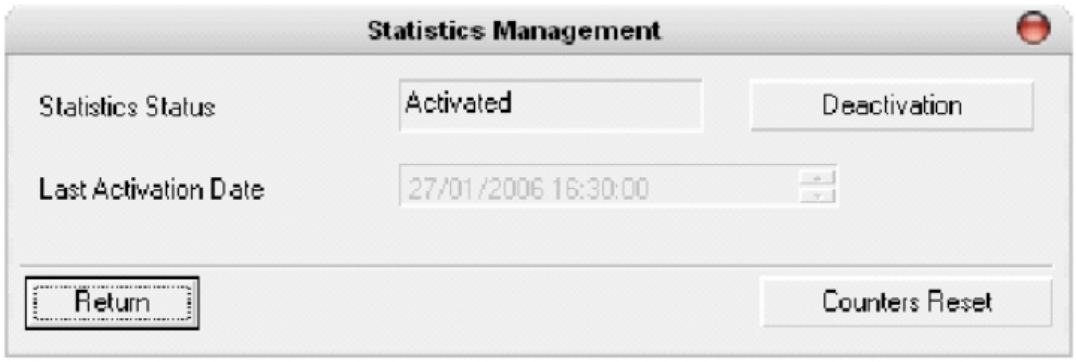
Dumping statistics

OMC allows you to save WLAN statistics on your PC.

1. In the OMC menu tree view, expand the WLAN folder and select the "Statistics Management" item.

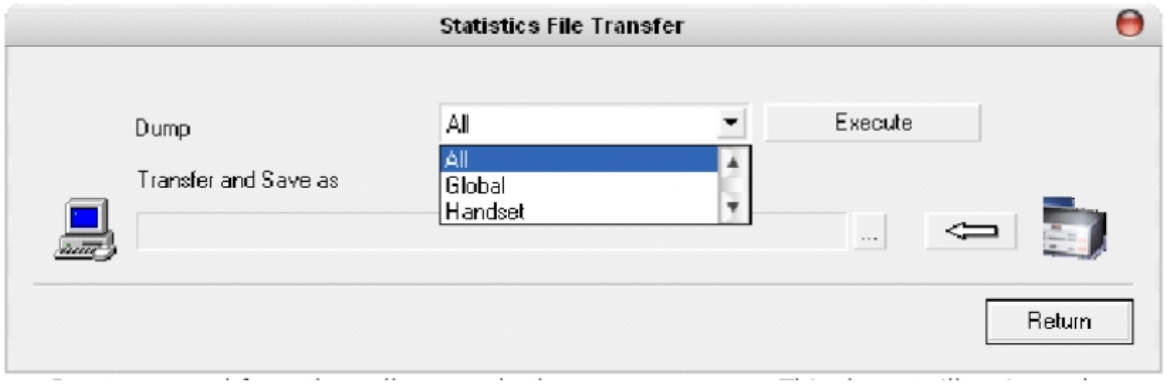
2. In the "Statistics Management" dialogue box, activate the statistics by clicking the **Activation** button beside the "Statistics Status" field.

   The **Activation** button updates the **Last Activation Date**field with the day's date.
   When statistics are active, the field displays "Activated" and the button turns to **Deactivation**.
   Press the **Counters Reset** button to restart the counters from zero. This is the only way to restart the counters. A message box displays the result of this action.



3. In the OMC menu tree view, select "Statistics File Transfer" in the WLAN folder.

4. In the "Statistics File Transfer" dialogue box, you can create and transfer the Statistics file.



5. Select one options of the **Dump** drop down list. Here, you activate the reading of a "CSV" file from the call server and copy it on the PC disk. You can then read the "CSV" file in Microsoft Excel.

   The **Dump** drop down list shows what statistics can be dumped:

   Global System statistics, Handset statistics, Access Point statistics or All statistics.

Note:
Dumping the statistics does not reset the counters to 0 in the call server.
A message box displays the result of this action.

6. Click **Execute**
7. Click **...** to enter the path to save the statistics file on your PC. The Windows "Save As ..." window shows up.
   OR
   Click the Arrow button to directly transfer the statistics file to your PC.
   This process only works if you have activated statistics and executed a dump selection in the "Statistics Management" dialogue box (see steps 1 to 4). Otherwise, an error message indicates that the statistics file has not been created.

Logs

In order to follow any particular behaviour on one Access Point or WLAN handset better, and to localize one particular problem on a device better each time some event happens, the call server writes a string in a .log file. This file is a cyclic one.

Define the length of the file in a way that you have at least a whole day traces in the same file. You will thus avoid losing information if, for any given day, the last event comes to erase the first one.

Older traces are never saved, they are lost when the writing pointer reaches the end of the file. The new traces erase the older ones.

Activating logging

Logging is activated and deactivated with WLAN statistics, using the same flag. The OMC interface for statistics activation is used and is transparent: i.e. there is no explicit flag for log files.

Events to log

The following events are logged for each handset:

- Restart of a handset:
  Each time the handset reboots, manually or after out/in coverage.
- Out of coverage:
  The handset does not answer the "keep alive" messages. (Only during communication)
- In coverage:
  The handset answers again the "keep alive" messages. (Only during communication)
- Losing a communication:
  The communication is cut because the "keep alive" messages are not answered or the handset reboots.
- Active state:
  The handset goes out of idle state, for a new communication or when starting a configuration.
- Idle state:
  The handset comes back to idle state, at the end of a communication or when closing a configuration.
- Audio hole:
  A possible audio hole is detected. No answer on "keep alive" messages during communication. This event also gives the audio hole duration, in seconds.

- Switching bi:
  Two-way audio switching between the handset and another device.
- Switching uni:
  Unidirectional audio switching between the handset and another device.
- Disconnect audio:
  The audio switching is disconnected in both ways.
- Connect tone:
  A tone is connected to the handset.
- Disconnect tone:
  A tone is disconnected from the handset.
- Connect conference:
  Three-party connection between the handset and two other devices.
- Connect Aux:
  An auxiliary source (VMU, message, etc.) is connected to the handset.
- Disconnect Aux:
  The auxiliary source is disconnected.
- Connect MF:
  An MF code is sent to the handset.

The following events are logged for each AP:

- Handover:
  A new handset has been associated to the AP.
- Call cut:
  A call has been lost on the AP. No answer to "keep alive" messages during the call.
- Start of saturation:
  The number of handsets in active state, located on the AP, has reached the number of handsets configured for the system. Other handsets can use this AP but it might affect quality.
- End of saturation:
  The number of handsets in active state, located on the AP, is now lower than the number of handsets configured for the system.

Structure of one line string

For easier software development and integration, all logged string events will have the same format. Each line is one event, structured as follows:

- Date and time (10 char.)
- Access Point (AP) or Handset (HS) (2 char.)
- MAC address (14 char.)
- Event string
- **Total**: about 60 characters

Examples:

22/11/06 14:25:21 HS 00:22:c2:31:ab out of coverage

22/11/06 14:25:32 HS 00:22:c2:31:ab in of coverage

File length

3 different files are saved (about 4500 traces). After that, the oldest file is deleted and replaced by the current working file. The current working file is lost in case of a system crash. All the traces are saved if there is a warm or cold restart.

Reading the log file

The file is dumped using the webdiag interface tool (httpd web server offering services to operators, installers and developers), accessible by the installer session.

The webdiag web site makes it possible to dump an archive that contains a dump of the target (log files, for instance).

5.2.1.8 AOS-W R3.1 Migration

The AOS-W 3.1 release introduces a new framework for configuring Alcatel-Lucent Access Points (APs). This chapter describes the configuration differences between pre-3.1 and the 3.1 AOS-W releases and how to upgrade your WLAN Switch running a pre-3.1 release to AOS-W 3.1.

5.2.1.8.1 Migrating to AOS-W R3.1

This section describes configuration differences between pre-3.1 and the 3.1 and later AOS-W releases.

AP Names and Groups

In previous AOS-W releases, APs were configured with location codes in the form of *building.floor.location*. In AOS-W 3.1, each AP is given an AP name and an AP group:

- For APs that were provisioned in a previous AOS-W release, the AP name defaults to *building.floor.location*.
- For APs that were not previously configured, the AP name defaults to the Ethernet MAC address of the AP in the format `xx:xx:xx:xx:xx:xx`.

  Note 1:
  You can change the name of an AP. For more information on configuring Access Points, see the AOS-W User Guide.

- Unprovisioned APs and APs with 0.0.0 location IDs initially belong to the “default” AP group. You can create additional groups as necessary, however keep in mind that an AP can belong to only one AP group at a time. For more information on configuring Access Points, see the AOS-W User Guide.

  Note 2:
  The AP-52 is not supported with the AOS-W 3.1 release. Do not upgrade to AOS-W 3.1 at this time if your network contains AP-52s.

APs in RF Plan: In RF Plan or RF Live, the AP name can be part of a fully-qualified location name (FQLN) in the format APname.floor.building.campus (the APname portion of the FQLN must be unique).

Note the following about APs that were provisioned with location IDs when you upgrade from AOS-W 2.5.x to 3.1:

- If the AP data contained in the switch’s RF Plan has a building name that corresponds to the building ID and a floor name that corresponds to the floor ID, the FQLN for the AP is automatically set after the upgrade and the AP should appear on an existing campus or building plan.
- If the AP data contained in the switch’s RF Plan does not have a building name that

corresponds to the building ID and a floor name that corresponds to the floor ID, there is no FQLN set for the AP after the upgrade. You must manually set the FQLN for the AP by clicking the AP FQLN Mapper button in RF Plan. After you set the FQLN, the AP should appear on an existing campus or building plan.

Configuration File Migration

When you boot the WLAN switch with AOS-W 3.1, the configuration file created in the AOS-W 2.5.4 (or later) is saved, then automatically migrated to a new configuration file. During the migration, the following occurs:

- The “default” profiles are populated by global configuration parameters (for example, authentication) and AP configuration parameters for location 0.0.0.
- Wildcard configurations are used to create AP groups and profiles that are assigned to them. Location *building.floor.0* configuration entries are used to create groups named “*building.floor.0*” with location *building.0.0* configurations inherited appropriately. Location building.0.0 configuration entries are used to create groups named “*building.0.0*”. Appropriate group settings are automatically programmed onto the corresponding APs.
- AP-specific configuration entries are used to create AP name-based configurations using the name “*building.floor.location*”. If an SNMP hostname is specified in the AP configuration, that name is used instead and is automatically provisioned on the AP.

The following figure is an example of a 2.5.x configuration and how the configuration will appear after the automatic migration.

2.5.x Configuration

```
ap location 1.0.0
  ageout 700
  phy-type a
    channel 64
  !
!

ap location 1.2.0
  lms-ip 10.3.4.5
!

ap location 1.2.3
  rf-band a
!
```

After Automatic Migration

```
wlan ssid-profile 1.0.0
  ageout 700
!

wlan virtual-ap 1.0.0
  ssid-profile 1.0.0
!

rf radio-profile 1.0.0
  a-channel 64
!

ap system-profile 1.2.0
  lms-ip 10.3.4.5
!

ap system-profile 1.2.3
  lms-ip 10.3.4.5
  rf-band a
!

ap-group 1.0.0
  virtual-ap 1.0.0
  dot11a-radio-profile 1.0.0
  dot11g-radio-profile 1.0.0
!

ap-group 1.2.0
  virtual-ap 1.0.0
  dot11a-radio-profile 1.0.0
  dot11g-radio-profile 1.0.0
  ap-system-profile 1.2.0
!

ap-name 1.2.3
  ap-system-profile 1.2.3
!
```

The automatic migration also causes all APs with location 1.2.x to be provisioned into group 1.2.0. All other APs with location 1.x.x are provisioned into group 1.0.0.

Mapping of Show Commands

The CLI command **show command-mapping** maps AOS-W 3.1 to AOS-W 2.5.x commands, as shown in the following table. Use the **reverse** option to display 2.5.x to 3.1 command mapping.

table 5.54 : Command Map

New Command	Old Command
show ap active	show wlan ap
show ap arm neighbours	show ap arm-neighbours
show ap arm rf-summary	show am rf-summary
show ap arm scan-times	show am scan-times
show ap arm state	show wlan arm
show ap association	show stm association
	show wlan client
	show wlan remote-client
show ap blacklist-clients	show stm dos-sta
show ap bss-table	show stm connectivity
show ap client status	show stm state
show ap coverage-holes	show rfsm coverage-holes
show ap database	show ap global-list
	show sapm ap search
	show ap registered
show ap debug association-failure	show wlan association-failure
show ap debug bss-config	show stm ap-config
show ap debug bss-stats	show ap detailed-stats
show ap debug client-mgmt-counters	show stm counters
show ap debug client-stats	show ap detailed-stats
show ap debug client-table	show ap status
show ap debug counters	show sapm counters
show ap debug datapath	show stm hidden-essid
show ap debug driver-log	show ap status
show ap debug log	show ap debug-log
show ap debug mgmt-frames	show stm packets
show ap debug radio-stats	show ap detailed-stats
show ap debug received-config	show ap received-config
show ap debug system-status	show ap status
show ap debug trace-addr	show stm trace-addr
show ap essid	show wlan essid
show ap licence-usage	show wlan licence-usage
show ap load-balancing	show rfsm load-balance
show ap monitor active-laser-beams	show am active-laser-beams
show ap monitor ap-list	show am ap-search
show ap monitor arp-cache	show am arp-cache
show ap monitor association	show am association

New Command	Old Command
show ap monitor channel	show am channel
show ap monitor client-list	show am sta-search
show ap monitor debug counters	show am counters
show ap monitor debug status	show am status
show ap monitor ids-state	show am ids-state
show ap monitor pot-ap-list	show am pot-ap-list
show ap monitor pot-client-list	show am pot-sta-list
show ap monitor stats	show am stats
show ap monitor stats advanced	show am state
show ap monitor wired-mac	show am wired-mac
show ap pcap status	show pcap status
show ap provisioning	NEW
show ap remote association	show stm ap association
show ap remote bridge-table	show ap bridge-table
show ap remote counters	show stm ap counters
show ap remote debug mgmt-frames	show stm ap packets
show ap tech-support	show ap-tech-support
show ap vlan-usage	show wlan vlan-usage
provision-ap	program-ap
show provisioning-params	show ap-params

Command Changes

Removed Commands

The following AOS-W 2.5.x AP commands do not exist in 3.1:

Commands removed in 3.1	Use the following commands instead
ap location	ap-group
	ap-name
show ap config location	show ap config ap-group
	show ap config ap-name
	show ap config bssid
show ap locations	show ap-group
	show ap-name
show ap node-config location	N/A
show enet1-config location	show ap enet-link-profile
show enet1-effective-config location	N/A

Commands removed in 3.1	Use the following commands instead
show ap snmp location	show ap snmp-profile
	show ap snmp-user-profile
show ap keys location	N/A

Replaced Commands

The following AOS-W 2.5.x commands are replaced with the new **show ap database** command:

- **show ap global-list**
- **show ap registered**
- **show sapm ap search**

Modified Commands

The **show log** command includes the following new options:

- **ap-debug**
- **bssid-debug**
- **errorlog**
- **essid-debug**
- **network**
- **security**
- **system**
- **user**
- **user-debug**
- **wireless**

The AOS-W 2.5.x **show log** command options are available with the **show trace** command.

New Parameters for **apboot** Command

When issuing the apboot command, you can now specify the following additional parameters:

- **all** to reboot all APs connected to this switch. You can optionally specify **global** to reboot APs on all switches, or **local** to reboot APs registered on the switch on which you entered the **apboot** command.
- **ap-name *name*** to reboot the specified AP.

  Note 1:
  *If you are rebooting an AP after changing its name, use the "old" name for the AP with the **apboot** command.*
- **ap-group *name*** to reboot APs in the specified group. You can optionally specify global to reboot APs on all switches, or local to reboot APs registered on the switch on which you entered the **apboot** command.

  Note 2:
  If you are rebooting APs after assigning them to a new group, use the "old" AP group name.

WLAN Switch Country-Specific Code

Beginning with 3.1, the country code is saved to the hardware and, for certain countries, cannot be changed. If you upgrade to this release in the United States or Israel, the WLAN switch is restricted to operating only in these countries.

The country code determines the 802.11 wireless transmission spectrum in with the WLAN switch operates. Most countries impose penalties and sanctions for operators of wireless networks with devices set to improper transmission spectrums.

Note:

Before upgrading to 3.1, make sure the correct country code is saved in the configuration file. For more information, see *§ Installing AOS-W 3.1* *.*

Feature-Specific Differences

Note:

The AP-52 is not supported with the AOS-W 3.1 release. Do not upgrade to AOS-W 3.1 at this time if your network contains AP-52s.

Captive Portal

In AOS-W 2.5.2 and later 2.5.x releases, captive portal users in the base operating system are placed into the predefined *cpbase* initial user role before authentication. The *cpbase* role is not supported in AOS-W 3.1. You need to create captive portal authentication profiles in the base operating system, as described in “Configuring Captive Portal” in Volume 4 of the AOS-W User Guide. Creating a captive portal authentication profile automatically generates the required policies and role.

In 3.1, the captive portal authentication profile instance is configured for a user role. The user role can be the logon user role, a role that is configured for that SSID, or a role that is derived from user or server derivation rules. You must manually apply the captive portal authentication profile to a user role.

IP Mobility

There is no migration of AOS-W 2.5.x mobility features to mobility domain configuration; all previously-configured layer-3 mobility configuration will be lost.

Mobility is disabled by default on WLAN switches in 3.1. You must explicitly enable and configure mobility domains as described in “Configuring IP Mobility” in the AOS-W User Guide.

Server Derivation Rules

In 3.1, you configure server rules for a server group and not for individual servers. If you configured server rules for specific servers in 2.5.x releases, the server rules are automatically applied to all servers in the server group in 3.1.

User Roles and Policies

User role policies that reference specific location codes (building.floor.location) in 2.5.x releases must be manually reconfigured for an AP group, since there is no automatic mapping of location IDs to an AP group.

Mobility Manager Configuration Management

AOS-W 3.1 introduces support in the WLAN switch for configuration management by the OmniVista Mobility Manager System 2.0. Your WLAN switch must be running 3.1 or later, and your OVMM server or OmniVista Mobility Manager Appliance must be running release 2.0 or later. OVMM configuration management is not supported in pre-3.1 releases.

On the master WLAN switch, you configure the IP address of the OVMM server and an SNMP username and password for the OVMM server to use to communicate with the WLAN switch. To support configuration by the OVMM server, you must enable the master WLAN switch to receive, apply, and communicate the status of configuration changes with the OVMM server (this is disabled by default).

For more information about configuring a master WLAN switch for OVMM, see “Alcatel Mobility Manager System” in Chapter 18, “Configuring Management Access” in the AOS-W User Guide for 3.1.

Voice Services Module Licence

AOS-W 3.1 introduces the Voice Services Module license for many voice-related features. This licence must be installed in the WLAN switch and is available for each Alcatel-Lucent WLAN switch model or supervisor card.

The following features available in 2.5.x now require the Voice Services Module licence:

- Call admission control for SIP, SCCP, Vocera, SVP, and NOE
- Active VoIP load balancing and disconnect of excess calls options in the CAC profile
- Voice-aware ARM scanning
- Automatic assignment of voice traffic to high-priority queues without a PEF licence

Note:
When the PEF licence is installed in the WLAN switch, you can permit/deny or assign queues for voice traffic in a session ACL even if the Voice Services Module licence is not present.

See the AOS-W 3.1 Release Notes for information about new features available with the Voice Services Module licence.

Client Blacklisting

AOS-W 3.1 allows you to enable automatic client blacklisting specifically for spoofed deauthentication, as seen with “man-in-the-middle” attacks; you enable this blacklisting in the IDS DoS profile. Automatic client blacklisting due to other reasons is enabled by default in the virtual AP profile. The virtual AP profile also allows you to configure both the amount of time that a client is blacklisted due to authentication failure and the amount of time that a client is blacklisted due to other reasons.

Adaptive Radio Management (ARM) and Calibration

Previous AOS-W releases support two methods for calibrating and managing radio settings for the wireless network: through Adaptive Radio Management (ARM) or through site survey calibration run on a per-building, per-ratio type basis. With the 3.1 release, only ARM is supported.

For new installations, the Adaptive Radio Management (ARM) feature for single-band radio assignment is enabled by default. If you were running an earlier version of AOS-W with ARM disabled, ARM remains disabled when you upgrade to this release. If you were running radio calibration in a previous release, you now need to use ARM.

Predefined Management User Roles

With AOS-W 3.1, there are predefined roles that can be assigned to management users:

- root: superuser role
- guest-provisioning: allows for guest provisioning only
- read-only: allows execution of read-only commands

If you previously configured a management user with a user role that is not one of the above predefined roles, you need to reconfigure the management user to use one of the predefined roles. Use either the **Configuration > Management > Administration** page in the WebUI or the **mgmt-user** CLI command.

Syslog Processor

With AOS-W 3.1, the ESI feature is expanded to support a more flexible message parser. If you previously used ESI to process messages from a Fortinet antivirus firewall device, you need to reconfigure the ESI rules for the expanded syslog processor capabilities:

1. Define the syslog processor domain. For example, in the following command, ***ipaddr*** is the IP address of the Fortinet syslog source:

   ```
   esi parser domain fortinet
   server < ipaddr >
   ```

2. Define the syslog processor rule. For example:

   ```
   esi parser rule forti_rule
   condition "log_id=[0-9]{10}[ ]"
   match ipaddr "src=(.*)[ ]"
   set blacklist
   domain fortinet
   enable
   ```

See the “External Services Interface” chapter in the AOS-W 3.1 User Guide for more information.

Per-SSID RADIUS Server Selection

With 2.x releases, you can specify the “match ESSID” option when configuring RADIUS servers. This allows authentication server selection on a per-SSID basis. With AOS-W 3.1, you configure this function with profiles: configure the authentication server group, select the authentication server group in the AAA profile, then map the AAA profile to a virtual AP profile.

AOS-W 3.0 Station Management Profile Deprecated

With AOS-W 3.1, the station management profile introduced in AOS-W 3.0 is deprecated. Most of the parameters that were in the station management profile are now configured in the virtual AP profile, as shown in the following table.

3.0 Station Management parameter	**3.1 Parameter**	**3.1 Profile**	**3.1 Default Value**
DoS Prevention	DoS Prevention	Virtual AP	disabled
Station DoS Prevention[1]	Blacklist	Virtual AP	enabled

3.0 Station Management parameter	3.1 Parameter	3.1 Profile	3.1 Default Value
	Spoofed Deauth Blacklist	IDS Denial of Service	disabled
Station DoS Block Time	Blacklist Time	Virtual AP	3600 seconds
Auth Failure Block Time	Authentication Failure Blacklist Time	Virtual AP	0 seconds
Fast Roaming	Fast Roaming	Virtual AP	disabled
Strict Compliance	Strict Compliance	Virtual AP	disabled
Vlan Mobility	VLAN Mobility	Virtual AP	disabled

[1] *This release allows you to enable automatic client blacklisting specifically for spoofed deauthentication attacks; see § Client Blacklisting .*

If you changed the default values in the station management profile, you need to re-enter them after updating to this release.

5.2.1.8.2 Before Upgrading

Note:

Before upgrading your WLAN switch, review the configuration changes for AOS-W 3; see § Migrating to AOS-W R3.1 . Also, review the "Known Issues and Limitations" section in the AOS-W 3.1 Release Notes for upgrade issues.

Verify the Configured Country Code

With AOS-W 3.1, the country code is saved to the hardware and cannot be changed for certain countries. Before upgrading to 3.1, make sure the correct country code is saved in the WLAN switch's configuration file.

To verify the country code using the CLI, use the following command in enable mode:

```
(alcatel) # show startup-config | include country
```

If the country code is correct, proceed with the upgrade. Remember that you must have AOS-W 2.5.4 or later installed on the WLAN switch before you upgrade to AOS-W 3.1.

If the country code is incorrect, disable master-local WLAN switch updates by either disconnecting the local WLAN switch link or increasing the heartbeat value to a large interval (for example, use the CLI command **cfgm set heartbeat 100000**).

You have the following options to correct the country code before upgrading to AOS-W 3.1:

- Restore the WLAN switch to its factory defaults and perform a fresh manual configuration. This method is recommended for switches where there is a minimum amount of configuration required, for example, a local switch that downloads most of its configuration from a master switch.
- Send the Compact Flash backup file to Alcatel-Lucent Technical Support, along with the country to be configured. Technical Support will send back a revised file which you then restore to the switch.

The following sections describe the steps for each option.

Restore the WLAN Switch to Factory Defaults and Reconfigure

Complete the following steps to modify the country code and perform a fresh configuration on the WLAN switch. After configuring the switch, proceed to the steps in § Upgrading to AOS-W 3.1 .

To restore the WLAN Switch to factory defaults using the WebUI:

1. Backup the current configuration; see § Backing up Critical Data .
2. Disconnect the WLAN switch from the network.
3. Reset the WLAN switch. Navigate to the **Maintenance > Switch > Clear Config** page.
4. Click **Continue**.
   This returns the WLAN switch to its factory defaults and reboots it with the default IP address 172.16.0.254.
5. Run the Initial Setup.
   During the Initial Setup, specify the country code for the country in which the WLAN switch will operate. After completing the setup, the switch reboots with the new country code. See the AOS-W 3.1 Quick Start Guide for information about running the Initial Setup.
6. When the boot process is complete, verify the country code; see § Verify the Configured Country Code .
   If the country code is incorrect, contact Alcatel-Lucent customer support
   If the country code is correct, reconnect the WLAN switch to the network and reconfigure the WLAN switch.

To restore the WLAN Switch to factory defaults using the CLI:

1. Backup the current configuration, see § Backing up Critical Data .
2. Disconnect the WLAN switch from the network.
3. Reset and reboot the WLAN switch, using the following command sequence:

```
(alcatel) # write erase
All the configuration will be deleted. Press 'y' to proceed: y
(alcatel) # reload
Do you really want to reset the system(y/n): y
```

   This returns the WLAN switch to its factory defaults and reboots it with the default IP address 172.16.0.254.
4. Run the Initial Setup.
   During the Initial Setup, specify the country code for the country in which the WLAN switch will operate. After completing the setup, the WLAN switch reboots with the new country code. See the AOS-W 3.1 Quick Start Guide for information about running the Initial Setup.
5. When the boot process is complete, verify the country code.
   If the country code is incorrect, contact Alcatel-Lucent customer support.
   If the country code is correct, reconnect the WLAN switch to the network and reconfigure the WLAN switch.

Send the Compact Flash Backup File to Technical Support

Back up the entire Compact Flash file system to the `flashbackup.tar.gz` file. Send the file to Alcatel-Lucent Technical Support, along with the country to be set. Technical Support will

send back a revised `flashbackup.tar.gz` file, which you then restore to the WLAN switch. See backup and restore instructions in § Backing up Critical Data . After you restore the Compact Flash file system, proceed to the instructions in § Upgrading to AOS-W 3.1 .

5.2.1.8.3 Upgrading to AOS-W 3.1

Note 1:

If you are currently running AirOS or AOS-W 2.4.x on your WLAN switch, you must upgrade the WLAN switch image to AOS-W 2.5.4 or later before you upgrade the WLAN switch to AOS-W 3.1. Upgrading from 2.4.x directly to 3.1 is not supported.

Note 2:

Before upgrading to AOS-W 3.1 make sure the correct country code is saved in the configuration file. See § Verify the Configured Country Code .

Depending on the size and complexity of your configuration, you may want to start over with a fresh configuration when upgrading to 3.1, rather than migrating your existing configuration. Contact Alcatel-Lucent Customer Support for assistance.

Managing Flash Memory

All Alcatel-Lucent WLAN switches store critical configuration data on an onboard compact flash memory module. To maintain the reliability of your Alcatel-Lucent WLAN network, Alcatel-Lucent recommends the following general best practices with respect to the use of your Alcatel-Lucent WLAN switch and its compact flash memory.

Be careful not to exceed the size of the flash file system. For example, loading multiple large building JPEGs for RF Plan can consume flash space quickly. Warning messages alert you that the file system is running out of space if there is a write attempt to flash and 5 Mbytes or less of space remains.

Other tasks which are sensitive to insufficient flash file system space include:

- Using the internal database. DHCP lease and renew information is also stored in flash. If the file system is full, DHCP addresses will not be distributed or renewed.
- If an Alcatel-Lucent WLAN switch encounters a problem and it needs to write a core file, it will not be able to do so if the file system is full and critical troubleshooting information will be lost.

Prerequisites

You should ensure the following before installing a new image on the WLAN switch:

- Make sure you have at least 10 MB of free compact flash space.
- Remove all unnecessary saved files from flash.
- Run the **tar crash** command to make sure that there are no "process died" files clogging up memory and TFTP the files off the WLAN switch.

Backing up Critical Data

It is important to back up frequently all critical configuration data and files on the compact flash file system to an external server or mass storage facility. At the very least, you should include the following files in these frequent backups:

- Configuration data
- WMS database

- Local user database
- Licencing database
- Floor plan JPEGs
- Customer captive portal pages
- Customer x.509 certificates

All the above files reside on the compact flash file system on the Alcatel-Lucent WLAN switch.

If supported on your current AOS-W image, the WebUI provides the easiest way to back up and restore the entire Compact Flash file system.

To back up and restore the Compact Flash File system using the WebUI:

1. Navigate to the **Maintenance > File > Backup Flash** page.
2. Click **Create Backup** to back up the contents of the Compact Flash file system to the file `flashbackup.tar.gz`.
3. Click **Copy Backup** to copy the file to an external server.
   You can later copy the backup file from the external server to the Compact Flash file system. To restore the revised `flashbackup.tar.gz` file:
4. Copy the backup file from an external server to the Compact Flash file system by navigating to the **Maintenance > File > Copy Files** page.
5. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page. Click **Restore**.

To back up and restore the entire Compact Flash file system using the CLI:

1. Enter **enable** mode in the CLI on the WLAN switch. Use the **backup** command to back up the contents of the Compact Flash file system to the file `flashbackup.tar.gz`:

```
(alcatel) # backup flash
Please wait while we tar relevant files from flash...
Please wait while we compress the tar file...
Checking for free space on flash...
Copying file to flash...
File flashbackup.tar.gz created successfully on flash.
Please copy it out of the switch and delete it when done.
```

2. Use the **copy** command to transfer the backup flash file to an external server:

```
(alcatel) # copy flash: flashbackup.tar.gz tftp: <TFTP Server IP address> <filename>
```

3. You can later transfer the backup flash file from the external server to the Compact Flash file system with the **copy** command:

```
(alcatel) # copy tftp: <TFTP Server IP address> <filename> flash: flashbackup.tar.gz
```

4. Use the **restore** command to untar and uncompress the flashbackup.tar.gz file to the Compact Flash file system:

```
(alcatel) # restore flash
```

Installing AOS-W 3.1

Caution:

When upgrading the software in a multi-WLAN switch network (one that uses two or more Alcatel-Lucent WLAN switches), special care must be taken to upgrade all the WLAN switches in the network and to upgrade them in the proper sequence. See § Upgrading Multi-WLAN Switch Networks .

Obtain the latest, valid Alcatel-Lucent WLAN switch software image from the Alcatel-Lucent Customer Support website. Back up your current WLAN switch configuration and data files, as described in § Backing up Critical Data .

Alcatel-Lucent recommends scheduling network downtime when upgrading your WLAN switches to AOS-W 3.1.

Note 1:

The most current Alcatel-Lucent Mobility WLAN switch software image may be newer than that available at the time these release notes were written. Alcatel-Lucent recommends that you always download the latest software image from Alcatel-Lucent Customer Support before proceeding with these installation instructions.

The following steps describe how to install the AOS-W software image from a PC or workstation using the WebUI on the WLAN switch. (You can also install the software image from a TFTP or FTP server using the same WebUI page.)

To use the WebUI to install the software image:

1. Upload the new software image to a PC or workstation on your network.
2. Log in to the WebUI from the PC or workstation.
3. Navigate to the **Maintenance > Switch > Image Management** page.
4. Select the Upload Local File option, then click the Browse button to navigate to the image file on your PC or workstation.
5. Determine which memory partition will be used to hold the new software image. It is recommended to load the new image into the backup partition. (To see the current boot partition, navigate to the **Maintenance > Switch > Boot Parameters** page.)
6. Select **Yes** for Reboot Switch After Upgrade.
7. Click **Upgrade**.
8. When the software image is uploaded to the WLAN switch, a popup appears. Click **OK** in the popup window. The boot process starts automatically within a few seconds (unless you cancel it).
9. When the boot process is complete, log in to the WebUI and navigate to the **Monitoring > Switch > Switch Summary** page to verify the upgrade, including country code. The Country field displays the country code configured on the WLAN switch.

The following steps describe how to install the AOS-W software image using the CLI on the WLAN switch. You need to have a TFTP server on your network from which the image will be downloaded to the WLAN switch.

To use the CLI to install the software image:

1. Upload the new software image to a TFTP server on your network.
2. From the CLI on the WLAN switch, verify the network connection from the target WLAN switch to the TFTP server:

```
(alcatel) # ping <TFTP server IP address>
```

Note 2:
*A valid IP route must exist between the TFTP server and the WLAN switch. Also required, a place-holder file with the destination filename and proper write permissions must exist on the TFTP server prior to executing the **copy** command.*

3. Determine which memory partition will be used to hold the new software image. Use the **show image version** command to check the memory partitions. The following figure shows an example of the output of the **show image version** command.

```
(alcatel) # show image version
---------------------------------
Partition               : 0:0 (/dev/hda1) **Default boot**
Software Version        : AOS-W 2.5.4.1
Build number            : 13515
Label                   : 13515
Built on                : 2006-10-24 13:22:04 PDT
---------------------------------
Partition               : 0:1 (/dev/hda2)
/dev/hda2: Image not present
---------------------------------
Partition               : 1:0 (/dev/hdc1)
Not plugged in.
---------------------------------
Partition               : 1:1 (/dev/hdc2)
Not plugged in.
```

Alcatel-Lucent recommends loading the new image into the backup partition. In the above example, partition 0 contains the active image. Partition 1 is empty (image not present) and can be used for loading the new software.

4. Use the **copy** command to load the new image into the Alcatel-Lucent WLAN switch:

   ```
   (alcatel) # copy tftp: <server address> <image filename> system: partition {0|1}
   ```

   Note 3:
   *When using the **copy** command to load a software image, the specified partition automatically becomes active the next time the WLAN switch is rebooted. There is no need to manually select the partition.*

5. Verify that the new image is loaded:

   ```
   (alcatel) # show image version
   ```

   Information about the newly loaded software image should be displayed for the appropriate partition.

6. Reboot the WLAN switch:

   ```
   (alcatel) # reload
   ```

7. When the boot process is complete, use the **show version** command to verify the upgrade. The following figure shows an example of the output of the **show version** command.

```
(alcatel) #show version
Alcatel Operating System Software.
AOS-W (MODEL: OAW-4324-US), Version 3.1.0.0
Website: http://www.alcatel.com/enterprise
Copyright (c) 2002-2007, Alcatel.
Compiled on 2007-01-30 at 03:10:13 PST (build 14050) by p4build

ROM: System Bootstrap, Version CPBoot 1.1.6 (Aug  9 2004 - 11:56:58)

Switch uptime is 2 days 3 hours 44 minutes 5 seconds
Reboot Cause: User reboot.
Supervisor Card
Processor (revision 16.20 (pvr 8081 1014)) with 256M bytes of memory.
32K bytes of non-volatile configuration memory.
256M bytes of Supervisor Card System flash (model=CF 256MB).
(aruba) #
```

In this example, version 3.1 is loaded and running, indicating that the upgrade is complete.

5.2.1.8.4 Upgrading Multi-WLAN Switch Networks

In a multi-WLAN switch network (a network with two or more WLAN switches), special care must be taken to upgrade all WLAN switches in the proper sequence, based on the WLAN switch type (master or local). Be sure to back up all WLAN switches being upgraded, as described in § Before Upgrading .

Note:

For proper operation, all WLAN switches in the network must be upgraded to use the same version of AOS-W software. For redundant (VRRP) environments, the WLAN switches should be the same model.

To upgrade an existing multi-WLAN switch system to AOS-W 3.1:

1. Load the 3.1 software image onto all switches (including redundant master switches).
2. Reload all switches at the same time.

5.2.1.8.5 Reverting to AOS-W 2.5.4 or Later

If necessary, you can to return to AOS-W 2.5.4 or later software after upgrading to AOS-W 3.1. Be sure to back up your WLAN switch before reverting the OS. Also import the local database and the WMS database.

Caution:

When reverting the WLAN switch software, whenever possible use the previous version of soft-

ware known to be used on the system. Loading a different prior release not specifically confirmed to operate in your environment could result in an improper configuration.

To revert to AOS-W 2.5.4 or later:

1. Use the **show boot** command to determine the name of the current configuration file:

   ```
   (alcatel) # show boot
   Config File: default.cfg
   Boot Partition: PARTITION 1
   ```

   In this example, `default.cfg` is the name of the configuration file.

2. Determine where your backup software is stored. Use the **show image ver** command to check the memory partitions. The following figure shows an example of the output of the **show image ver** command.

```
(alcatel) #show image ver
---------------------------------
Partition               : 0:0 (/dev/hda1)
Software Version        : AOS-W 2.5.4.1
Build number            : 13515
Label                   : 13515
Built on                : 2006-10-24 13:22:04 PDT
---------------------------------
Partition               : 0:1 (/dev/hda2) **Default boot**
Software Version        : AOS-W 3.1.0.0
Build number            : 14050
Label                   : 14050
Built on                : 2007-01-26 02:22:50 PST
---------------------------------
Partition               : 1:0 (/dev/hdc1)
Not plugged in.
---------------------------------
Partition               : 1:1 (/dev/hdc2)
Not plugged in.
```

   In this example, partition 0 contains the release 2.5.4.1 backup. Partition 1, the active partition, contains the AOS-W 3.1 image.

   To select the backup partition as the new boot partition:

   ```
   # boot system partition 0
   ```

3. If you have your backup configuration file on an external TFTP server, use the following command to copy it to the WLAN switch:

   ```
   # copy tftp: <TFTP server IP address> <backup filename> flash: <backup configuration filename>
   ```

4. Boot with your backup file as you cannot overwrite the active configuration file.

```
# boot config <backup configuration filename>
```

5. Replace the current configuration file with your backup.

   ```
   # copy flash: <backup configuration filename> flash: default.cfg
   ```

6. Boot with your `default.cfg` file.

   ```
   # boot config <default.cfg>
   ```

7. Replace the current WMS database file with your backup.

   If you have your backup database file on an external TFTP server, use the following commands to import it:

   ```
   # copy tftp: <TFTP server IP address> <backup wms filename> flash: <wms filename>
   # wms import-db <wms filename>
   ```

   If no backup image is present, load one:

   ```
   # copy tftp: <server address> <image filename> system: partition {0|1}
   ```

8. Select the backup partition as the new boot partition:

   ```
   # boot system partition {0|1}
   ```

9. Reboot the WLAN switch:

   ```
   # reload
   ```

10. When the boot process is complete, verify that the WLAN switch is using the correct software:

    ```
    # show version
    ```

5.2.1.8.6 Troubleshooting

If there is trouble with the WLAN switch (for example, there is less than 10 MB of flash space), do the following:

1. Disconnect the link to the APs.
2. Remove all unnecessary files from flash, including the `db_dump.sql` type files.
3. Remove any crash files.
4. Import the old wms DB file and reboot.
5. Reconnect the link for the APs.

Before you place a call to Technical Support, please follow these steps:

1. Provide a detailed network topology (including all the devices in the network between the user and the OmniAccess WLAN switch with IP addresses and Interface numbers if possible).

   The diagram can be a Visio, PowerPoint, JPEG, TIF, etc. file, or it can even be hand written and faxed to Technical Support.

2. Provide the WLAN switch logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
3. Provide the syslog server file of the WLAN switch at the time of the problem.

   Alcatel-Lucent strongly recommends that you consider adding a syslog server if you do not already have one to capture logs of the WLAN switch.

4. Let the support person taking your call know if this is a new or existing installation. This

helps the support team to determine the troubleshooting approach, depending on whether you have:

- An outage in a network that worked in the past.
- A network configuration that has never worked.
- A brand new installation.

5. Let the support person know if anything has recently changed in your network (external to the OmniAccess system), or if anything has recently been changed in the WLAN switch or AP configuration.
6. If there was a configuration change, list the exact configuration steps and commands used.
7. Provide the date and time (if possible) when the problem first occurred.
8. If the problem is reproducible, list the exact steps taken to recreate the problem.
9. Provide any wired or wireless Sniffer traces taken during the time of the problem.
10. Provide the wireless device's make and model number, OS version (including any service packs or patches), wireless NIC make and model number, wireless NIC's driver date and version, and the wireless NIC's configuration.
11. Provide the WLAN switch site access information, if possible.

    Alcatel-Lucent recommends that access to your site should only be enabled when a problem occurs, and that access be restricted to a VPN (PPTP, L2TP, SSL) connection that limits the support person to only have IP access to the WLAN switch. Alternatively, limit access methods to analog dialup to the WLAN switch or SSH access to a device that the support person can then telnet to the WLAN switch.

5.2.2 IPTouch 310/610 WLAN Handset

5.2.2.1 Description

The Alcatel-Lucent IP Touch 310/610 WLAN Handsets are designed for mobile workplace use within a facility using 802.11 Access Points in a wireless LAN. The 310 and 610 handsets give users the freedom to roam throughout the workplace while providing the voice over IP features and functionality of the PCX.

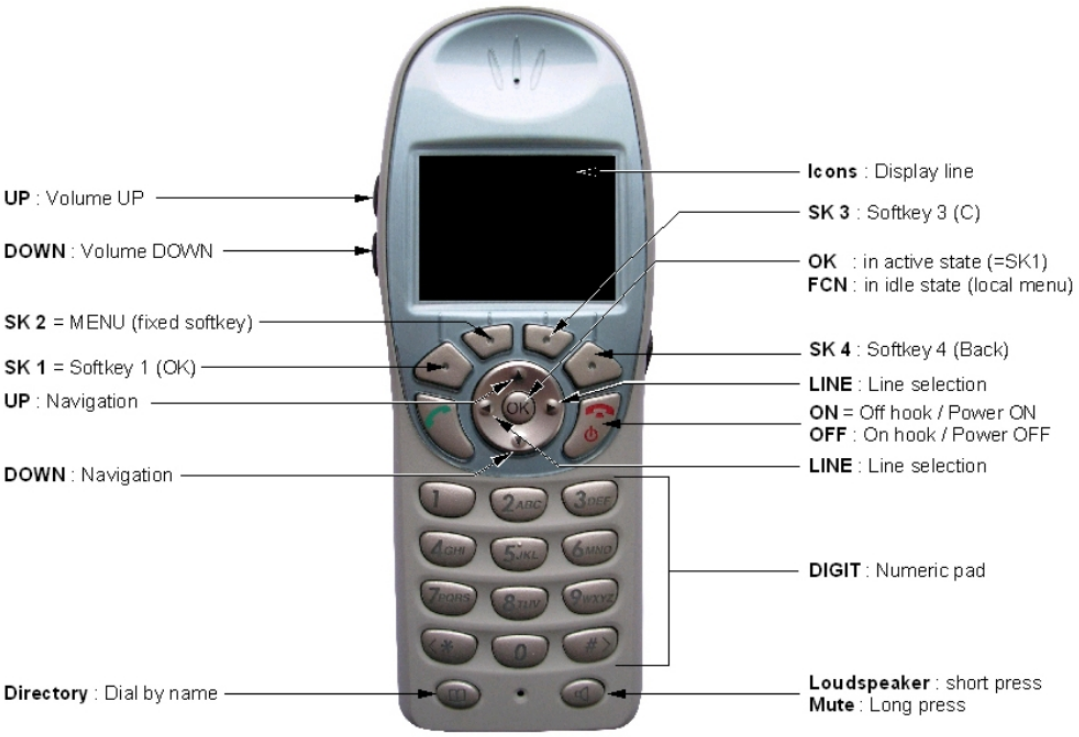


Figure 5.72 : Alcatel-Lucent IP Touch 310/610 WLAN Handsets

5.2.2.1.1 Specifications

The following table presents the main specifications and features of the 310 and 610 handsets.

Radio frequency (selectable)	- 802.11a: 5.150–5.825 GHz - 802.11b, 802.11g: 2,4-2,4835 GHz
Transmission type	- 802.11a, 802.11g: Orthogonal Frequency-Division Multiplexing (OFDM) - 802.11b: Direct Sequence Spread Spectrum (DSSS)
Transmit power	Up to 100 mW (configurable), less than1 mW on average, depending on the radio frequency
Transmit data rate	Up to 54 Mb/s
Radio QoS	- With Spectralink Voice Priority (SVP) server: Spectralink Radio Protocol, Timed Delivery, Spectralink CAC - Without SVP server: WiFi Multimedia (WMM), U-APSD, Tspec
Wireless security	- Wired Equivalent Privacy (WEP) as defined by the 802.11 specification with both 40-bit and 128-bit encryption - Wi-Fi Protected Access (WPA and WPA2) in the pre-shared key (PSK) mode as defined in the 802.11i protocol - Cisco FSR

FCC certification	Part 15.247
Management	Software download using TFTP
Voice encoding	G.711, G.729a/ab
VoIP Protocol	Alcatel-Lucent New Office Environment (NOE)
Dimensions and weight:	310 handset: - 13.7 x 5.1 x 2.3 cm (5.4" x 2.0" x 0.9") - 110.6 g (3.9 oz.) with Standard Battery Pack 610 handset: - 14,5 x 5.1 x 2.3 cm (5,7" x 2.0" x 0.9") - 119.1 g. (4.2 oz.) with Standard Battery Pack
Display	- Up to four lines of text, plus an icon status row, and a row for softkey labels - Display of 256 Latin characters, plus Greek and Cyrillic Unicode characters - Supported languages: French, English, Spanish, German, Dutch, Portuguese, Italian, and Greek - Monochrome display - Green backlight: The backlight comes on when the user presses a key (even if the keypad is locked) or when there is an incoming call. The backlight turns off after 10 seconds of inactivity (no key is pressed)

Note:
The Alcatel-Lucent IP Touch 310/610 WLAN Handsets do not support H.323 Voice over IP signaling protocol.

5.2.2.1.2 Keys

The following table lists the handset keys and their functions (see figure : Alcatel-Lucent IP Touch 310/610 WLAN Handsets).

Key	Function
Volume up **Volume down**	While the handset is in conversation, increases/decreases the headset/handset speaker volume. While in standby, increases/decreases the loudspeaker/ring volume.
Softkeys (4)	Select commands in the Admin and Local menus. For more information on softkey functions, see module IP Touch 310/610 WLAN Handset - Configuration § Navigating the menus . Softkey labels appear on the bottom line of text of the display, just above the softkeys. When the handset is in standby, the second softkey from the left acts as the Menu key, giving access to the PCX-specific menu.
TALK	Activates Push-to-talk mode (610 handset only).
START	Answers an incoming call. Starts an outgoing call after dialling.
Directory	Accesses the Dial by name feature with one short press.

Key	Function
Speakerphone/Mute	Activates/deactivates the speakerphone with one short press. Answers an incoming call. Starts an outgoing call after dialling. While in conversation, activates/deactivates muting of the microphone with one long press.
Keypad	Emulates an alphanumeric keyboard when alphanumeric emulation is active. Each press on a digit key lets the user select a digit or a letter successively. The first press selects the first choice, the second press on the same key within an elapsed time selects the second choice, and so on. When alphanumeric emulation is not active, a key press selects digits only (0-9, # and *).
Nav keys	Select the current line and move the cursor left and right.
END	Powers on the handset. While in conversation, ends the current call (hangs up). While ringing, silences ringing or vibrating with one short press without interrupting the call. Turns off the handset with long press.
NavOK	While handset is in standby, accesses the Local configuration menu. Validates choices and options while using Local and Admin menus.

5.2.2.1.3 Indicator icons

The following table shows the icons displayed on the top line of the display and their meanings.

Icon	Meaning
	The amount of charge remaining in the battery. *Note:* *When only one bar remains, the battery needs to be charged.*
	The loudspeaker is active.
	Normal radio signal strength. The user has normal radio field coverage. The radio signal strength icons assist the user in determining if the handset is moving out-of-range.

Icon	Meaning
	Weak radio signal strength. The user has weak radio field coverage and may have audio problems, such as gaps in communication or sizzling sound.
	Out of coverage radio signal strength. If the user moves outside the covered area during a call, the handset will recover the call if the user moves back into range within 10 seconds. At the end of the 10 seconds, if the handset has not found a suitable Access Point, it displays, the message “No Net Found, No APs”. The user hears the "out of service" unhappy tone after which the handset restarts. This warning tone, along with the other warning tones in the handset, can be disabled in the Admin menu.
	The keypad is locked to prevent accidental activation.
	The handset is downloading code or determining if downloading is necessary. This icon appears during the initialization phase. A progression bar appears while the handset is running over-the-air downloader
	The vibrator is enabled.
	The microphone is not transmitting sound. Press the **Speakerphone/Mute** key again (long press) to un-mute the microphone.
	The handset is locked by the user.
	An appointment is programmed and the PCX will call the handset when the appointment time arrives (PCX feature).
	Calls are forwarded (PCX feature).
	A text or voice message is waiting in the inbox (PCX feature).
	Up and down arrows are displayed when the Local menu has additional options above or below. Left or right arrows are displayed during editing when the cursor may be moved left or right.

5.2.2.1.4 Power

Power is supplied by a Lithium Ion. Three Battery Packs are available, providing different capacity levels. The Battery Packs are interchangeable:

- Standard Battery Pack capacity 4 hours talk, up to 80 hours standby, approximately 2 hours charge time

- Extended Battery Pack capacity 6 hours talk, up to 120 hours standby, approximately 4 hours charge time
- Ultra-Extended Battery Pack capacity 8 hours talk, up to 160 hours standby, approximately 6 hours charge time

The battery icon indicates approximate remaining battery life. The handset notifies the user when the battery becomes low. When there is approximately 15-30 minutes of battery life left:

- If in conversation, the handset emits a soft beep in the earpiece every 30 seconds. The alerts increase to every 6 seconds when there is about 1 minute of battery life left.
- If in standby, the handset displays the Very Low Battery icon with the message “Battery low” (in English) and beeps every 20 seconds.

The handset cannot be used until the battery starts to recharge. If the battery is empty, the handset turns off and is not operational.

Charging starts as soon as the user inserts the handset in the charger. The handset remains operational through the speakerphone during charging. If the handset is in standby, it displays the extension number and the message `Charging…` (in English) and will ring if called. If the handset is powered off, it displays only the message `Charging...`, and will not receive calls. When the battery is fully charged, the handset displays the message `Charging complete`.

Note:

The handset does not display charging information during a call.

5.2.2.1.5 Startup sequence

To power on the handset, press the **END** key.

The handset steps through an initialization sequence. It displays the line icons 1-9 and counts down the steps of the sequence. If an error occurs that prevents initialization from continuing, the handset displays an error message and leaves the related number icon(s) on.

For more information on how to handle error messages that occur during initialization, see module IP Touch 310/610 WLAN Handset - Maintenance § Status messages .

The following table shows what happens at different steps in the initialization sequence.

Icon display	**The icon shown in bold turns off when...**
123 5 78**9**	The handset locates, authenticates and associates with at least one Access Point and proceeds to bring up higher-layer networking functions.
123 5 7**8**	If DHCP is configured, the DHCP discovery process starts.
123 5 **7**	If DHCP is configured, the handset receives a DHCP response confirming the configuration.
123 **5**	All networking functions are complete (notably, DHCP) and the handset is proceeding to establish the SRP link to the SVP Server (if not in WMM Power Save Mode).

At the end of this sequence, the handset compares its software version to the version on the TFTP server. If the software is out of date, the handset starts a download process.

If the handset is configured for DHCP, it gets the TFTP server IP address from the DHCP server which is used to download both handset and PCX configuration files.

If the handset is configured for static IP addresses, it contacts the **TFTP Server IP** configured

in the Admin menu for handset configuration files, and the **TFTP1 IP** and **TFTP2 IP** servers for the PCX configuration files.

As soon as the handset has acquired the system and registered with the PCX, it displays the date and the extension number. The handset is in standby and is ready to use.

Note 1:

The handset starts in MIPT 300/600 compatibility mode.

To turn the handset off, press and hold the **END** key until one beep sounds.

Note 2:

You cannot turn off the handset during a call. End the call before turning off the handset.

5.2.2.1.6 Special operating modes

The handsets run in special operating modes as described below: Site Survey, Syslog, and Push-to-talk. Use the Admin menu to configure the modes.

For information on the Admin menu, see module IP Touch 310/610 WLAN Handset - Configuration .

Site Survey mode

The handsets include a Site Survey function that allows you to scan an area for Access Points, gain information about Access Points, and evaluate the coverage in a particular area.

For more information about running the handset in Site Survey mode, see module IP Touch 310/610 WLAN Handset - Survey Mode .

Syslog mode

You can configure the handset to send log information to a Syslog server present on the network. The information helps you to characterize a problem, identify a malfunction, or collect statistics on a periodic basis.

For information on running the handset in Syslog mode, see module IP Touch 310/610 WLAN Handset - Maintenance § Syslog mode .

Push-to-talk mode

The Push-to-talk (PTT) mode is available on Alcatel-Lucent IP Touch 610 WLAN Handset handsets only. Using the handset in PTT mode is like using a walkie-talkie: it operates in a group multicast mode, which means that only one participant can talk at a time. The user starts a session by pressing the TALK key, enabling instant group calling. A session can involve two or more participants.

The PTT mode uses a common channel for incoming and outgoing radio communication. A group is identified by the channel it uses. All handsets monitoring the same channel hear the voice transmission that is broadcast on this channel.

By default, 25 multicast channels (24 normal channels, plus 1 priority channel) are available for PTT. The default channel is the lowest channel that has been allowed. You can limit the channels a handset can use in the Admin menu by entering the allowed channel number. You can allow/disallow PTT mode for a handset.

Note 1:

Channel 25 is always the priority channel and cannot be disabled. If a communication comes in on the priority channel, it takes precedence over the communication on other channels.

Using the Local menu, the user can select any of the allowed channels to join the corresponding group. Only one channel can be selected at a time. The user enables/disables PTT mode in the Local menu. The option appears only if PTT mode is allowed in the Admin menu.

Note 2:

Users who do not wish to receive PTT calls should disable the feature. When PTT is enabled, the handset's battery life is decreased to about 30 hours.

For more information on using the Local and Admin menus, see module IP Touch 310/610 WLAN Handset - Configuration .

5.2.2.2 Configuration

The Alcatel-Lucent IP Touch 310/610 WLAN Handsets provide two configuration menus:

- The Admin menu allows you to configure options for site-specific requirements. Access to the menu can be protected by a password.
- The Local menu allows users to customize their handset settings and access handset configuration information.

The Handset Administration Tool provides the ability to configure handsets via a graphical user interface. The handset charger is connected to a PC and uses a Windows-based application to change and store settings on the handsets. With the tool, you can store multiple configurations to support different user profiles, upload or download a complete configuration profile directly to the handset's flash memory, or update handset parameters.

For more information on using the Handset Administration Tool, see module IP Touch 310/610 WLAN Handset - Handset Administration Tool .

5.2.2.2.1 Navigating the menus

The navigation keys, just below the softkeys, are used to navigate through and select menu options. These are referred to as **Nav** ▲ , **Nav** ▼ , **Nav** ◄ , **Nav** ► and **NavOK**.

Figure 5.73 : Navigation keys on Alcatel-Lucent IP Touch 310/610 WLAN Handsets

Some menu options have only two possibilities and operate on a toggle basis. The current setting is shown on the second row of the display, called the info line. Press **NavOK** to toggle between the settings.

Example:

*When **Enable PTT** is the menu option, **PTT Disabled** will show on the info line. If you select **Enable PTT**, **PTT Enabled** will show on the info line and the menu option will toggle to **Disable PTT***

An asterisk (*) next to an option on the display indicates that it is selected.

Enter numbers by pressing keys on the keypad. The blinking underscore identifies the current cursor position. When entering alphanumeric strings, the CAPS/caps softkey will appear and may be pressed to toggle the case. Enter letters by repeatedly pressing the corresponding key until the desired letter displays on the screen. Use the CAPS softkey to change the case as needed.

To edit during entry, delete the character to the left of the cursor by pressing the **Del** softkey. To replace an entry, delete it by pressing the **Clr** softkey and then enter the new data. To edit an existing entry, use **Nav** ◄ and **Nav** ► to move the cursor position, and then press the **Del** softkey to delete the character to the left. Insert new data by pressing the keys on the

keypad.

5.2.2.2.2 Admin menu

Use the Admin menu to configure options for site-specific requirements. The configuration is stored locally on the handset.

To open the Admin menu:

1. With the handset powered off, press and hold down the **START** key. While holding down the **START** key, press and release the **END** key.
2. When the Admin menu appears, release the **START** key.

Note 1:

If a password has been configured, the handset asks you to enter it before opening the Admin menu.

To exit the Admin menu, press the **END** key once, or press the **Cncl** softkey successively through the menu hierarchy.

Note 2:

The handset exits the Admin menu automatically after 20 seconds of inactivity (no keys pressed).

The following table describes the Admin menu options. An asterisk next to an option indicates it is the default.

Admin menu option				**Use this option to...**
Phone Config	Language	*English, French, German, Spanish, Portuguese, Dutch, Italian		Select the language for the handset.
	Licence Option	Type 030, *Type 031, Type 036, Type 043		Select the VoIP protocol that your site is licenced to download and run. Use protocol **Type 31**. Any other protocol will cause the handset to malfunction. Other options are reserved for future use.
	Password Disable/ *Enable			Set a password to control access to the Admin menu. The password is enabled by default with the password 123456. To modify the password requirement, the default or previously set password must be entered to verify the change. The password must be set in each handset for which controlled access is desired.
	Change Password:			Change the password. *Note 3:* *This option appears only if the password is enabled.*

Admin menu option				Use this option to...
	Push-to-talk Disable/ Enable	Allowed Channels	Channels *1-*24	Allow channels for Push-to- talk (PTT). All 24 PTT channels are allowed by default. Allowed channels are displayed with an asterisk (*). To toggle the status of any channel, scroll to the channel to be allowed/disallowed and press **NavOK**. Only those channels allowed in the Admin menu will appear on the Local menu where the user can subscribe to them.
		Name Channels	Channels 1-24	Name channels. The name will appear instead of channel number when channel information is displayed on the handset.
		Priority Channel On/Off	Name Channel	Set the priority channel, also referred to as channel 25. When a PTT broadcast is made on the priority channel, it overrides any active PTT transmission on all other channels. You can enter a name for the priority channel.
Network Config	IP Addresses	*Use DHCP, Static IP	Alcatel DHCP only, *Favour Alcatel DHCP	Enable/disable Dynamic Host Configuration Protocol (DHCP). **Use DHCP**: Each time the handset is turned on, the handset uses DHCP to assign an IP Address. The handset receives all other IP address configurations from the DHCP server. If you select: - **Alcatel DHCP only**, the handset will only look for a DHCP server that has a special Alcatel-Lucent field set. - **Favour Alcatel**, the handset will look for an Alcatel-Lucentl DHCP server that has a special Alcatel-Lucent field set first, but if not found will use any DHCP server. **Static IP**: Allows you to manually set a fixed IP address. The handset prompts you for the IP address of each configurable network component. When entering addresses, enter the digits only, including leading zeroes. No periods are required.

Admin menu option				Use this option to...
			Phone IP	Enter the IP address of the handset. If using Static IP, you must obtain a unique IP address for each phone from your network administrator. If using DHCP, the IP address is automatically assigned by the DHCP server.
			Default Gateway	Identify subnets in a complex network. **Static IP**: Configure the IP address for both the Default Gateway and Subnet Mask. **Use DHCP**: For handsets to contact network components on a different subnet, configure the Default Gateway (option 3) and the Subnet Mask (option 1) on the DHCP server.
			Subnet Mask	Identify subnets in a complex network (with **Default Gateway**)
			TFTP Server IP	Enter the IP address of a TFTP server on your network. In dynamic mode only, the TFTP server provides the configuration file that allows the handset to register with the PCX. If this feature is configured, the handset checks for newer software each time it is powered on or comes back into range of the network.
			Syslog Server IP	Enter the IP address of the Syslog server.
			SVP IP	Enter the IP address of the SVP Server. *Note 4:* *Required only if **QoS Type** is SVP.*
			Alcatel TFTP Info	Enter IP addresses for: - TFTP 1 IP (the primary TFTP server's IP address, used to download PCX configuration files) - TFTP 2 IP (the redundant TFTP server's IP address) - TFTP 3 IP (not currently used) - TFTP Port (the port to use for all TFTP requests after the firmware download)
	ESS ID			Enter the SSID.
	Security	*None		Disable any 802.11 encryption or security authentication mechanisms.

Admin menu option				Use this option to...
		WEP	Authentication: *Open System, Shared Key	Configure Wired Equivalent Privacy (WEP). Configure the handset to correspond with the encryption protocol set up in the Access Points. **Open System**, the default, is recommended.
			WEP *Off/On	Turn WEP on or off.
			Key Information: Default Key, Key Length, Key 1-4	Enter information about encryption key used by the handset.
			Rotation Secret	Enter secret used for proprietary WEP key rotation.
		Cisco FSR	Username	Enter the username that matches an entry on the Radius server for the Fast Secure Roaming mechanism.
			Password	Enter the password that corresponds to this Username for the Fast Secure Roaming mechanism.
		WPA-PSK	*Passphrase	Enter passphrase between eight and 63 characters used by the security features of Wi-Fi Protocol Access (WPA) using PreShared Key (PSK).
			Pre-Shared Key	Enter the 256-bit PSK for WPA.
		WPA2-PSK	*Passphrase	Enter passphrase between eight and 63 characters used by the security features of WPA2.
			Pre-Shared Key	Enter the 256-bit PSK for WPA2.

Admin menu option				Use this option to...
	Reg. Domain[1]: 01 for North America, 02 for Europe and Japan (channels 1-13)	802.11 Config for 802.11 a, b, and b/g mixed	802.11a, *802.11 b and b/g mixed:	Set regulatory domain, 802.11 type and transmit power. Once the domain and 802.11 type are established, the transmit power menu opens. Only those power levels which apply to the domain and 802.11 mode are listed. Only one level may be selected. The selected level is marked with an asterisk (*). For 802.11a: - 5.150-5.250 - 5.250-5.350 DFS - 5470-5,725 DFS - 5,725-5,825 DFS *Note 5:* *For 80.211a, non-DFS channels are recommended.* For 802.11 b and b/g mixed: - 5 mW (7dbm) - 10 mW (10dbm) - 20 mW (13dbm) - 30 mW (15dbm) - 40 mW (16dbm) - 50 mW (17dbm) - 100 mW (20dbm) The 802.11 mode and the transmit power level should be set to match the corresponding settings used by the Access Points in your facility. If changed from the default, the transmit power setting must be the same on all handsets and all Access Points. *Note 6:* *50 mW and 30 mW appear only if Regulatory Domain is set to None or 01*
	QoS Type	*SVP		Set the QoS type to SVP. The SVP option uses the SVP Server to prioritize traffic.
		WMM Power Save		Set the QoS type to WMM Power Save. If WMM Power Save is selected, the Access Points (AP) and the handset prioritize traffic instead of going through the SVP Server. *Reminder:* *Verify that WMM is activated on the APs.*

Admin menu option				Use this option to...
Diagnostics	Run Site Survey[2]			Activate the Site Survey mode. The site survey starts immediately upon selecting this option.
	Diagnostics[3] Disable/ Enable			Enable diagnostics.
	Syslog Mode	*Disabled, Errors, Events, Full		Enable Syslog mode. *Note 7:* *When enabling Syslog mode, remember to configure the Syslog server's IP address.*
	Error Handling Mode: Halt on Error, *Restart on Error			Set error handling mode.
Restore Defaults				Set all user and administrative parameters except Licence Option to their defaults.

[1]To enter the **Reg Domain** menu, press the **Speakerphone** key.

[2]For more information on Site Survey, see module IP Touch 310/610 WLAN Handset - Survey Mode .

[3]For more information on Diagnostics, see module IP Touch 310/610 WLAN Handset - Maintenance

5.2.2.2.3 Local menu

The Local menu allows users to customize their handset settings and access handset configuration information.

The Local menu is only available when the handset is on standby.

To start the Local menu, press the **NavOK** key.

While using the Local menu, incoming calls are not presented. The handset is seen as being busy.

To exit the Local menu, press the **END** once, or press the **OK** or **Back** softkey successively through the menu hierarchy.

Note 1:

The handset exits the Local menu automatically after 5 seconds of inactivity (no keys pressed).

The following table describes the Local menu options.

Local menu option				Use this option to...
Lock keys				Lock the keypad.

Local menu option				Use this option to...
User Profiles: Silent, Vibrate, Loud, Soft, Custom	Set as Active			Select a user profile.
	Ring Settings: Telephone, Auxiliary Ring 1, Auxiliary Ring 2	Ring cadence	Off, PBX, Continuous, Short Pulse, Long Pulse	Select the ring cadence. By default, ring cadence is off for the Silent and Vibrate profiles, and PBX for the Loud, Soft, and Custom profiles. *Note 2:* *Auxiliary Ring 1 and 2 are not used.*
		Ring Tone	Tones *1-10	Select a ring tone.
		Ring Volume	1-8 levels	Set the ring volume. By default, ring volume is level 1 for the Silent and Vibrate profiles, level 7 for Loud, level 3 for Soft, and level 5 for Custom.
		Vibrate Cadence	Off, PBX, Continuous, Short Pulse, Long Pulse	Select vibrating cadence. By default, vibrate cadence is off for the Silent, Soft, and Loud profiles, and PBX for the Vibrate and Custom profiles. *Note 3:* *Vibrate cadence and ring cadence can be active simultaneously.*
		Ring Delay	No Delay, 5 second delay, 10 second delay	Set ring delay.
	Noise Mode	Normal, High, Severe		Set environment noise characteristics. Use normal for most office environments, high for moderate background noise, severe for extremely noisy conditions.
	Ring in Headset, Ring in Speaker			

Local menu option				Use this option to...
	Warning Tones			Disable/Enable warning beeps such as system up or down, out of range. By default, warning tones are disabled for the Silent and Vibrate profiles, and enabled for the Loud, Soft, and Custom profiles.
	Key Tones			Enable/disable keyclicks when keys are pressed. By default, key tones are disabled for the Silent and Vibrate profiles, and enabled for the Loud, Soft, and Custom profiles.
	Push-to-talk			Enable/disable Push-to-talk mode. By default, Push-to-talk is disabled for the Silent and Vibrate profiles, and enabled for the Loud, Soft, and Custom profiles.
Phone Settings	Keypad Autolock	Disable, 5 seconds, 10 seconds, 20 seconds		Enable/disable keypad lock automatically when in standby.
	Language	English, French, German, Spanish, Portuguese, Dutch, Italian		Set language for the handset.
	Display Contrast	Set Contrast		Fine tune the contrast (from 30% to 83%) for different lighting situations.
	Use Hearing Aid, Use no Hearing Aid			Enable or disable use of a hearing aid.
	Startup Song Play/Inibit			
System Info	Phone IP Address			Display the Phone IP Address currently assigned to the handset.
	Alias IP Address			Display the Alias IP Address currently assigned to the handset.
	SVP IP Address			Display the SVP IP address.
	Firmware Version			Display the hardware identification number (MAC address) and the software version running the handset.

Local menu option				Use this option to...
Alcatel Options	Main CPU0 IP			Display the IP Address of the main CPU.
	Main CPU1 IP			Display the IP Address of the redundant main CPU.
	TFTP Port			Display the TFTP port.
	TFTP1 IP			Display the TFTP1 IP address.
	TFTP2 IP			Display the TFTP2 IP address.
	TFTP3 IP			Display the TFTP3 IP address (currently not used).
PTT Caller ID				
Push-to-talk	Default Channel	Channels 1-24		Select a channel for Push-to-talk (PTT). By default, the selected channel is the lowest allowed channel as set in the Admin menu.
	Subscribed Channels	Channels 1-24		Enable a PTT channel that has been allowed in the Admin menu.
	PTT Audio Volume			Adjust volume of PTT audio using the **Nav** ▲ and **Nav** ▼ keys. *Note 4:* *You can override the volume setting by adjusting volume with the **Volume up** and **Volume down** keys during a PTT call.*
	PTT Tone Volume			Adjust volume of PTT tones using the **Nav** ▲ and **Nav** ▼ keys.

5.2.2.3 Handset Administration Tool

The Handset Administration Tool is a software utility developed by OEM Corporation to automate the configuration of multiple Alcatel-Lucent IP Touch 310/610 WLAN Handsets. This document explains how to use the Handset Administration Tool to configure the handsets.

5.2.2.3.1 Handset Administration Tool Installation

The Handset Administration Tool is a software utility installed on a PC with a USB port that can be cabled to the USB port of the Dual Charger. It is designed as a time-saving device for rapid administration and configuration of a number of handsets. Configuration options include:

- Setting all options on the Admin menu,
- Setting all options on the Local menu,
- Assist troubleshooting by recording error information,
- Upgrade handset software.

Installing the USB driver

Necessary components:

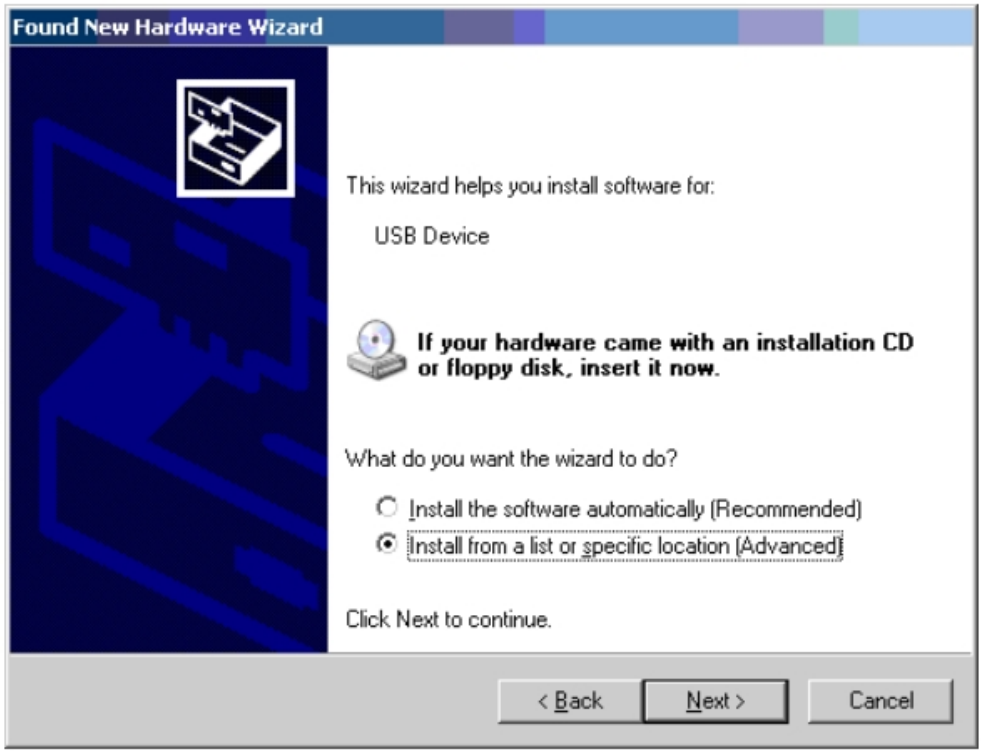
- PC running Windows 2000 or Windows XP with a USB port,
- Dual Charger for the Alcatel-Lucent IP Touch 310/610 WLAN Handsets,
- Power supply for the appropriate country or region,
- OEM USB cable or comparable cable (with 5-pin “mini-B” connector).

Note:
USB cables vary in their ability to make a proper connection to the Dual Charger’s USB port. Use of the USB cable available through OEM is recommended to ensure compatibility.

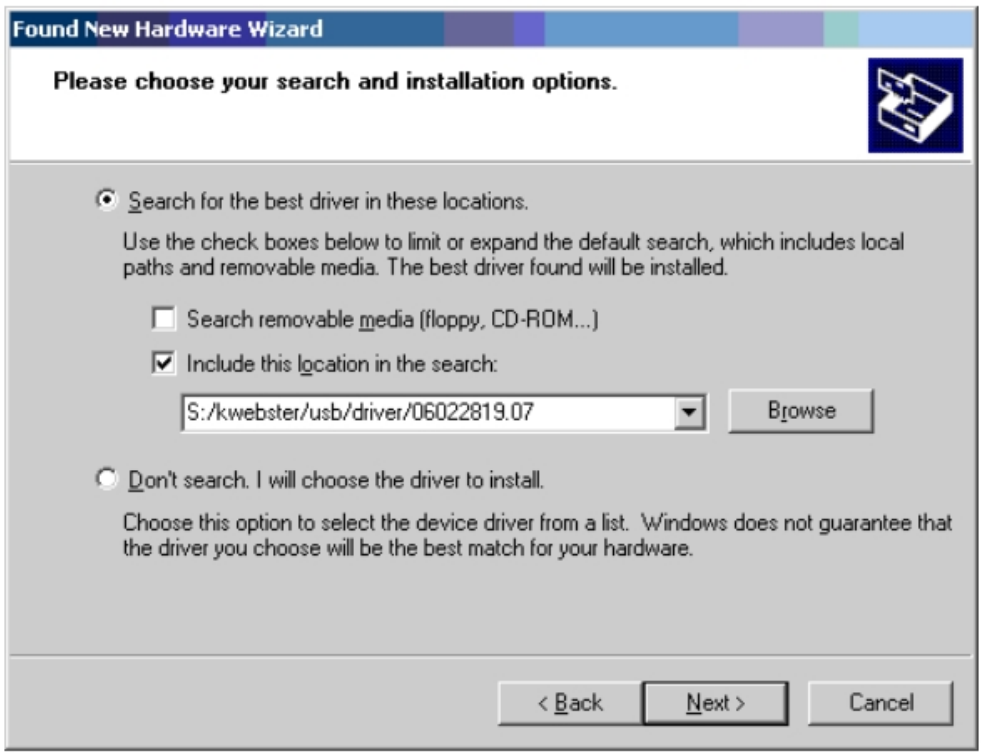
To install the USB driver:

1. Set up a folder on the PC for the configuration of Alcatel-Lucent IP Touch 310/610 WLAN Handsets. Load the Handset Administration Tool software into this folder. If the `.exe` file is delivered in a zip file, extract the individual file(s).
2. The USB driver may be delivered in a separate zip file. If so, set up a folder for the USB files and extract the two files from the zip file into this folder. The two files are named `slnkusb.sys` and `slnkusb.inf`.
3. Place the Dual Charger on a flat, horizontal surface and plug the power supply into the Dual Charger and into an appropriate wall outlet. Plug the USB cable into the Dual Charger and into an available USB port on the PC.
4. Power off a handset, remove the Battery Pack, and place the handset in the Charger. The handset will automatically power up in USB mode.
5. Microsoft Windows will start the Found New Hardware Wizard and ask if it can connect to Windows Update to search for software. Click **No, not this time**. Click **Next**.

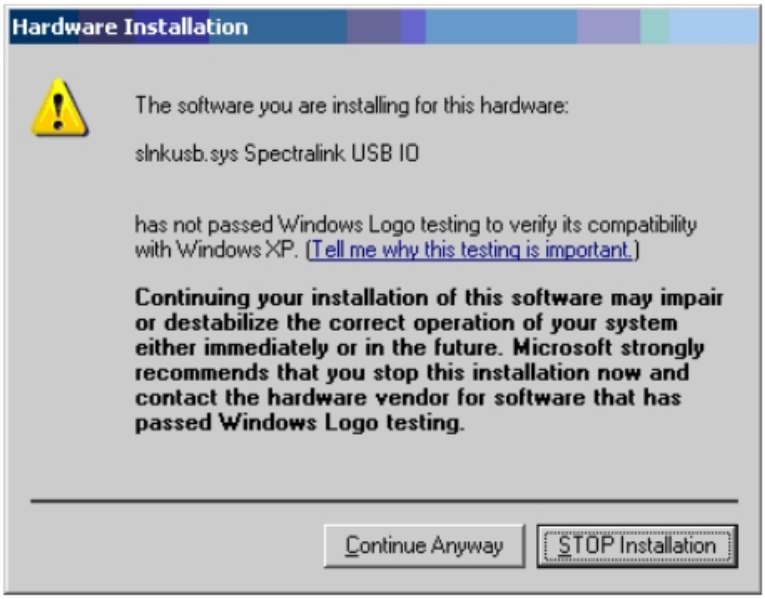
6. The next screen prompts you for information about installing the USB device. Click **Install from a list or specific location** and click **Next**.



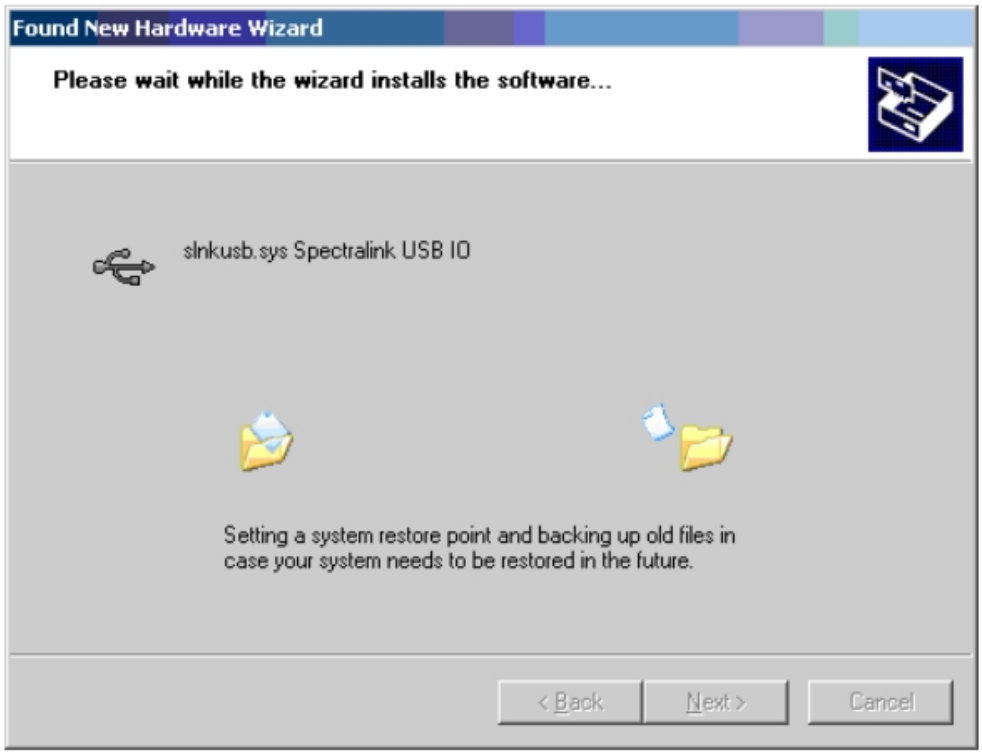
7. The next screen prompts you for the location. Click **Search for the best driver in these locations**. Clear the **Search removable media** checkbox. Select the **Include this location in the search** checkbox, click **Browse** and navigate to the location of the USB driver files. Click **Next**.



8. The Microsoft Wizard will display a warning message. The USB software has been fully tested in OEM laboratories and will not harm your system. Click **Continue Anyway**.



9. Microsoft Wizard will now install the software.

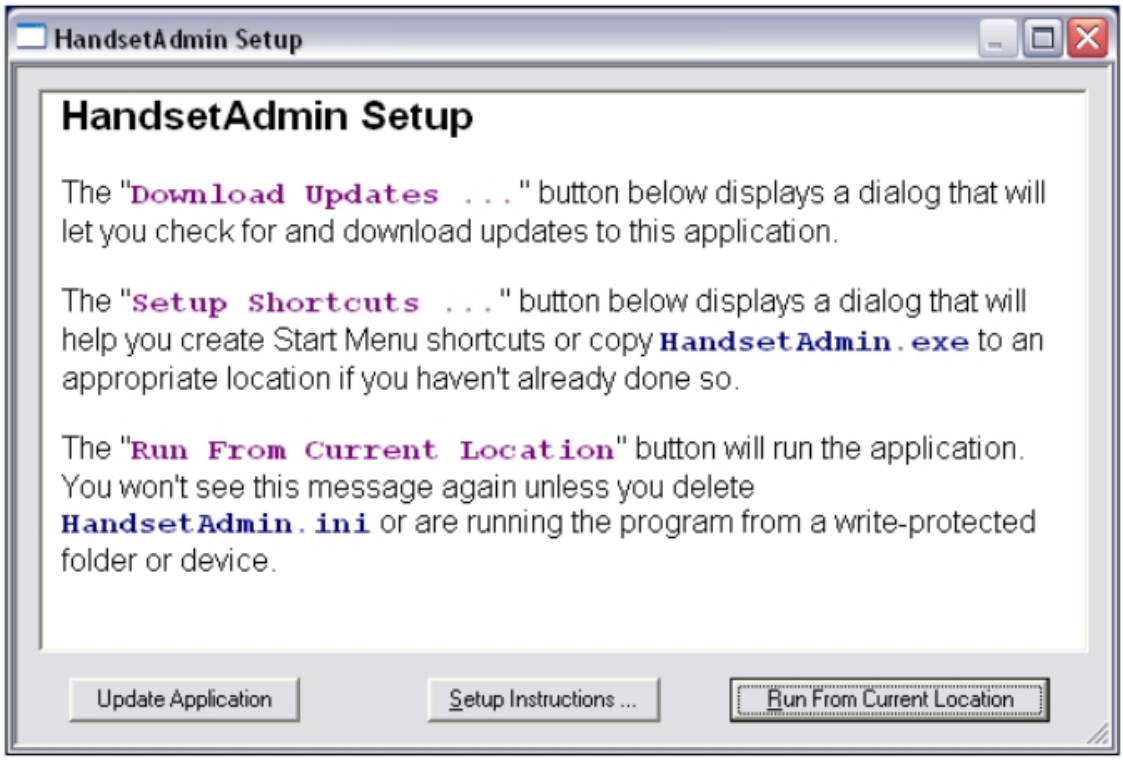


10. The final screen indicates that the USB driver has been successfully installed. Click **Finish** to close the wizard and proceed with handset configuration.

Install the Handset Administration Tool

There is no installer or uninstaller for the Handset Administration Tool since the program does not modify your system or registry. It runs from its current location and stores its settings locally.

1. If not already done, create a folder for the Handset Administration Tool files and then copy the `.exe` file into it.
2. Navigate to the folder established in step 1, and click the `HandsetAdminXxyy_yy_yy_yy.exe` file to run the utility.
3. Accept the **SpectraLink Software Licence Agreement**.
4. The **HandsetAdmin Setup** window allows you to run the program from its current location or set up Start Menu shortcuts and/or move the program to a different folder, if desired.

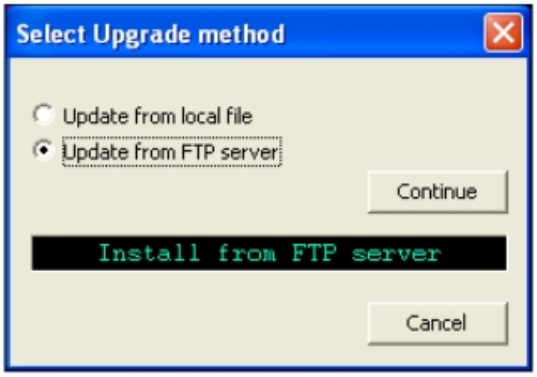


If you select **Run From Current Location**, the Handset Administration Tool will start.

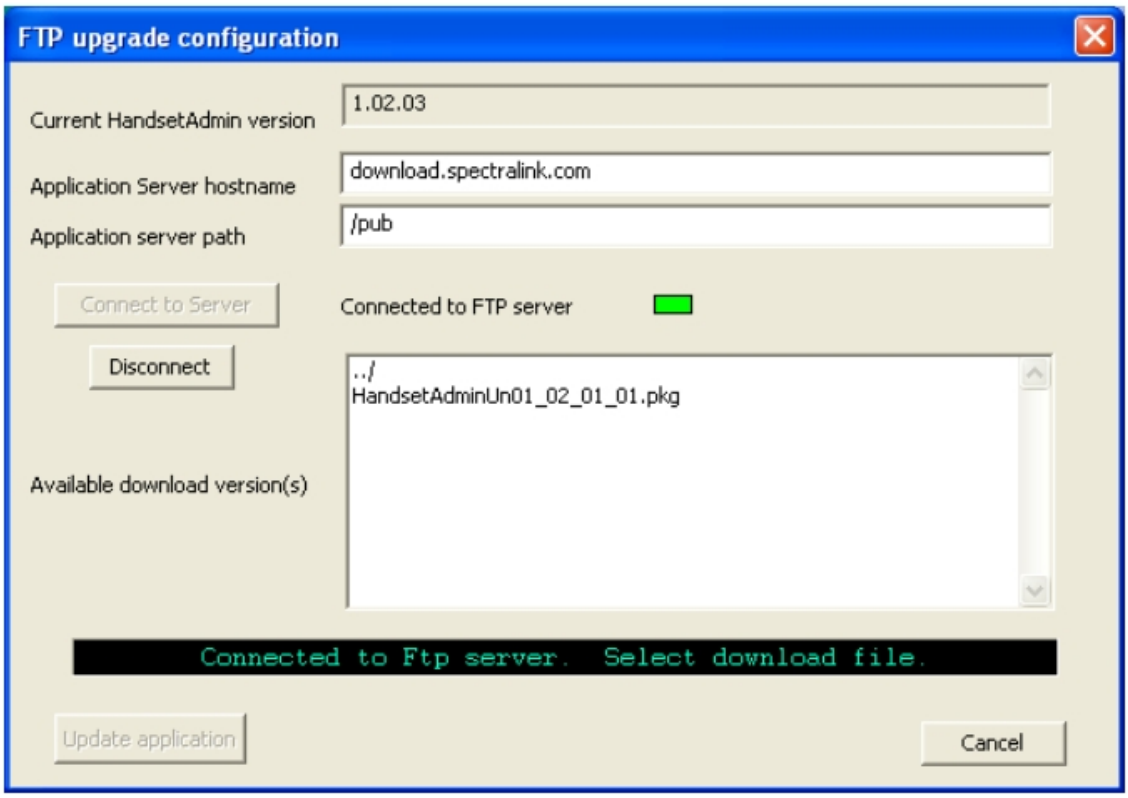
Note:
The tool will not be fully functional if it is run from a non-writeable location such as a CD.

5. The **Update Application** button allows you to retrieve a more recent version of the Handset Administration Tool from a local folder or from the SpectraLink FTP site.

   SpectraLink recommends downloading the updated versions from the FTP site when first installing the program.



If the FTP option is selected, a dialogue box will open to direct you to the FTP site. If selecting the **Update from FTP server** option, be sure your computer has Internet access.

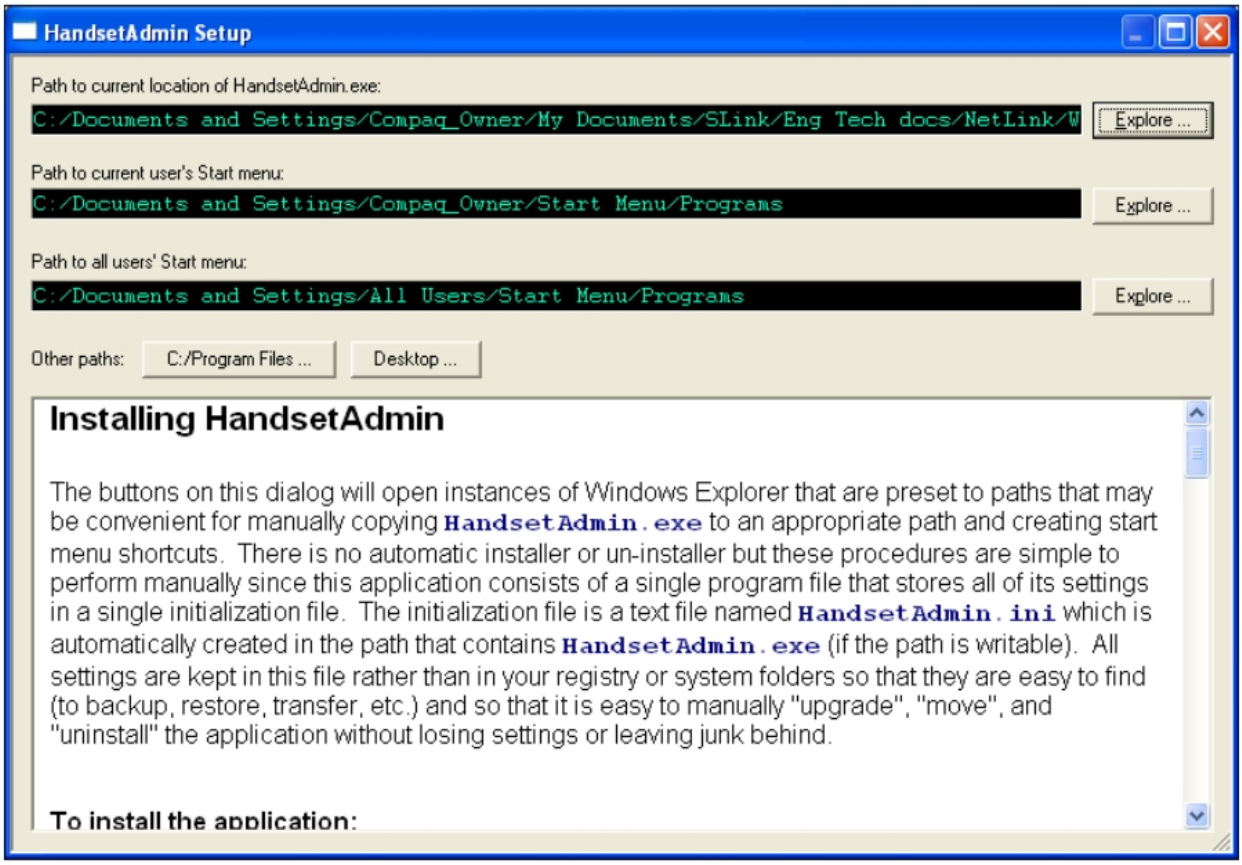


Once you connect to the server, you can select and download the file. The file extension is `.pkg` and the filename shows the version in this format:`HandsetAdminXxyy_yy_yy_yy.pkg`.

Package (pkg) files are bundled versions of the Handset Admin Tool executable (`.exe` file). Package files are made available by SpectraLink for download via an anonymous FTP site. Users must have a valid `HandsetAdmin.exe` installed on the connecting PC in order to unpack and install the upgrade.

Package files are located beneath the /pub folder on the FTP server. From there, navigate to the appropriate folder for your PBX and vendor type.

6. The **Setup instructions...** button allows you to access a series of tips and tricks for installing the Handset Administration Tool on your system. A dialogue box with instructions on installing it on the Start Menu displays.



The full instructions shown in the box above are reproduced in full below.

Installing HandsetAdmin

The buttons on this dialogue will open instances of Windows Explorer that are preset to paths that may be convenient for manually copying `HandsetAdmin.exe` to an appropriate path and creating start menu shortcuts. There is no automatic installer or un-installer but these procedures are simple to perform manually since this application consists of a single program file that stores all of its settings in a single initialization file. The initialization file is a text file named `HandsetAdmin.ini`, which is automatically created in the path that contains `HandsetAdmin.exe` (if the path is writable). All settings are kept in this file rather than in your registry or system folders so that they are easy to find (to backup, restore, transfer, etc.) and so that it is easy to manually "upgrade", "move", and "uninstall" the application without losing settings or leaving junk behind.

To install the application:

- Copy `HandsetAdmin.exe` to a write-enabled folder. If you create a new folder specifically for this application, the folder can double as a convenient place to save handset firmware updates or other files associated with this application.
- Create Start menu or desktop shortcuts if desired.
- The first time you run it from its new location, you will need to accept the Licence Agreement then choose "Run From Current Location" when the "Setup" dialogue appears. These dialogues will not appear again unless you delete

HandsetAdmin.ini.

To upgrade the application:

- Overwrite HandsetAdmin.exe with a newer version. New versions of the application are compatible with (will recognize) the old settings contained in your existing HandsetAdmin.ini file.

To move the application:

- Move HandsetAdmin.exe and HandsetAdmin.ini to a new path or move or rename the folder containing these two files. Windows XP will automatically modify shortcuts for you when their targets are moved or renamed via Windows Explorer, so, even if you created start menu shortcuts to these files, you can move them using Explorer without having to re-do the shortcuts.
- If moving the application to a new machine, you will have to create new shortcuts, if desired, on the new machine. By copying HandsetAdmin.ini to the new machine, your old settings will be retained.

To uninstall the application:

- Delete HandsetAdmin.exe, HandsetAdmin.ini, and any shortcuts or folders you created for it.

How to use Windows Explorer and create Start menu shortcuts

Consult the documentation that came with your operating system for details. The instructions below describe one set of tips and techniques. Other techniques exist and are just as valid. These instructions were written for Windows XP and may or may not work under different operating systems.

To move or copy a file, drag it from one Explorer window and drop it into another Explorer window.

To create a shortcut, use the right mouse button to drag a file or folder (for instance, HandsetAdmin.exe) to an Explorer window, then choose "Create Shortcuts Here" from the menu that appears when you release the right mouse button. A file, folder, or shortcut in one of the Start menu paths (either "current user" or "all users") will show up in the Start menu under the "All Programs" submenu. Folders show up as submenus and the contents of folders show up as items under the folder's submenu.

To make a shortcut show up in your Start menu up above the most-recent list (rather than under the "All Programs" submenu), right-click the target or existing shortcut (either in the Start menu or in Windows Explorer), then choose "Pin to Start menu". To reverse this effect, right-click the Start menu shortcut and choose "Unpin from Start menu".

Ini tricks and tips:

- The program reads HandsetAdmin.ini when it starts, keeps settings in memory while it runs, and writes HandsetAdmin.ini when it exits. Thus if you modify HandsetAdmin.ini while the program is running, your changes will have no effect.
- Delete, move, or rename HandsetAdmin.ini to make the program forget its history and revert to default settings (for example, to make it re-show this dialogue which is normally shown only once).
- Copy HandsetAdmin.ini to another machine to share or transfer settings.
- Edit HandsetAdmin.ini with a text editor to erase or modify specific settings.
- Backup and restore HandsetAdmin.ini to preserve settings.
- If you rename HandsetAdmin.exe, then the name of the .ini will likewise change (just replace ".exe" with ".ini" to determine the new name). The old .ini will be orphaned unless you also rename it.

To print or copy this text

Copy-and-paste this text into WordPad. All formatting will be preserved. Use WordPad to

save or print the text.

5.2.2.3.2 Using the Handset Administration Tool Console

The Handset Administration Tool has two separate functional areas: the Administration Console and the Handset Settings Editor. The Administration Console helps you connect to the handset, set and change the password, retrieve error messages, update handset software, and update the Handset Administration Tool software. The Handset Settings Editor enables you to configure handsets and allows you to create, save and copy Admin menu options. See § Configuring Admin Menu Settings for detailed instructions on using the Handset Settings Editor.

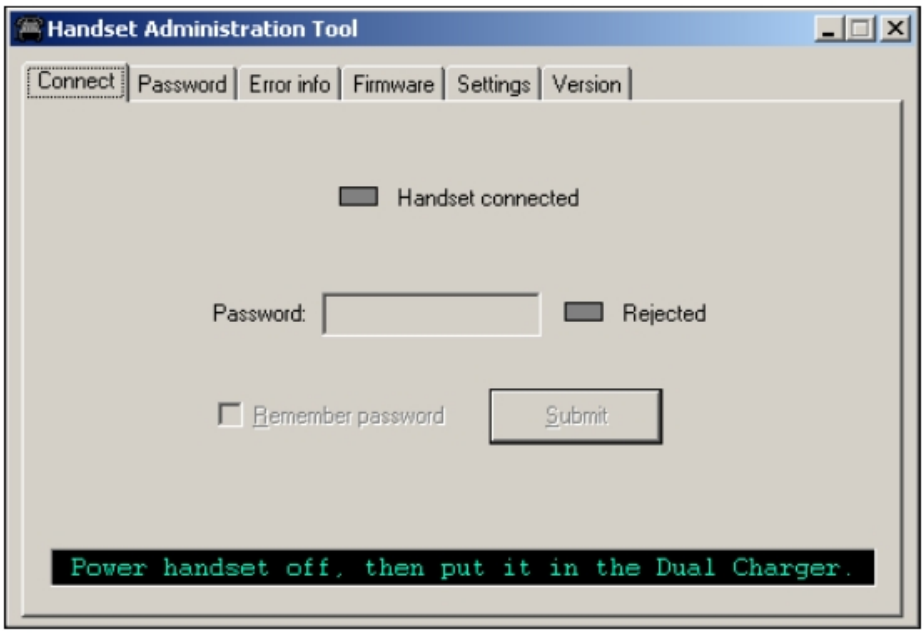
The Handset Administration Tool uses indicators to alert you to the status of the action being performed:

- Green: the adjacent label is “true” and this state is desirable or required.
- Yellow: the adjacent label is “true” and this state requires caution or attention. For example, a yellow **New folder** indicator cautions that the file path will be created. A yellow **File exists** indicator cautions that the file will be overwritten.
- Red: the adjacent label is "true" and this state is undesirable or is accompanied by an error, in which case a message on the prompt line or a dialogue box will describe the nature of the error.
- Grey: the adjacent label is not "true". For example, the handset is not connected.
- Blinking: file status indicators blink yellow when the file status is being queried but is not yet known, for example, when attempting to access slow drives or unresponsive network devices. File status indicators blink red when the path is invalid (mistyped). The Handset indicator blinks when the handset's password needs to be entered.

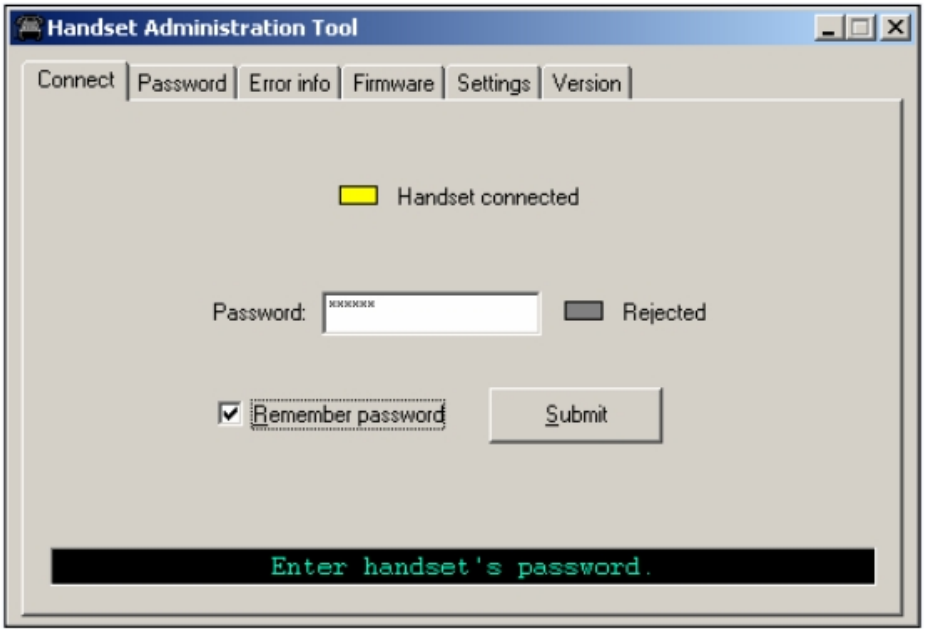
A prompt line at the bottom of the window provides information about what action should be taken or the status of the utility.

Connecting the Handset

The first window prompts you to insert a handset into the Dual Charger. The tab labels describe each of the available functions.



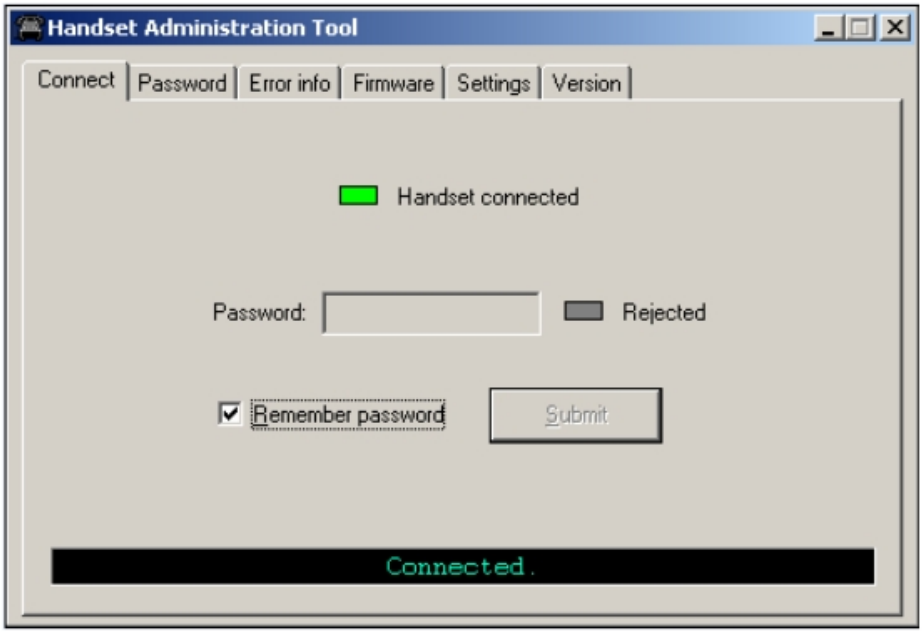
Insert the handset into the Dual Charger and enter the password.



When the handset is inserted for the first time, the password must be entered. If you check the **Remember password** box, the password is retained as the default password for all handsets.

Unique passwords for each handset are not remembered. Enter the password and click **Submit**. The default password is `123456`.

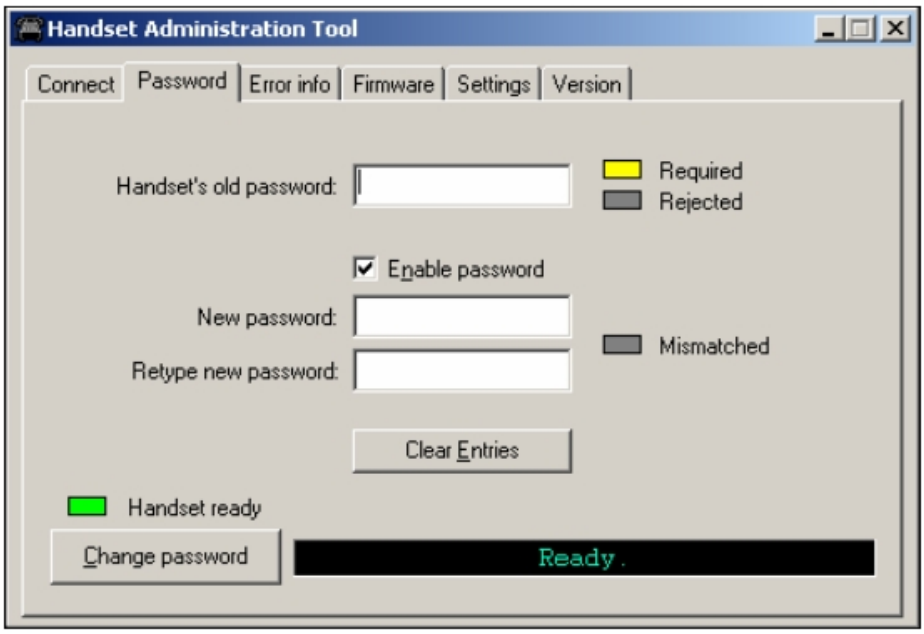
When connection is established between the program and the handset the **Handset connected** indicator turns green and **Connected** displays on the prompt line. The handset is now ready for configuration.



Password Configuration

In order to change a password, the existing password must be entered. Then the new password may be entered and confirmed. If the **Enable password** checkbox is unchecked, no password will be required to access the **System Info** and **Alcatel Options** in the Local menu.

A password may be up to 18 characters.



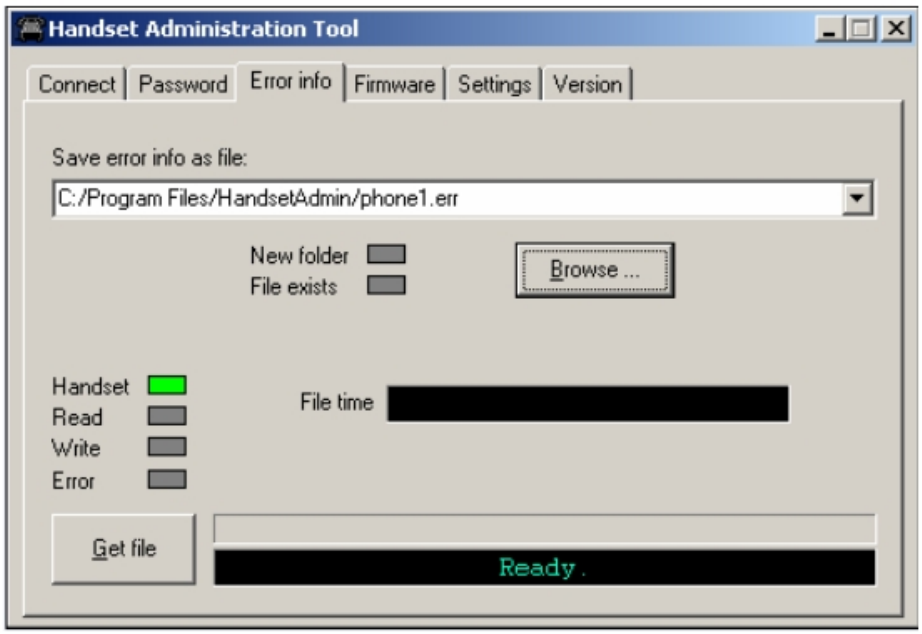
Error Information

The **Error info** tab provides a utility to assist the OEM customer service team to troubleshoot handset errors. When directed by customer service, this utility enables you to save any errors as a file which can then be sent to OEM for handling.

Click **Browse** to establish the path and then enter the filename. Future saves will point to this same location as the default so that the same file may be overwritten if desired. A dropdown list box displays the most recently used filenames. The **File time** window displays the modification timestamp of the file in the **Save…as** window.

Save the file by clicking **Get file**. The file will be copied from the handset to the location. The **Read/Write** indicators will reflect the action as it occurs. File transfer progress is shown by a progress indicator above the prompt line.

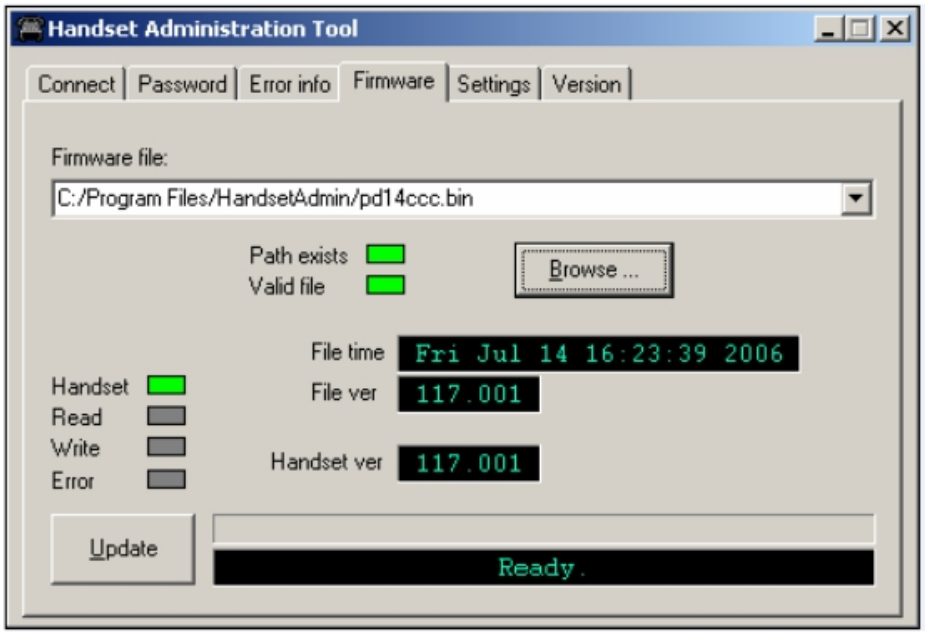
This sample screen shows a new file being created in an existing folder.



Software Updates

The **Firmware** tab allows you to update the software in the handset by copying it from a location on your computer to the handset memory.

1. Download the software update from the Business Partner Web site at *https://www.businesspartner.alcatel-lucent.com*.
2. Extract the bin files from the zip file to a folder set up for this purpose. Each file must be individually downloaded into the handset. This is not an efficient method of updating any quantity of handsets, but it works for testing new code and in extremely small installations. Be aware that if there is a TFTP server with older code broadcasting, the handsets will continue to download code over the air and revert to older code when power cycled.
3. Click **Browse** to locate the software file. A dropdown list box displays the most recently used filenames. The **File time** window displays the modification timestamp of the file in the **Firmware file** window. The file version and handset version will also display for comparison. Verify that the information indicates that the correct file will be downloaded and then click **Update**. The file will be copied from the location to the handset. The **Read/Write** indicators will reflect the action as it occurs.



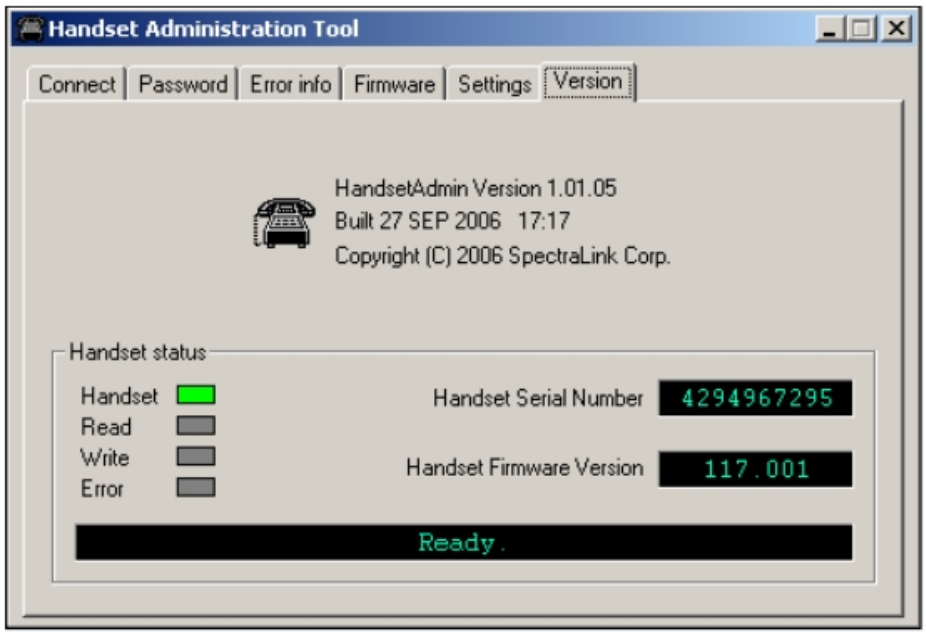
Note:
The firmware file path, file time, file version and handset version shown in the above sample screen are for illustration only.

Should an Error indication occur, retry the update after ensuring that the handset is properly seated and that the USB cable is in good condition and connected securely. Contact Customer Service if an error persists.

While a firmware update is in progress, you may open other tabs and the handset indicators shown on those tables will inform you of the status of the update.

Version

The **Version** tab displays the serial number of the handset and the software version being run.



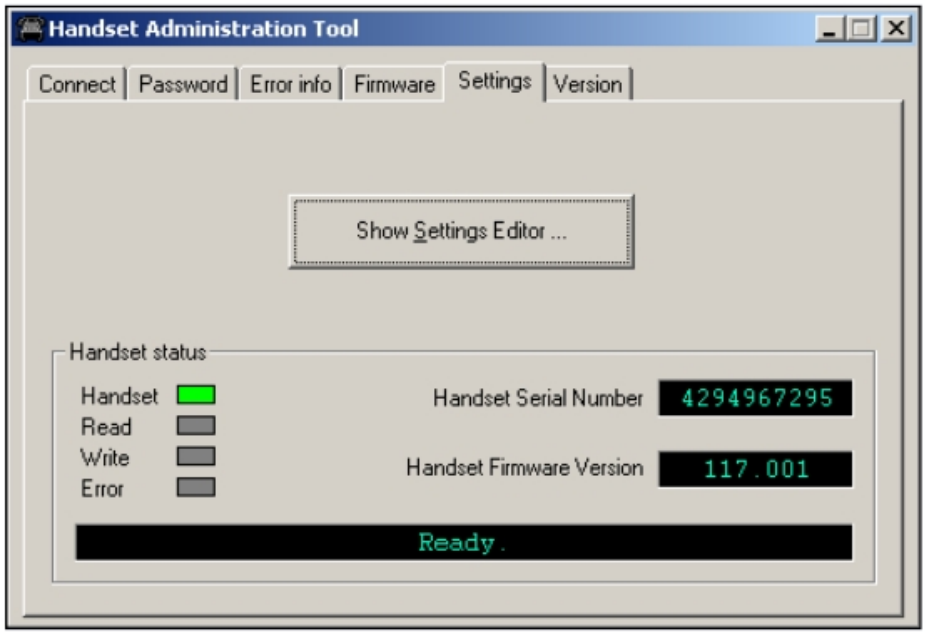
You can also update the Handset Administration Tool by selecting the **Update Application** button in the **HandsetAdmin Setup** window. For more information, see § Install the Handset Administration Tool .

5.2.2.3.3 Configuring Admin Menu Settings

The **Settings** tab allows you to configure required and optional settings in the Admin menu. PABX-specific menu options such as user name may also be assigned. Which options are available depends on the software used by the handsets. Specific configuration requirements are detailed in the Configuration and Administration document that pertains to the protocol used by your facility's system.

The **Settings** tab displays the serial number of the handset and the software version being run. The Tool Version button will display the version of the config charger software you are running.

To enter and modify menu settings, click **Show Settings Editor**.



When you have opened the **Handset Settings Editor**, you may click **Close this window** to close the **Settings** tab window. Display it again from the **Handset Settings Editor** by clicking the **View** and **Admin** functions.

The Handset Settings Editor Toolbar

The **Handset Settings Editor** toolbar allows you to name, open, and save configuration files and download and upload configuration settings to and from the handset in the charger.

The three filename windows allow you to open and save settings by **System**, **Group** or **User** type as separate files. Any filename can be assigned by entering it into the field and clicking **Save**. By default, the files will be saved in a new folder named `ConfigData` under the folder where the program is stored. The new folder will be created automatically the first time a file is saved. To open an existing file, click **Open...** and navigate to the file. Use the **File** menu to customize the file structure, if desired.

The file indicators beside the **Save** buttons have four colours to indicate the status of the file displayed in the window:

- Red: file does not exist. The filename in the window has not been created.
- Yellow: file not loaded. The filename in the window exists in the `ConfigData` folder but

has not been loaded into the **Editable settings**.

- Green: unsaved edits. When changes are made in the **Editable settings** field(s), the green indicator indicates these have not been saved.
- Grey: file up-to-date. The settings have been saved.

There are two columns of configuration options. The **Editable settings** column shows settings that may be saved as files. The **Handset settings** column shows settings that have been copied from or may be copied to the handset in the cradle. The **Copy settings** arrows and boxes allow you to copy settings to the handset column where they may then be written to the handset in the charger. The configuration in a handset may be copied to the **Editable settings** area and edited or saved. The **Sys Grp Usr** checkboxes allow you to copy just the settings you require.

Click **Read Handset** or **Write Handset** to initiate the transfer of configuration data from or to the handset in the charger.

The four labelled indicators on the right indicate the status of the configuration transfer.

Creating Your Configuration Plan

When first setting up a configuration plan you will enter information into the **Editable settings** fields, indicate which of the three categories each option belongs to, and save as **System**, **Group** or **User** files.

Important:

Do not create a plan that saves an option in two different categories. Option categories should be established and should not overlap. Example: Speakerphone and Push-to-talk settings are typically tagged as Grp options and saved in Group files.

Once you have established which options will be categorized as **System**, **Group** or **User**, enter the configuration information into the **Editable settings** fields. Start with the System options and enter all system-level field values. Click **Sys** category on the left side of the window for each option. Save these settings as a System file by entering the filename in the **System** filename field and clicking **Save**.

Note:

When a setting is changed, it is highlighted in yellow until it is saved.

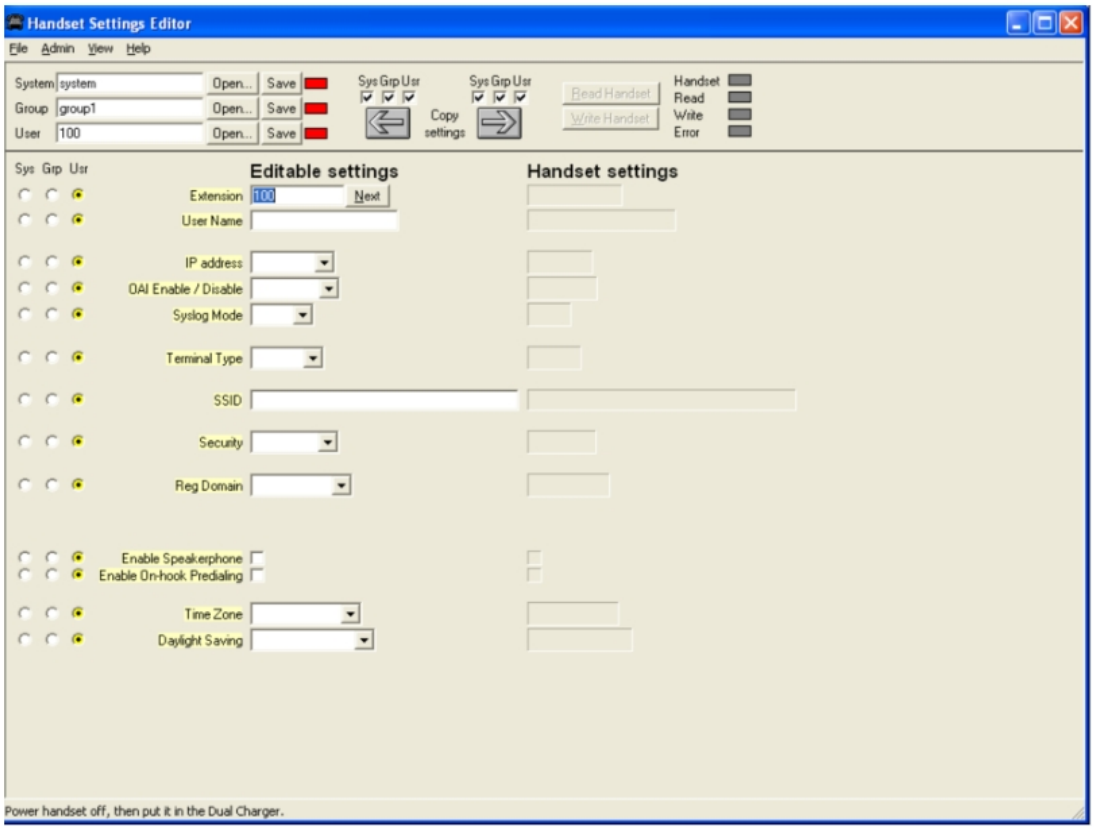
In the same way, create each Group plan by entering the values in the fields designated as Group types. Click **Grp** category on the left side of the window for each option. Save each plan under a different name in the **Group** filename field.

Create one basic User file for default (or desired) values for each **User** field. Click **Usr** category on the left side of the window for each option.

User settings don't necessarily need to be saved for each handset, but they can be saved if desired. It may be useful, for example, to save a user's ring preferences from a handset being replaced so that the new handset can be configured the same way. If you determine that each handset configuration should be saved, it is easiest to do this during the configuration process. See § Downloading and Uploading Configuration Plans .

Sample configuration window

Shown below is an abbreviated example of some configuration options that have not yet been set. The list of options that appears in your editor will differ.



Configuration planning worksheet

Use this or a similar worksheet to design your configuration plan.

Plan category_____ Filename_____

Sys	Grp	Usr	Label	Editable Setting

Downloading and Uploading Configuration Plans

Once your configuration plans are established, the settings are easily downloaded into the handsets.

To download a configuration plan to a handset:

1. Use the toolbar to open the **System**, **Group** and **User** plans for this handset.
2. Enter information unique to the handset, for example, **Extension** and **User name**.

   Note:
   *The **Extension** field has a **Next** button that is useful when configuring a quantity of handsets.*
3. Copy the settings to the **Handset settings** fields.
4. Click **Write Handset** to begin the download.
5. You may save the settings unique to this handset by ensuring the correct extension number or other filename is entered in the **User** filename field and then clicking **Save**. You may also load files or edit settings for the next handset (steps 1 and 2) during the download.
6. When the **Handset** indicator turns off, the download has finished and the handset may be removed from the charger.

To upload a configuration plan from a handset:

1. Click **Read Handset** to begin the upload.
2. When the **Handset** indicator turns off, the handset's settings will appear in the **Handset settings** fields.
3. You may copy these settings over to the **Editable settings** fields to use them to create configuration plans as described above or to save them by user or extension.

5.2.2.4 Survey Mode

Site survey is used to evaluate the facility coverage before certifying that an installation is complete. It can also be used at any time to evaluate coverage by testing signal strength, to gain information about an Access Point (AP), and to scan an area to look for all APs regardless of Service Set Identification (SSID). The information available through the site survey includes:

- SSID
- Beacon Interval
- Information regarding support of 802.11d, 802.11g, 802.11h and other 802.11 amendment standards as required
- Current security configuration

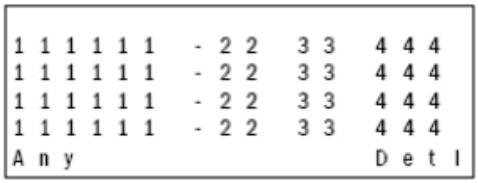
5.2.2.4.1 Single SSID, AP summary mode

Start the site survey by selecting Run Site Survey from the Admin menu. Survey mode starts immediately.

Note 1:
Before running the site survey, you must configure the handset with an SSID in the Admin menu.

For more information on the Admin menu, see module IP Touch 310/610 WLAN Handset - Configuration .

When the test is started, it is by default in single SSID mode. As you move through the site, the display shows the top four APs detected by the handset. The following figure shows the multiple AP summary display.



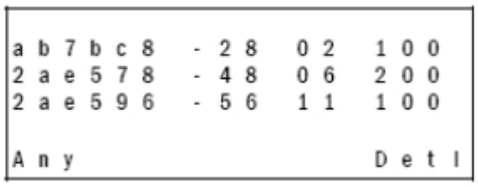
Where:

- **111111** is the last three octets of the on-air MAC address for a discovered AP.
- **22** is the signal strength for the specified AP.
- **33** is the channel number of the specified AP.
- **444** is the beacon interval configured on the specified AP.
- **Any/MyID** is the softkey to toggle between single SSID and any SSID mode.
- **Detl/Smry** is the softkey to toggle between the multiple AP summary display, and the detail display for a single AP.

Note 2:

Numbers racing across the handset display indicate AP information is being obtained. A Waiting message indicates the system is not configured properly and the handset cannot find any APs.

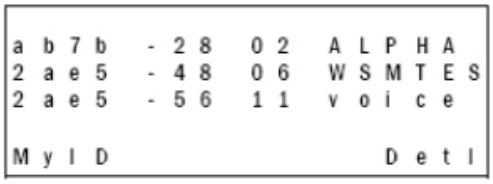
The following screen shows a sample display when there are three APs configured with an SSID that matches that of the handset. The first has a signal strength of –28dbm, is configured on channel 2, with a beacon interval of 100 ms. The second has a signal strength of –48dbm, is configured on channel 6, with a beacon interval of 200 ms. The third has a signal strength of –56dbm, is configured on channel 11 with a beacon interval of 100 ms.



5.2.2.4.2 Any SSID mode

To display all APs regardless of SSID, press the **Any** softkey. The summary display contains

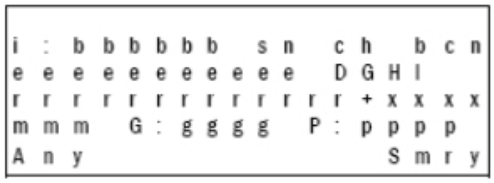
the first six characters of the AP's SSID instead of the beacon interval as shown in the following figure.



To return to single SSID mode, press the **MyID** softkey.

5.2.2.4.3 Detail mode

To display details for one AP, press the **Detl** softkey. Use the Left/Right arrow keys to move between AP indices. The following figure shows the display in detail mode.



Where:

- **i** is the index of selected AP (value will be from 0 to 3 inclusive).
- **bbbbbb** is the last three octets of the BSSID for a discovered AP.
- **sn** is the signal strength in –dbm.
- **ch** is the channel.
- **bcn** is the beacon interval.
- **eeeeeeeeeee** is the SSID (up to first 11 characters).
- **DGHI** is the standards supported.
- **rrrrrrrr** is the rates supported. Basic rates will have a “b” following the rate.
- **+ –** indicates that more rates are supported than those displayed.
- **xxxx** is the WMM or UPSD, if those QoS methods are supported
- **mmm** is the security mode
- **G:gggg** is the group key security.
- **P:pppp** is the pairwise key security.
- **Any/MyID** is the softkey to toggle between “single SSID” and “any SSID” modes.

- **Detl/Smry** is the softkey to toggle between the multiple AP summary display and the detail display for a single AP.

To return to summary mode, press the **Smry** softkey.

5.2.2.5 Maintenance

The Alcatel-Lucent IP Touch 310/610 WLAN Handsets have two modes of operation for handling error messages:

- **Restart On Error**. In this mode the handset recovers from a fatal software error and returns to the standby without user interaction or audible notification.
- **Halt On Error** . In this mode the handset halts operation and displays an error message. In order to restore the handset to normal operation, the user must power off and on the handset, or remove and replace the battery.

In both modes, the handsets save the error message on the Syslog server, if configured. Use the Admin menu to configure the error handling modes.

For information on the Admin menu, see module IP Touch 310/610 WLAN Handset - Configuration § Admin menu .

5.2.2.5.1 Diagnostics

Diagnostics is used to evaluate the overall quality of the link between the handset, AP, and infrastructure equipment, such as the IP, PCX, SVP Server, and gateways. Unlike site survey, Diagnostics is used while the functional code is running, and during a call. With Diagnostics enabled, the handset can display diagnostic screens any time it is in active mode.

Enable Diagnostics in the Admin menu.

To start the display of information, press the **Nav** ◄ or **Nav** ► key.

Only four of the diagnostic counters listed below can be shown at a time. Press the Nav keys multiple times to cycle through the various counters and the normal standby display. The numeric icon at the top of the display indicates what screen number is being displayed. For example, the first time the Nav key is pressed, the 1 icon is shown, and the first four counters are displayed. The next time it is pressed, the 2 icon is shown, and the next four counters are displayed, and so on until there are no more counters to be displayed.

The following figure shows the Diagnostics information displayed on screen 1.

Where:

- **MissedRcvCnt** is the missed receive packet count since power up.
- **MissedXmtCnt** is the missed transmit packet count since power up.

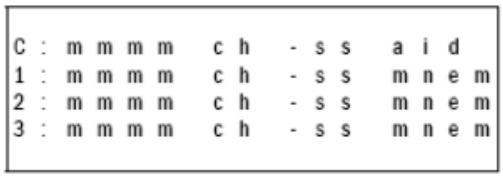
- **RxRetryCount** is the receive retry count since power up.
- **TxRetryCount** is the transmit retry count since power up.

The following figure shows the Diagnostics information displayed on screen 2.

Where:

- **Jitter** is the average error or “wobble” in received packet timing, in microseconds.
- **LastRate** is the last successful transmit data rate.
- **GatewyType** is the Gateway type and **mnemo** is a mnemonic that indicates what type of gateway is being used.

Screen 3 contains a list of the APs discovered. The following figure shows the Diagnostics information displayed for each AP.

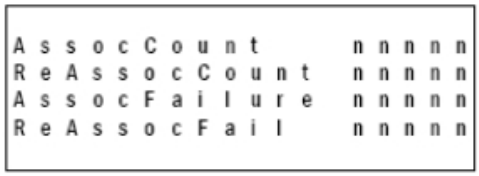


Where:

- **C** indicates this is the current AP. The digit **1, 2,** or **3** indicates this is an index into the list of other APs discovered.
- **mmmm** is the last 2 octets of the MAC address of the AP.
- **ch** is the channel number.
- **ss** is the signal strength.
- **aid** is the 802.11 Association ID from the current AP.
- **mnem** is a mnemonic for the reason code indicating why the handset didn’t hand off to this other AP. Reason codes are:
  - Unkn – reason unknown
  - Weak – signal strength too weak
  - Rate – one or more basic rates not supported

- Full – AP cannot handle bandwidth requirements
- AthT – authentication timeout
- AscT – association timeout
- AthF – authentication failure
- AscF – association failure
- SecT – security handshake timeout
- SecF – security handshake failure
- Cnfg – AP not configured correctly for security, QoS mode, or infrastructure network

The following figure shows the Diagnostics information displayed on screen 4.



Where:

- **AssocCount** is the association count since power up.
- **ReAssocCount** is the re-association count since power up.
- **AssocFailure** is the association failures since power up.
- **ReAssocFail** is the re-association failures since power up.

The following figure shows the Diagnostics information displayed on screen 5.

Where:

- **Sec-ErrCount** is the security error count since power up.
- **LstSecErrSeq** is the MAC sequence number of frame with last security error.

5.2.2.5.2 Syslog mode

You can configure a handset to send messages to a Syslog server present on the network. The information helps you to characterize a problem, identify a malfunction, or collect statistics

on a periodic basis.

A Syslog server must be present on the network in order for the handset to send the log messages and have them saved. You find the Syslog server with DHCP option 7 if the handset is using DHCP. If static addresses are used, configure the Syslog server's IP address in the Admin menu.

All Syslog messages include:

- Date and time (to 1/100th of second) elapsed since handset power on (currently set to Jan-1 00:00.00)
- The handset's MAC address
- The handset's IP address
- A sequence number

Messages are formatted like the following example:

Jan 1 00:01:26.72 0090.7a02.2a1b (172.16.0.46) [001a] RStat: AP 00:40:96:48:1D:0C (-56 dBm), Sent 783523, Recvd 791342, MSnt 245, MRcd 5674, BSnt 43, BRcd 10783, TX drop 43 (0.0%), TX retry 578 (1.2%), RX retry 1217 (1.6%)

In the Admin menu, you can configure three levels of logging:

- **Errors** - the handset logs only messages considered to be errors
- **Events** - the handset logs errors, plus other interesting events
- **Full** - the handset logs all errors and events, plus additional information

The following table lists the Syslog messages, which level of logging produces them, and the additional information provided for each message type.

Message type	**Errors**	**Events**	**Full**	**Additional information in message**
Failed Handoff	Yes	Yes	Yes	- Failed Access Point (AP) MAC - Failed AP signal strength - Current AP MAC - Current AP signal strength - Failure reason
Successful Handoff	No	Yes	Yes	- New AP MAC - New AP signal strength - Old AP MAC - Old AP signal strength - Reason for handoff - Other candidate APs: MAC, Signal strength, Reason not used
Security Error	Yes	Yes	Yes	- AP MAC - AP signal strength - Security mode - Error details (mode-dependent)
Call Start/End	No	Yes	Yes	Call Start only: - Call type (telephony, OAI, PTT) Call Start and End: - AP MAC - AP signal strength

Message type	Errors	Events	Full	Additional information in message
Audio stats	No	No	Yes (every 5 secs)	- AP MAC Payloads received - AP signal strength - Payload size (in msec) - Payloads sent - Payloads missed (not received) - Payloads missed rate (over last 5 seconds) - Payloads late - Payloads late rate (over last 5 seconds) - Average jitter
Audio error threshold exceeded	Yes	Yes	Yes	Same as audio stats
Radio stats	No	No	Yes (every 5 secs)	- AP MAC - AP signal strength - Directed packets sent - Directed packets received - Multicast packets sent - Multicast packets received - Broadcast packets sent - Broadcast packets received - TX dropped count - TX drop rate (over last 5 seconds) - TX retry count - TX retry rate (over last 5 seconds) - RX retry count - RX retry rate (over last 5 seconds)
Radio error threshold exceeded	Yes	Yes	Yes	Same as radio stats

The following table lists the codes that indicate the reason for the handoff in Syslog mode.

Code	Handoff Reason
0	OK
1	TOO_FEW_AVERAGE_PROBES
2	WORSE_SIGNAL
3	INVALID_SSID
4	NO_PARAMS_FOUND
5	BAD_RATES
6	OFF_CHANNEL_PROBE_RESP
7	AP_TOO_BUSY
8	AUTH_TIMEOUT

Code	Handoff Reason
9	ASSOC_TIMEOUT
10	FAILED_AUTHENTICATION
11	FAILED_ASSOCIATION
12	SOFT_NEIGHBOR
13	NO_SIG_IMPROVEMENT
16	NO_KEEPALIVE
17	LOST_AUDIO
18	NO_RESPONSE
19	NO_PRIVACY
20	APP_UNHAPPY
21	DISASSOCIATED
22	NO_HANDOFF
23	HANDOFF
24	INITIAL_ASSOC
25	LOST_AP
26	TX_FAILURES
27	CHANGING_RATES
28	UNDEFINED
29	EAP_START_TIMEOUT
30	LEAP_CHALLENGE_TIMEOUT
31	EAP_SUCCESS_TIMEOUT
32	LEAP_CHALLENGE_RESPONSE_TIMEOUT
33	NONCE_CCKM_TIMEOUT
34	RSNIE_AP_TIMEOUT
35	NONCE_GTK_TIMEOUT
36	EAPOL_LOGOFF
37	EAPOL_FAILURE
38	NO_WPA_ELEMENT
39	BAD_MIC
40	BAD_PROBE_RESP
41	BAD_CAP_INFO_AD_HOC
42	ACTION_TIMEOUT
43	FAILED_ACTION
44	DELTS
45	QOS_REQUIRED
46	CHANGED_LISTEN_INTERVAL

5.2.2.5.3 Status messages

Status messages provide information about the handset's communication with the Access Points (AP) and the PCX. The following table summarizes, in alphabetical order, the status messages.

Status Message	Description	Action
3 chirps	Handset is not able to communicate with the best AP, probably because that AP has no bandwidth available.	None. This is only a warning, the call will hand-off to the best AP once it becomes available.
Address Mismatch	Handset software download files are incorrect or corrupted.	Download new software.
Assoc Failed xxxxxxxxxxxx	x…x – AP MAC address Handset association was refused by AP; displays MAC of failing AP.	Check handset and AP security settings. Ensure AP is configured per Configuration Note. Try another AP.
Assoc Timeout xxxxxxxxxxxx	x…x – AP MAC address Handset did not receive association response from AP; displays MAC of failing AP.	Check handset and AP security settings. Ensure AP is configured per Configuration Note. Try another AP.
Auth Failed xxxxxxxxxxxx	x…x – AP MAC address Handset authentication was refused by AP; displays MAC of failing AP.	Check handset and AP security settings. Ensure AP is configured per Configuration Note. Try another AP.
Auth Timeout xxxxxxxxxxxx	x…x – AP MAC address Handset did not receive authentication response from AP; displays MAC of failing AP.	Check handset and AP security settings. Ensure AP is configured per Configuration Note. Try another AP.
Bad Code Type xx Expected Code Type yy	xx, yy – software licence types Handset software does not match current handset licence selection.	Download new software.
Bad Config	Some needed configuration parameter has not been set.	Check all required handset configuration parameters for valid settings.
Bad SSID	The handset is configured for “static SSID” (as opposed to “Learn once” or “Learn always” and no SSID has been entered.	Enter an SSID in the configuration settings or change to one of the “Learn” modes.
Bad Phintl File	Handset software download files are incorrect or corrupted.	Download new software.
Bad Program File	Handset software download files are incorrect or corrupted.	Download new software.

Status Message	Description	Action
Bad Term, Type	Gatekeeper rejected registration request from the handset.	Verify the gatekeeper or PCX's configuration
(battery icon), Battery Low, beep (audio)	Low battery.	In call: the battery icon displays and a soft beep will be heard when the user is on the handset and the Battery Pack charge is low. User has 15–30 minutes of Battery Pack life left. The Battery Pack can be changed while the call is still in progress. Do not press END. Place call on Hold or Park. Quickly remove the discharged Battery Pack and replace with a charged Battery Pack, START the handset, and press START to resume the call in progress. Not in call: The battery icon displays whenever the Battery Pack charge is low. The message Battery Low and a beep indicate a critically low Battery Pack charge when user is not on the handset. The handset will not work until the Battery Pack is charged.
Battery Failure	The Battery Pack is not functioning.	Replace the Battery Pack with a new or confirmed Battery Pack.
Battery Failed	Battery Pack is damaged or incompatible with handset.	Replace the Battery Pack with a new or confirmed Battery pack.
Can't Renew DHCP yyy.yyy.yyy.yyy	y…y – DHCP server IP address DHCP server is not responding to initial renewal attempt.	Configuration problem. Check the IP address configuration in the DHCP server.
Charging …	The handset is charging in the Desktop Charger.	No action needed.
Charge Complete	The handset is now fully charged.	No action needed.
Checking Code	Handset is contacting the TFTP Server to determine if it has a newer version of software that should be downloaded.	None, this message should only last for approximately one second. If message remains displayed, END and replace the handset.

Status Message	Description	Action
Checking DHCP IP	The handset is retrieving DHCP information from the DHCP server.	None. This is informational only.
Code Mismatch!	The software loaded into the handset is incorrect for this model handset.	Verify that the Licence Option value is correct. Replace the software image on the TFTP server with software that is correct for the handset model.
Connect Timeout	Wireless Telephone is not provisioned on the system. Message will display if no CONNECT message is received from the PCX within 30 seconds of the start of initialization.	Handset will restart after 20 seconds. If unsuccessful, check PCX configuration.
CRC Code Error	The software which has been TFTP downloaded has a bad redundancy code check.	Try the download again; it is possible the software was corrupted during download. If the error repeats, check that the download image on the TFTP server is not corrupted.
DCA Timeout	The handset has detected a fault for which it cannot recover, possibly due to a failure to acquire any network.	Turn the handset off then on again.
DHCP Error 1.	The handset cannot locate a DHCP server.	The handset tries every four seconds until a server is located.
DHCP Error 2.	The handset has not received a response from the server for a request to an IP address.	The handset retries until a server is found.
DHCP Error 3.	The server refuses to lease the handset an IP address.	The handset keeps trying.
DHCP Error 4.	The server offered the handset a lease that is too short. The minimum lease time is 10 minutes, but one hour minimum lease time is recommended.	The handset stops trying. Reconfigure the server and power the handset off and on.
DHCP Error 5.	Failure during WEP Key rotation process.	

Status Message	Description	Action
DHCP Lease Exp yyy.yyy.yyy.yyy	y…y – DHCP Server IP address. DHCP is not responding to renewal attempts (at least one renewal succeeded).	The handset failed to renew its DHCP lease, either because the DHCP server is not running, or because the configuration has been changed by the administrator. The handset will attempt to negotiate a new lease, which will either work or change to one of the above DHCP errors (1-4).
DHCP NACK error yyy.yyy.yyy.yyy	y…y – DHCP server IP address. DHCP server explicitly refused renewal.	The DHCP lease currently in use by the handset is no longer valid, which forces the handset to restart. This problem should resolve itself on the restart. If it does not, the problem is in the DHCP server.
DL Not On Sector	Handset software download files are incorrect or corrupted.	Download new software.
DO NOT POWER OFF	The handset is in a critical section of the software update.	None. Do not remove the Battery Pack or attempt to END the handset while this is displayed. Doing so may render the handset inoperable.
Duplicate IP	The handset has detected another device with its same IP address.	If using DHCP, check that the DHCP server is properly configured to avoid duplicate addresses. If using Static IP, check that the handset was assigned a unique address.
Erase Failed	Download process failed to erase the memory in the handset.	Operation will retry but may eventually report the error "int. error: 0F." Power cycle the handset.
Erasing Memory	Handset has determined that a download should occur and is erasing the current software from memory. This message also displays a progress bar. When the progress bar fills the display line the erase operation is complete.	None. When the progress bar fills the display line the erase operation is complete. Do not turn the handset off during this operation.

Status Message	Description	Action
Error!... [error details]	A fatal software error is detected. All handset operation is halted and any call is lost.	This message appears during Halt on Error mode. An error message is displayed. Note the message details and power cycle the handset.
Error in Config	Indicates an error in one of the static IP addresses set in the Admin menu.	Correct static IP addresses in the Admin menu.
Files Too Big	Handset software download files are incorrect or corrupted.	Download new software.
Flash Config Error	Handset internal configuration is corrupt.	Perform "Restore Defaults" operation via Admin menu, or reprogram with Handset Administration Tool.
Incompatible	The switch is rejecting the software version presented by the phone.	
Initializing …	The handset is performing START initialization.	None. This is informational only.
Internal Err. # #	The handset has detected a fault from which it cannot recover. OE – Error while writing the Flash (return handset to factory). OF – No functional code (contact technical support).	Record the error code so it can be reported. Turn the handset off then on again. If error persists, try registering a different handset to this telephone port.
Multiple GW Reg yyy.yyy.yyy.yyy	y…y – Gateway IP address. Handset received responses from multiple gateways; displays IP address of one responding gateway.	Check each Telephone Gateway for the handset's MAC address on the Telephone Line Configuration screen. Delete any duplicate entries, leaving only one entry on the correct Telephone Gateway and port for this handset.
Multiple SVP Reg yyy.yyy.yyy.yyy	y…y – SVP Server IP address. Handset received responses from multiple SVP Servers; displays IP address of one responding SVP Server.	This can happen if the handset has been re-configured to use a different SVP Server and then powered-up before the previous server has had time to determine that the handset is no longer connected to it. The problem should go away after about 30 seconds.

Status Message	Description	Action
Must Upgrade SW!	Handset software is incompatible with hardware.	Download new software.
Net Busy xxxxxxxxxxxx	x…x – AP MAC address. Handset cannot obtain sufficient bandwidth to support a call; displays MAC of failing AP.	Try the call again later.
No Answer	Called party did not answer the handset.	No action. Not an error.
No DHCP Server	Handset is unable to contact the DHCP server.	Check that DNCP is operational and connected to WLAN or use Static IP configuration in the handset.
No SSID	Attempted to run site survey application without an SSID set.	Let handset come completely up. Statically configure an SSID in the Admin menu.
No Func Code	Handset software download files are incorrect or corrupted.	Reconfigure the handset to gain access to the WLAN and download new code.
No Host IP (Addr)	The handset is configured for “static IP” (as opposed to “use DHCP”) and no valid host IP address (the handset’s IP address) has been entered.	Enter a valid IP address in the configuration settings or change to “use DHCP”.
No IP Address	Invalid IP.	Check the IP address of the handset and reconfigure if required.
No Net Access	Cannot authenticate / associate with AP.	Verify the AP configuration. Verify that all the WEP settings in the handset match those in the APs.
No Net Found No APs	Handset cannot find any APs. This indicates any of the following: - No radio link. - No SSID – Incorrect SSID. - AP does not support appropriate data rates. - Out of range. - Incorrect security settings	Verify that the AP is turned on. Verify the SSID of the wireless LAN and enter. Check the AP configuration against configuration document for AP. Try getting closer to an AP. Check to see if other handsets are working within the same range of an AP. If so, check the SSID of this handset. Verify that all the Security settings in the handset match those in the APs.

Status Message	Description	Action
No Net Found xxxxxxxxxxxx yy	x…x – AP MAC address. yy – AP signal strength. Handset cannot find a suitable AP; displays MAC and signal strength of “best” nonsuitable AP found.	Check AP and handset network settings such as SSID, Security, Reg domain and Tx power. Ensure APs are configured per Configuration Note Try site survey mode to determine more specific cause.
No NOE DHCP	DHCP is configured but no valid NOE option 43 was found.	Check DHCP configuration for option 43 and reconfigure if required.
No PBX Response	The handset has exceeded its retransmission limit with no ACK response from proxy server.	Verify that proxy server IP address and port are properly configured.
No Reg Domain	Regulatory Domain not set.	Configure the Regulatory Domain of the handset.
No SVP IP	The handset is configured for “static IP” (as opposed to “use DHCP”) and no valid SVP Server address has been entered.	Enter a valid SVP Server IP address in the configuration setting or change to “use DHCP.”
No SVP Response yyy.yyy.yyy.yyy	y…y – SVP Server IP address. Handset has lost contact with the SVP Server.	This may be caused by bad radio reception or a problem with the SVP Server. The handset will keep trying to fix the problem for 20 seconds, and the message may clear by itself. If it does not, the handset will restart. Report this problem to the system administrator if it keeps happening.
No SVP Server	Handset can’t locate SVP Server. SVP Server is not working. No LAN connection at the SVP Server.	IP address configuration of SVP Server is wrong or missing. Check error status screen on SVP Server. Verify SVP Server connection to LAN.
No SVP Server No DNS Entry	Handset unable to perform DNS lookup for SVP Server, server had no entry for SVP Server.	The network administrator must verify that a proper IP address has been entered for the SVP Server DHCP option.
No SVP Server No DNS IP	Handset is unable to perform DNS lookup for SVP Server, no IP address for DNS server.	The network administrator must verify proper DHCP server operation.

Status Message	Description	Action
No SW Found	A required software component has not been identified.	Check that the handset licence type has a corresponding entry in the slnk_cfg.cfg file. Check that the pd14ccc.bin and pi1400.bin entries exist under this license type in the slnk.cfg.cfg file.
Not Installed!	A required software component is missing.	Check that all required software files are on the TFTP server, if over-the-air downloading is being used. If the error repeats, contact technical support.
Phone Restarting	If the handset is not able to register at first try, the message is displayed for 20 seconds while it restarts. It also displays if the PCX causes the handset to restart.	None. If the handset does not register after a restart, check the configuration in the Admin menu and the PCX.
Press END	The far end of a call has hung up.	Hang up the near end.
Restarting…	The handset is in the process of rebooting. There will be a 20-second delay in an attempt to let potential network/system errors clear.	None.
Select Licence	The correct protocol has not been selected from the licence set.	Using the administrative menus, select one licence from the set to allow the handset to download the appropriate software.
Server Busy	Handset is attempting to download from a TFTP Server that is busy downloading other devices and refusing additional downloads.	None, the handset will automatically retry the download every few seconds.
Service Unavailable. Restarting…	An error has caused the handset to lose the call. It is now making its best effort to restart and return to standby mode.	Occurs during Restart on Error mode. The handset is attempting to register with the PCX and resume normal operation. Error details may be available through the Syslog server and by download with the Handset Administration Tool.

Status Message	Description	Action
Service Rej.	The SVP Server has rejected a request from the handset.	The handset will restart and attempt to reregister with the SVP Server, which should fix the problem. Report to your administrator if it keeps happening.
SKT Open Failed	Socket open fail. Occurs when the handset tries to connect to the PCX but there is no response. If resiliency is active, the handset will keep trying.	If the PCX is inoperative and resiliency is not active or the handset cannot locate a backup PCX, turn off the handset and repair the primary PCX. Note that it may be advisable to reconfigure the backup PCX to be the primary PCX if the repair is more time-consuming than the reconfiguration.
Socket Failure	Handset cannot communicate with the AP or the SVP Server.	This message may display with another diagnostic message. Follow diagnostic actions for the second message (such as No Net Found).
Storing Config	Handset is storing changes to handset configuration.	None. Informational only. The handset may display this briefly following a configuration change or software download.
SVP Service Rej.	The SVP Server has rejected a request from the handset.	The handset will restart and attempt to reregister with the SVP Server.
System Busy yyy.yyy.yyy.yyy	y…y – SVP Server IP Address. SVP Server has reached call capacity.	All call paths are in use. Try the call again in a few minutes.
System Busy	SpectraLink Voice Priority Processor is busy or out of resources.	All call paths are in use, try call again in a few minutes.
System Locked (with Busy Tone)	SpectraLink Voice Priority Processor is locked.	Try call again later, the system has been locked for maintenance

Status Message	Description	Action
TFTP ERROR(x):yy	A failure has occurred during a TFTP software download. (x) = The file number which was being downloaded. yy = an error code describing the particular failure. Possible error codes are: - 01 – TFTP server did not find the requested file. - 02 – Access violation (reported from TFTP server). - 07 – TFTP server reported "No such user" error. - 81 – File put into memory did not CRC. - FF – Timeout error. TFTP server did not respond within a specified period of time.	Error code 01, 02 or 07 – check the TFTP server configuration. Error code 81 – the handset will attempt to download the file again. For other messages, END the handset, then turn it on again to retry the download.
Too Many Errors	The handset continues to reset and cannot be recovered.	Fatal error. Replace handset.
Unknown xx:yy:zz	A phrase is missing from the phintl file.	Download new software.
Unsupported Codec	The proxy server has requested using a codec not supported by the handset.	Check proxy server configuration for supported codecs and reconfigure if necessary.
Updating …	The handset is internally updating its software images.	None. The handset may do this briefly after a download. This is informational only.
Updating Code…	Handset is downloading new software into memory. The number icons at the bottom of the display indicate which file number is currently being downloaded. This message also displays a progress bar. When the progress bar fills the display line the update operation is complete on that file.	None. When the progress bar fills the display line the update operation is complete on that file. Do not turn the handset off during this operation.
Waiting…	Handset has attempted some operation several times and failed and is now waiting for a period of time before attempting that operation again.	None. The handset is waiting for a specified period of time before attempting that operation again.

Status Message	Description	Action
Wrong Code Type	The software loaded into the handset is incorrect for this model handset.	Verify the licence type is set correctly. If the licence type is correct, replace the software image on the TFTP server with the software that is correct for the handset model.

5.2.3 Mobile IP Touch 300/600

5.2.3.1 Description

5.2.3.1.1 Alcatel-Lucent Mobile IP Touch 300/600 Overview

Figure 5.104 : Alcatel-Lucent Mobile IP Touch 300/600

1	Earpiece		10	Power OFF/End Call
2	Up		11	Menu
3	Select and Call by name		12	Function
4	Down		13	Line
5	Softkey A		14	Microphone
6	Softkey B		15	Charging contacts
7	Softkey C		16	Headset jack
8	Softkey D		17	Battery release
9	Power ON/Start Call		18	Push-to-talk radio control

Specifications

Radio frequency	2.4000 – 2.4835 GHz
Transmission type	Direct Sequence Spread Spectrum (DSSS)
Transmit data rate	Up to 11Mb/s
Radio QoS	Voice Priority (SVP)
Wireless security	- Wired Equivalent Privacy (WEP), 40 and 128 bit - WPA - WPA2
FCC certification	Part 15.247
Management	DHCP, TFTP
Voice encoding	G.711 (A and mu-law)/G.729A
VoIP Protocols	Alcatel-Lucent New Office Environment (NOE)
Transmit power	100 mW peak <10 mW average
Display	Pixel-based (up to 4-line x 18-characters) alphanumeric + One icon line + One line for soft keys
Alcatel-Lucent Mobile IP Touch 300 dimensions	5.5” x 2.0” x 0.9” (14.0 x 5.1 x 2.3 cm)
Alcatel-Lucent Mobile IP Touch 600 dimensions	5,9” x 2,2” x 1,0” (15,0 x 5,6 x 2.5 cm)
Alcatel-Lucent Mobile IP Touch 300 weight	4.2 ounces (119.0 g)
Alcatel-Lucent Mobile IP Touch 600 weight	6,0 ounces (170.1 g)
Battery capacity	4 hours talk time, 80 hours standby

5.2.3.1.2 Configuration

Each handset must be configured before use. Set configuration data includes:

- Standard IP set data: IP address, subnet mask, gateway IP address, TFTP IP address
  This data can be configured either manually or automatically by a DHCP server
- CLID number. This number is known in the PCX
- SVP server IP address
  This data can be configured either manually or automatically by a DHCP server
- SSID (Service Set IDentifier). This identifier is used for security and WLAN identification.
- Licence management: defines the protocol used. Enter 015
- Regulatory domain: defines the available channels. In the US enter: 01. Enter 02 for Europe. The line key manages this parameter.

For more information onAlcatel-Lucent Mobile IP Touch 300/600, see the handset's User Guide.

5.2.3.1.3 Switch On

When a handset is switched on, it:

- Associates to the nearest Access Point (AP)
- Requests update from the TFTP server. Binaries can be downloaded if required
- Requests registration from the SVP server. The Private IP address is transmitted
- Requests the lanpbx-mipt.cfg file from the TFTP server. This file contains its associated Call Server address. The lanpbx.cfg file, used on wired IPTouch sets, is not required on IP Touch WLAN handsets.
- Requests registration from its associated Call Server. The handset directory number and the password is requested at the first connection

When the handset is roaming the AP association can be changed.

5.2.3.1.4 System Functions

These functions are enabled/disabled by the system administrator using an access password.

IP Configuration

The handset has two modes for IP configuration:

- DHCP configuration.
- Static IP. In this mode, the administrator has to enter the IP addresses manually for each set.

Security

The handset can work in the following modes:

- No security: in this mode there is no authentication or encryption. This mode is only acceptable in a safe or trusted environment.
- WEP: authentication and encryption according to WEP standards
- WPA/PSK: authentication and encryption according to WPA/PSK standards
- WPA2: authentication and encryption according to WPA2 standards

Power Transmission

As of R1.1, the transmission power of a handset can be adjusted according to the radio environment.

Push to Talk Mode

The Alcatel-Lucent Mobile IP Touch 600 can work in the Push to talk mode (when validated). In this mode, the handset works as a walkie-talkie. All users in Push to Talk mode can hear the talking users.

Up to 8 push to talk channels can be used. As of R1.1, the system administrator can define the channels available, for each handset.

This mode limits the battery autonomy and data transmissions. The option **Ethernet multicast Support** must be enabled on the OAW.

In this mode, the Alcatel-Lucent OmniPCX Enterprise Communication Server and the SVP server are not used.

Syslog Mode

As of R1.1, a Syslog server can be defined. This server records the event history for the set, which can be used for further system diagnosis.

Site Survey Mode

This mode allows checks on the coverage area. The handset displays the signal radio strength and information on the associated AP.

5.2.3.1.5 User Functions

Lock Key

This function allows the user to lock the keypad and avoids accidental activation.

Ring Options

This function allows the user to choose the ring cadence, tone and volume of and/or vibrator.

Noise Mode

This function allows the user to choose the handset behavior according to the environmental noise.

Key Tone

This function allows the user to enable/disable a beep when a key is pressed.

Warning Tone

This function allows the user to enable/disable a beep on special events such as switch on or leaving coverage area.

Display Contrast

This function allows the user to modify the display contrast.

Keypad Autolock

This function allows the user to enable/disable an automatic keyboard lock after an inactivity time-out.

5.2.3.2 Configuration

5.2.3.2.1 Overview

There are two menus to configure the Alcatel-Lucent Mobile IP Touch 300/600:

- The management menu
  This menu allows the administrator to define functional parameters. It can be protected by a password.
- The preferences menu
  This menu allows users to customize their set

For information on cradle configuration for Alcatel-Lucent Mobile IP Touch 300/600, see § Cradle Configuration .

Navigating in Menus

To navigate within the menus, use the keys located on the left hand side of the handset.

Once a menu item is selected, contextual softkey options are displayed. The common softkey options include:

- **OK** to edit or activate an option
- **UP** to come back to the previous menu
- **SAVE** to validate
- **EXIT** to leave the menu
- **bksp** (backspace) to correct a character entry

Alphanumeric String Entry

Press the first digit/letter. The digit displays. Press the key again to scroll through the letters associated with that key.

Example: if you press 2 repeatedly, you see 2, A, B and C, a, b and c.

The following table indicates keys used to enter characters not represented on the keypad.

To enter	**Press**
Z or z	9
Q or q	7
Space	0
. - _ ! # $ % & ' ( ) , ; / \ = @ ~	1

When the correct entry is displayed, use the right arrow to validate the selection and move on to the next character.

- Press the left arrow or Bksp softkey to erase the previous character.
- Press the Save softkey to save the entry.

- Press the UP softkey to abort and return to the menu without saving any changes.

5.2.3.2.2 Management Menu

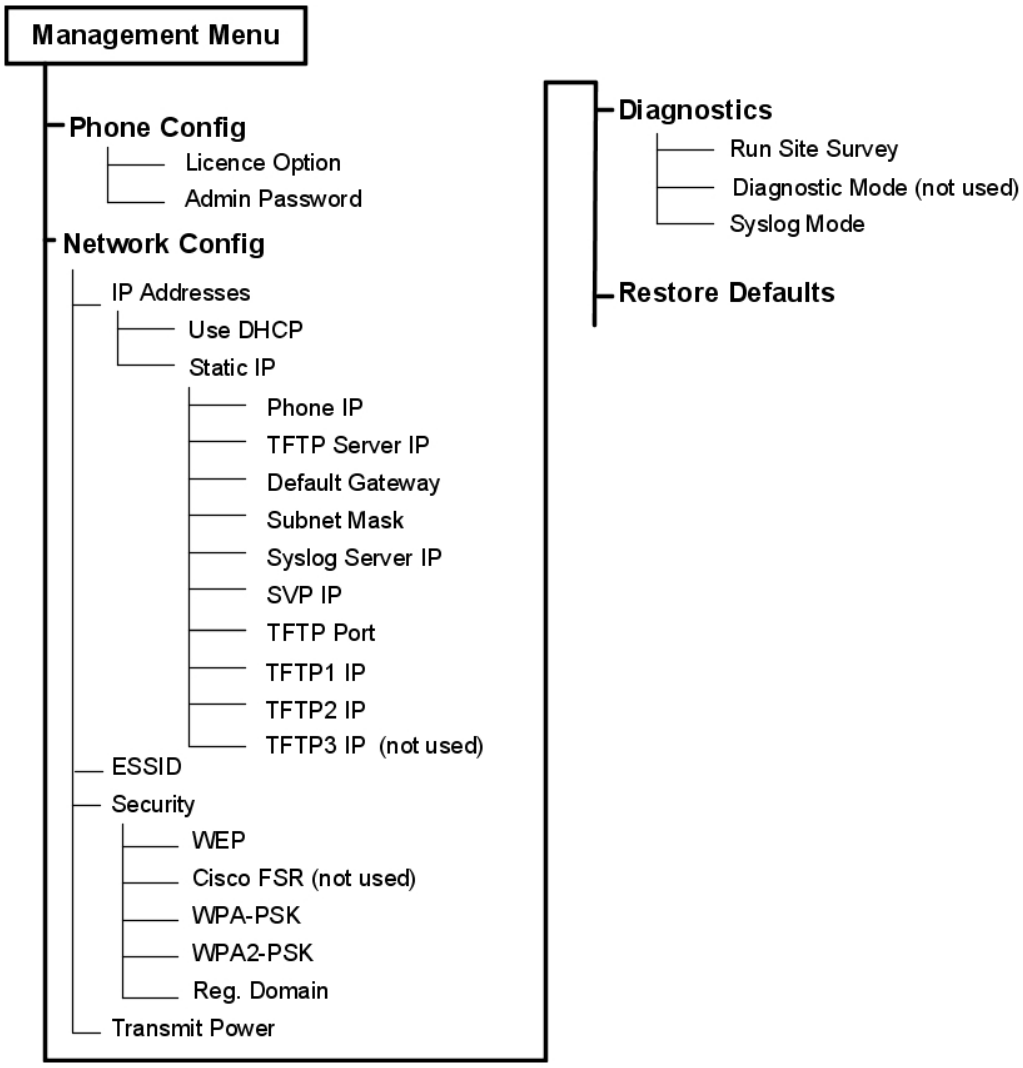
Access

To access the management menu:

1. Check that the handset is switched off.
2. Press the ON (green) and OFF (red) keys simultaneously.
3. Release the ON (green) key, then release the OFF (red) key.

The first level of the management tree structure is displayed.

Menu Tree Structure



Phone Configuration

Licence Option

The licence number must correspond to the VoIP protocol used in the system.

Select: 015 in the list

Admin Password

Configure a password to protect access to the handset's management menu (recommended).

Enter a password made up of numbers.

Network configuration

IP addresses

When the DHCP option is chosen, the handset sends a request to the DHCP server for the IP address information. The DHCP server parameters must support the following options:

- 01: Subnet Mask
- 03: Default Gateway
- 07: Syslog server
- 66: TFTP server
- 151: Specific option used for the SVP server IP address.

When the Static IP option is chosen, the IP addresses are entered manually by the administrator.

- **Phone IP**: enter the digits only including the leading zeros.
- **TFTP Server IP**: enter the IP address of a TFTP server which holds a software image for updating the handsets.
- **Default gateway** and **Subnet mask**: used to identify the subnets, when using a network that includes routers.
- **Syslog Server IP**: enter the IP address of the syslog server used to centralize messages coming from the handsets.
- **SVP Server IP**: enter the SVP server IP address.
- **TFTP Port:** port to use for all TFTP requests after firmware download.
- **TFTP1 IP**: primary TFTP server (possibly the PCX) used to download the lanpbx-mipt.cfg file.
- **TFTP2 IP**: redundant TFTP server (possibly the PCX) used to download the lanpbx-mipt.cfg file.
- **TFTP3 IP**: not used.

ESSID

The handset must know the Extended Service Set IDentification (ESSID) to be able to connect to the wireless network.

Select the option that will enable the handset to acquire Access Points (APs) with the correct ESSID each time it is turned on.

Note:

Broadcast ESSID must be enabled in the OmniAccess Wireless switch for the ESSID automatic learning to function. Refer to the Configuration Note of the OmniAccess Wireless LAN switch.

Overlapping wireless systems complicate the use of ESSID learning as the handset can receive conflicting signals. If this situation exists on your site, use Static Entry or Learn Once in an area without overlapping ESSIDs.

- **Learn Once**: allows the handset to scan all. Once either is found, the handset retains the ESSID from whichever access point it associates with at that point. When overlapping wireless systems exist, the Learn Once feature allows the handset to use only the ESSID established at first learn at all subsequent uses.

  This ESSID is retained by the handset until the ESSID option is reconfigured.
- **Learn Always**: allows the handset to automatically learn the ESSID at each power on or

loss of contact with the wireless LAN (out of range). This can be useful if the handset is used at more than one site.

- **Static Entry**: allows you to enter the correct ESSID manually following the alphanumeric string entry technique. This method is recommended for a secure WLAN solution.

Security

The handset's security configuration must be performed according to the OmniSwitch parameters.

Select the security mode:

- **None**: disables any encryption and security authentication mechanisms.
- **WEP**: The WEP mechanism is enabled.
  - **WEP On/Off:** this parameter enables/disables WEP data encryption
  - **Authentication** then **Shared key**: this parameter enables the authentication mechanism (not recommended)
  - **Key information**: this menu allows you to enter the WEP key parameters:
    - **Default key**: this parameter defines the reference of the default key (enter 1 to 4)
    - **Key length**: this parameters defines the key length (40-bit or 128-bit)
    - **Key #1** to **Key #4**: enter the value of the keys 1 to 4. Usually only one key is used. The keys 2 to 4 are optional.
- **WPA/PSK**: The WPA/PSK mechanism is enabled.
  - **Passphrase**: enter the passphrase and validate, the shared key is created by the handset
- **WPA2/PSK**: WPA2/PSK is enabled.
  - **Passphrase**: enter the passphrase and validate. The shared key is created by the handset

Reg. Domain

The regulatory domain defines the frequencies and the maximum legal power level.

Select the area where the system is installed:

- 01 FCC (North America)
- 02 ETSI (Europe & Asia-Pacific)

Note:
the choices 04 (Spain) and 05 (France) are not used.

Transmit Power

The transmit power can be defined. Possible values: 5, 10, 15, 20, 30, 50 and 100mW (Default value: 100mW).

Select the adequate transmit power and validate.

Diagnostics

SYSLOG Mode

Events and error messages can be sent to a syslog server running in the network. Select

working mode:

- Errors: only the error messages are sent to the syslog server.
- Events: only the event messages are sent to the syslog server
- Full: the error and event messages are sent to the syslog server

Run Site Survey

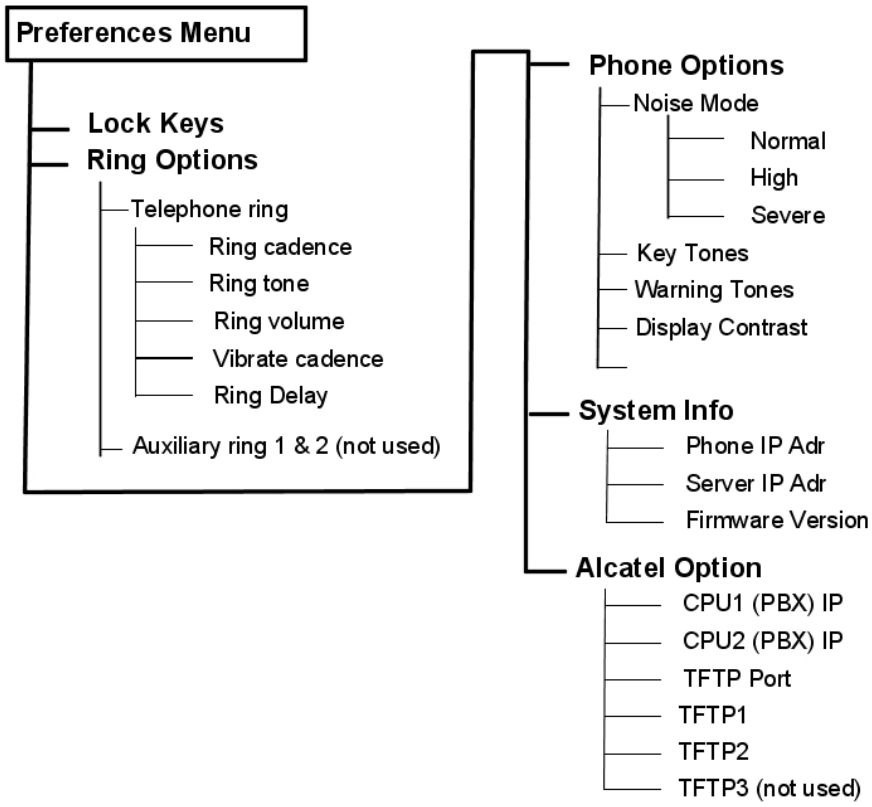
This feature is used to check the coverage area. For more information, see: module Mobile IP Touch 300/600 - Survey Mode .

5.2.3.2.3 Preferences Menu

Access

With the handset switched ON and in standby state, press briefly the « FCN » key.

Menu Tree Structure



Lock Keys

This option locks the keypad:

- Lock: press **OK**
- Unlock: press the **Unlk** softkey and then # key.

Ring Options

This menu provides options to manage the ringing (cadence, tone, volume) and the vibrator (cadence).

Phone Options

Noise Mode

This option is used to take into account the background noise level in the environment. The normal mode is recommended for most conditions. For High or Severe modes you may find it difficult to be heard on your wireless phone.

- Normal: for most office environments
- High: for moderate background noise
- Severe: for extremely noisy conditions

Key Tones

This option enables or disables a beep sound to be generated when a key is pressed.

Warning Tones

This option enables or disables a beep sound to be generated when certain events occur on the handset; switch on, out of range.

Display Contrast

This option adjusts the contrast of the display from 0 to 100% (default: 50%).

Keypad Autolock

This option automatically locks the keypad when no key is pressed. The delay can be configured for 5, 10 or 20 seconds.

System Info

Phone IP Addr

This option displays the IP address currently assigned to the phone (static or DHCP) and the alias IP address assigned to the phone by the SVP server.

Server IP Addr

This option displays the IP address of the SVP server in which the phone is registered.

Firmware Version

This option displays the software version loaded in the phone. This is indicated during the startup display.

Alcatel Option

- CPU1(PBX) IP: displays the IP address of the associated PCX (main)
- CPU2(PBX) IP: displays the IP address of the associated PCX (standby)
- TFTP Port: displays the IP address of the TFTP port
- TFTP1: displays the IP address of the primary TFTP1 server used to download the lanpbx_mipt.cfg file.
- TFTP2: displays the IP address of the redundant TFTP server used to download the lanpbx_mipt.cfg file.
- TFTP3: not used

5.2.3.2.4 Cradle Configuration

System Requirements

Windows NT/200/XP

Safety Reminder

- Only use the original Alcatel-Lucent plug-in power adapter
- Do not immerse the cradle in water or other liquid. Do not pour liquids into the slots

- Do not place anything in the cradle other than the Alcatel-Lucent Mobile IP Touch 300/600. You might damage the contacts. Bent contacts can prevent the cradle from working properly
- The cradle operates in a 50° to 85°F (10 to 30°C) environment. Do not expose it to freezing temperatures or direct sunlight

Configuration Cradle Overview

The configuration cradle is a two-slot cradle designed to automate the process of configuring the Alcatel-Lucent Mobile IP Touch 300/600. The front slot of the cradle is for the Alcatel-Lucent Mobile IP Touch 300/600, the rear slot is for the Alcatel-Lucent Mobile IP Touch 600. Only one handset may be configured at a time.

The configuration cradle is connected to a PC via a serial cable. The configuration cradle program runs on the PC and enables the system administrator to establish and store configuration options for System, Group and User levels. The configuration cradle program can be downloaded from the Alcatel-Lucent website: http://www.businesspartner.alcatel-lucent.com.

Configuration plans may be set up in the program and downloaded into a handset, or a configured handset may be placed in the cradle and its configuration may be uploaded, edited or saved.

Installing the Configuration Cradle

Set up the configuration cradle by first obtaining the appropriate Alcatel-Lucent power supply for your country, or region. Place the configuration cradle on a flat, horizontal surface and plug the power supply into the configuration cradle and into an appropriate wall outlet. Plug a straight serial cable into the configuration cradle and into an available serial port on the PC.

Note:

The serial cable must be plugged directly into the serial port on the PC. Please do not use port replicators or adaptors, as these do not properly handle the necessary communication requirements between the configuration cradle and the PC.

Set up a folder for Alcatel-Lucent Mobile IP Touch 300/600 configuration on the PC and download the programming software from the Alcatel-Lucent website: http://www.businesspartner.alcatel-lucent.com into this folder. Run the PhoneConfig.exe file.

Note that there is no uninstaller since the program does not modify your system or registry. It runs from its current location and stores its settings locally.

Serial port settings are handled automatically by the configuration cradle software. If necessary, the COM port the cradle is using can be set in the **Settings** menu.

Planning the Configuration Files

Each configurable option may be categorized as one of three types: System (**Sys**), Group (**Grp**) or User (**Usr**). System level options should be those that are stable across the entire system. DHCP vs. Static IP addressing would be an example of a System option. Options that are designated as of the Group type should be those that change by category of user, e.g. PTT Allow/Disallow and PTT Channel. A unique extension number is assigned to each handset by the system administrator and would be a User type. The remaining User types should be reserved for options that are normally set by the end user. For Standby menu options such as Ring Type and Noise Mode, default values may be entered with the expectation that the user may change them.

Typical Configuration Plans

Note 1:
Because the specific options that are available depend on the software version and Licence Option, the typical plan options for your facility may differ from those listed here.

- Typical System**Sys** file settings:

  Note 2:
  System file settings typically do not change across an installation.
  - Licence Option
  - Network Config
  - IP Addressing
  - ESSID
  - Security
- Typical Group file settings:
  If certain groups of people require different access to functions, such as PTT, these options are stored as Group files. Several different Group files can be established and the handsets can be configured by group. Typical **Grp** categories are PTT (Push to Talk) options on both Admin and Standby menus.
- Typical User file settings:
  If a setting can be changed by the user in the Standby menu, then it is typically stored in a User file. These can be the default settings or whatever your system requires. Typical **Usr** categories are:
  - Extension
  - Static IP Address
  - Ring Options

- Phone Options

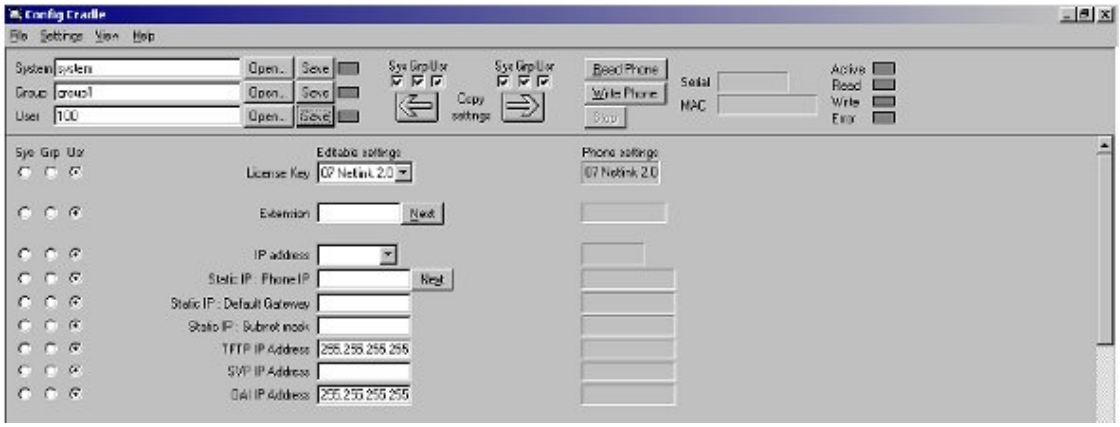
Note 3:
You may have areas in your facility that require different System settings, such as security. These settings can be moved to a Group file or you may set up two System files.

Configuration Cradle Window

When first opened, the **PhoneConfig** program displays the toolbar and a list of configurable options. All **Editable settings** fields are blank or are set to default values.

Initial Window

This is the window that appears when the Confg Cradle program is first opened. The default filenames appear and all category buttons on the left are to **Usr** by default



Configuration Cradle Toolbar

The Config Cradle toolbar allows you to name, open and save configuration files and download and upload configuration settings to and from the handset in the cradle.

The three filename windows allow you to open and save settings by **System**, **Group** or **User** type as separate files. The filenames shown above are the default names, but any filename can be assigned by entering it into the field and clicking the **Save** button. By default, the files will be saved in a new folder named **ConfigData** under the folder where the program is stored. The new folder will be created automatically the first time a file is saved. To open an existing file, click the **Open** button and browse to the file. Use the **File** menu to customize the file structure, if desired.

The three flags beside the **Save** buttons have four colours to indicate the status of the file displayed in the window:

- Red: file does not exist. The filename in the window has not been created
- Yellow: file not loaded. The filename in the window exists in the **ConfigData** folder but has not been loaded into the **Editable settings**
- Green: unsaved edits. When changes are made in the Editable settings field(s), the green flag indicates these have not been saved
- Grey: file up to date. The settings have been saved.

The **Copy settings** arrows and boxes allow you to copy settings to the handset side of the

window, where they may then be written to the handset in the cradle. The configuration in a handset may be copied to the **Editable settings** area and edited or saved. The **Sys Grp Usr** checkboxes allow you to copy only the settings you require.

When clicked, the **Read Phone** and **Write Phone** buttons initiate the transfer of configuration data from or to the handset in the cradle. The **Stop** button will halt the transfer.

The **Serial** and **MAC** windows display the serial number and MAC address of the handset in the cradle. This information is not stored.

The four labelled flags on the right indicate the status of the configuration transfer:

- **Active**: green when attempting communication with handset in cradle. Turns yellow if a timeout occurs (may be due to an improperly seated handset). The software will repeatedly re-attempt communication after a timeout, so re-seating the handset should correct this problem
- **Read**: green when information is currently being read from the handset in the cradle
- **Write**: yellow when information is currently being written to the handset in the cradle
- **Error**: red when an error has occurred. An error message will appear on the status bar at the bottom of the main window

Creating your Configuration Plan

When first setting up a configuration plan, you will enter information into the **Editable settings** fields, indicate which of the three categories each option belongs to, and save as **System**, **Group** or **User** files.

Note:

Do not create a plan that saves an option in two different categories. Option categories should be established and should not overlap. Example: PTT settings are typically tagged as ***Grp*** *options and saved in* ***Group*** *files.*

Once you have established which options will be categorized as System, Group or User, enter the configuration information into the **Editable settings** fields. Start with the System options and enter all system-level fields values. Click the **Sys** category button on the left side of the window for each option. Save these settings as a System file by entering the filename in the **System** filename field and clicking **Save**.

Note that when a setting is changed, it is highlighted in yellow until it is saved.

In the same way, create each Group plan by entering the values in the fields designated as Group types. Click the **Grp** category button on the left side of the window for each option. Save each plan under a different name in the **Group** filename field.

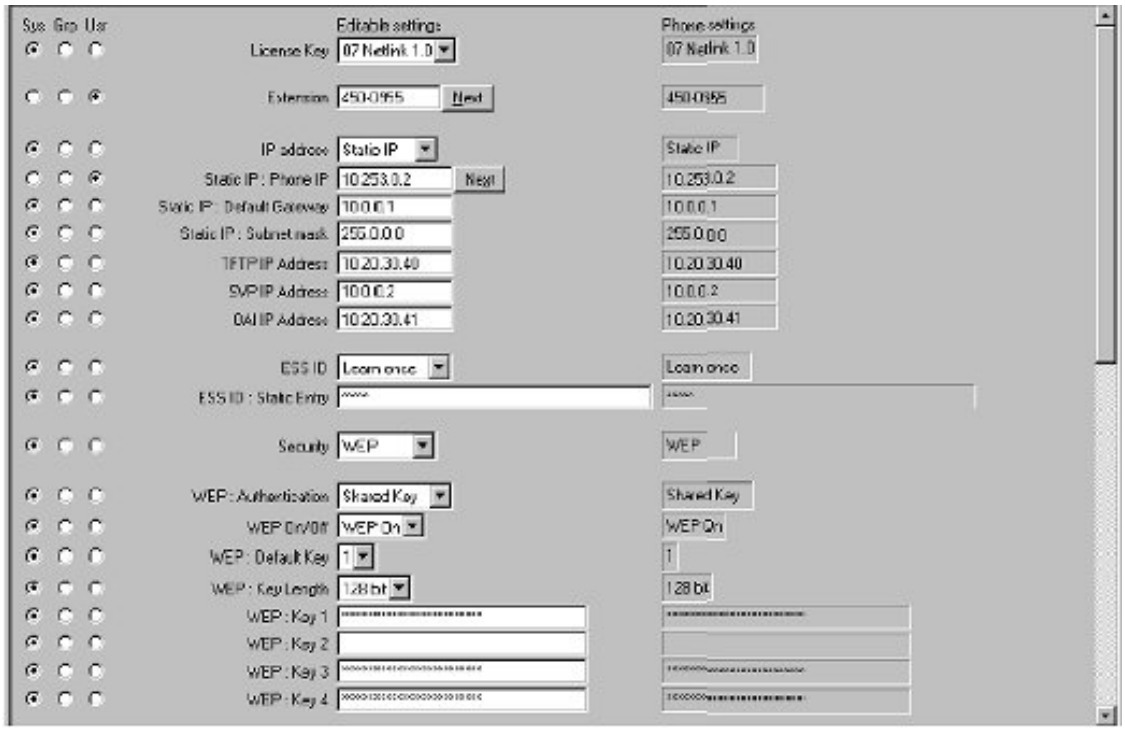
Create one basic **User** file for default (or desired) values for each **User** field. Click the **Usr** category button on the left side of the window for each option.

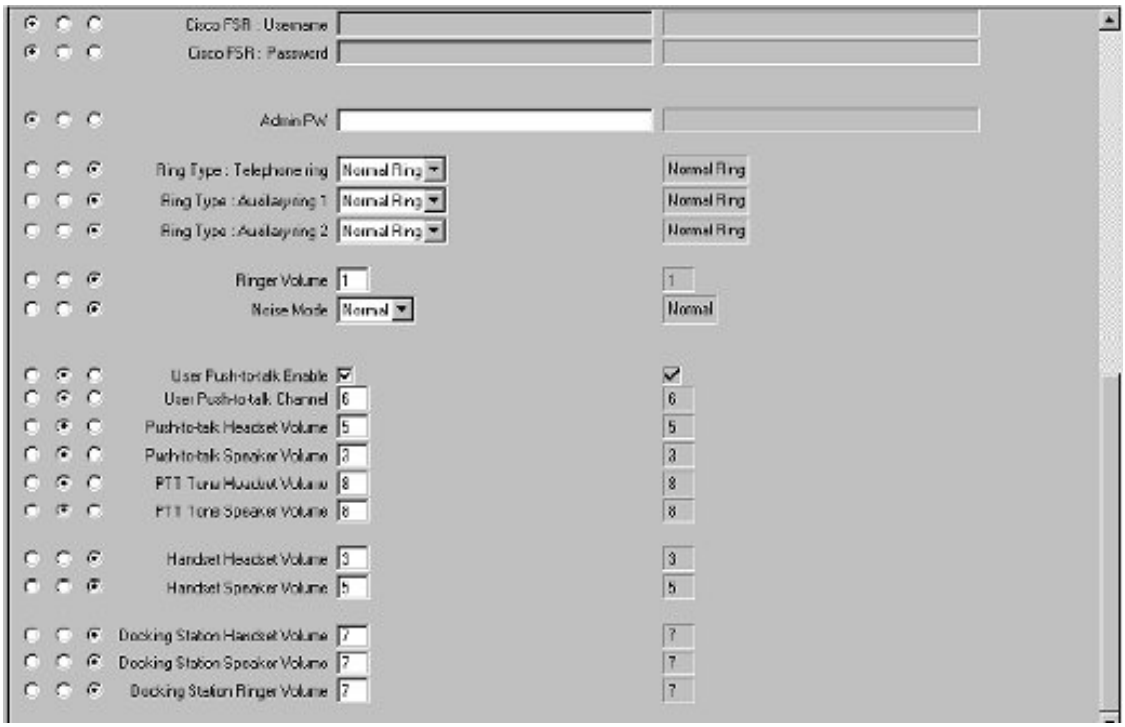
User settings do not necessarily need to be saved for each handset, but they can be saved, if desired. It may be useful, for example, to save a user's ring preferences from a handset being replaced, so that the new handset can be configured the same way. If you determine that each handset configuration should be saved, it is easier to do this during the configuration process. See § Downloading a Configuration Plan to a Handset below.

Sample Configuration Window

Below is a typical Static IP configuration using the WEP security method. All PTT settings are saved as a group. The settings in the **Editable settings** field were first uploaded from a

configured handset and then copied from **Phone settings**.





Downloading and Uploading Configuration Plans

Once your configuration plans are established, settings are easily downloaded into the handsets.

Downloading a Configuration Plan to a Handset

1. Place a handset **with the Battery Pack removed** into the appropriate slot
2. Use the toolbar to open the **System**, **Group** and **User** plans for this handset
3. Enter information unique to the handset - extension and IP address (if using static IP). Note the **Next** button useful to define the same setting for other handsets
4. Copy the settings to the **Phone settings** fields
5. Click **Write Phone** to begin the download
6. You may save the settings unique for this handset by ensuring the correct extension number or other filename is entered in the **User** filename field and then clicking **Save**. You may also load files or edit settings for the next handset (steps 2 and 3) during download
7. When the **Active** flag turns off, download is over and the handset may be removed from the cradle

Uploading a Configuration Plan from a Handset

1. Place a handset **with the Battery Pack removed** into the appropriate slot
2. Click the **Read Phone** button to begin upload
3. When the **Active** flag turns off, the handset settings will appear in the **Phone settings** fields
4. You may copy these settings over to the **Editable settings** fields to use them to create configuration plans as described above or to save them by user or extension

Software Maintenance

The configuration cradle uses proprietary software programs written and maintained by the Alcatel-Lucent. The software version can be displayed via the **Help** menu.

Download the latest Configuration Cradle software from: http://www.businesspartner.alcatel-lucent.com.

The software is delivered in a zip file. Install the update by extracting the zip and overwriting the existing PhoneConfig.exe and other files.

Please follow usual backup procedures to preserve file integrity.

5.2.3.3 Survey Mode

Before using the survey mode, you must configure an ESSID for the Alcatel-Lucent Mobile IP Touch 300/600 . For more information on configuring the handsets, see: module Mobile IP Touch 300/600 - Configuration .

5.2.3.3.1 Verifying Access Point Coverage Using the Handset in Site Survey Mode

This section explains how to test signal strength in the covered area by performing a Site Survey using Alcatel-Lucent Mobile IP Touch 300/600.

This is achieved by activating the Site Survey mode on the handset and walking the coverage

area to observe the displayed signal strengths and details.

To activate Site Survey mode:

1. Press the On key (green) and Off key (red) simultaneously.
2. Release the On key.
3. Release the Off key.
4. Select Diagnostics and confirm with the OK key.
5. Select Run Site Survey and confirm with OK key.

The handset will remain in Site Survey mode until it is powered off.

5.2.3.3.2 Survey Coverage and Conflicts

As you walk the perimeter, the display will show the top four Access Points (APs) detected by the handset. The schematic positions of the code is illustrated in figure : Schematic handset display .

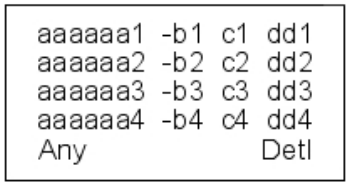


Figure 5.114 : Schematic handset display

- aaaaaa1 through aaaaaa4 are the last six digits of the access point MAC address. The APs are displayed in order of signal strength.
- -b1 through -b4 indicate the power level in dBm at which the handset receives the associated AP signal . There should be in all areas, at least one AP reading stronger than -70 dBm .
- c1 through c4 indicates the channel number used by the AP
- dd1 through dd4 is the DTIM value used by the access point
- Any: displays the AP information whatever the ESSID broadcast
- Detl: displays details of an AP

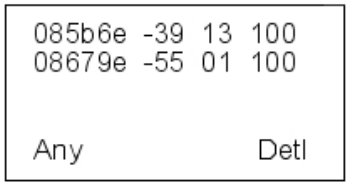


Figure 5.115 : Example of display

In order to avoid conflicts, it is preferable that no overlaps exist anywhere in your facility. If the Site Survey mode indicates two or more APs using the same channel, then at least one AP

must be 10 dB stronger than the other APs.

5.2.3.3.3 Confirm Supported Data Rates

Walk around the site to determine supported data rates, one AP at a time. In any location, you may use the Detl key to display details about one AP.

Each data rate (1,2,5.5, or 11Mb/s) that is supported by the AP is shown. Those rates that are in the Basic Rate set (sometimes referred to as “required” rates) are indicated by a ‘b’ following the rate number. The Supported and Basic data rate(s) should be the same on all APs as is appropriate for your environment.

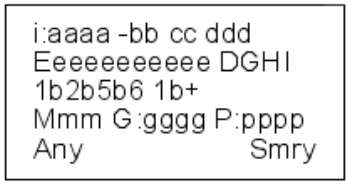


Figure 5.116 : Schematic detail display

- i: index of the AP
- aaaa: last four digits of the AP MAC address
- -bb: indicates the power level in dBm at which the handset receives the associated AP signal
- cc: channel used by the AP
- ddd: DTIM value of the AP
- Eeeeeeeeeee: ESSID of the AP (11 characters displayed)
- DGHI: supported standards
- 1b2b5b6 9 11b+: supported bandwidth (+ means a higher bandwidth is supported)
- Mmm: security mode
- G: group key
- P: pairwise key

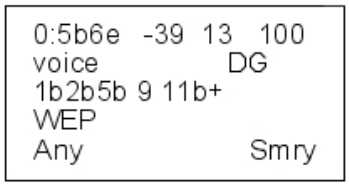


Figure 5.117 : Example of display

In this example:

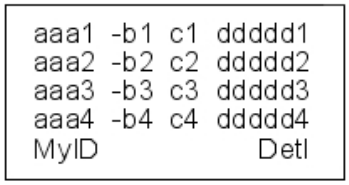
- voice: SSID is voice
- DG: the 802.11d and 802.11g standards are supported

- supported bandwidth:
  - 802.11b: 1, 2, 5.5 and 11 Mbps
  - 802.11g: 6 and 9 Mbps or more

  WEP: security mode

5.2.3.3.4 Check the SSID Broadcast

In any location, you may use the Any key to display the SSID broadcast.



- aaa1 through aaa4 are the last four digits of the access points' MAC address.
- b1 through b4 are the power levels in dBm at which the handset heard the associated access point.
- c1 through c4 are the channels used by the AP
- dddd1 through d4 are the first four characters of the ESSID of the AP

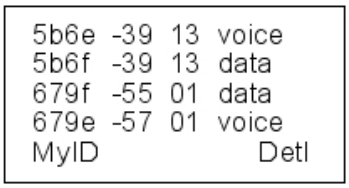


Figure 5.119 : Example of display

5.2.3.4 Maintenance

5.2.3.4.1 Alcatel-Lucent Mobile IP Touch 300/600 Error Message Table

Message	**Description**	**Action**
3 chirps (audio)	handset is not able to communicate with the best AP, probably because that AP has no bandwidth available.	None. This is only a warning, the call will handoff to the best AP once it becomes available.
Address Mismatch	Handset software download files are incorrect or corrupted.	Download new software from the Alcatel-Lucent website per Software Maintenance.

Message	Description	Action
ASSERTxxx.c Line yyy	The handset has detected a fault from which it cannot recover.	Record the error code so it can be reported. Turn the handset off then on again. If error persists, try registering a different handset to this telephone port. If error still persists, contact Technical Support and report the error.
Assoc Failed xxxxxxxxxxxx	x…x = AP MAC address. Handset association was refused by AP; displays MAC of failing AP	Check handset and AP security settings. Ensure AP is configured per Configuration Note. Try another AP.
Assoc Timeout xxxxxxxxxxxx	x…x = AP MAC address. Handset did not receive association response from AP; displays MAC of failing AP.	Check handset and AP security settings. Ensure AP is configured per Configuration Note. Try another AP.
Auth Failed xxxxxxxxxxxx	x…x = AP MAC address Handset authentication was refused by AP; displays MAC of failing AP.	.Check handset and AP security settings. Ensure AP is configured per Configuration . Note. Try another AP.
Auth Timeout xxxxxxxxxxxx	x…x = AP MAC address. Handset did not receive authentication response from AP; displays MAC of failing AP	Check handset and AP security settings. Ensure AP is configured per Configuration Note. Try another AP.
Bad Code Type xx Expected Code Type yy	xx, yy = software licence types. Handset software does not match current handset licence selection.	Download new software from the Alcatel-Lucent website per Software Maintenance.
Bad Config	Some needed configuration parameter has not been set	Check all required handset configuration parameters for valid settings
Bad ESSID	The handset is configured for “static ESSID” (as opposed to “Learn once” or “Learn always” and no ESS ID has been entered.	Enter an ESSID in the configuration settings or change to one of the “Learn” modes.
Bad Term, Type	Gatekeeper rejected registration request from the handset	Verify the gatekeeper or PCX’s configuration
Bad Phintl File	Handset software download files are incorrect or corrupted.	Download new software from the Alcatel-Lucent website per Software Maintenance.
Bad Program File	Handset software download files are incorrect or corrupted.	Download new software from the Alcatel-Lucent Web site per Software Maintenance.

Message	Description	Action
(battery icon), Low Battery, beep (audio)	Low battery	In call: the battery icon displays and a soft beep will be heard when the user is on the handset and the battery charge is low. User has 15–30 minutes of battery life left. The Battery Pack can be changed while the call is still in progress. Do not press Power Off / End Call. Quickly remove the discharged battery and replace with a charged battery, power on the handset, and press Power On / Start Call to resume the call in progress. Not in call: The battery icon displays whenever the Battery Pack charge is low. The message Low Battery and a loud beep indicate a critically low battery charge when user is not on the handset. The handset will not work until the Battery Pack is charged.
Battery Failure	The Battery Pack is not functioning.	Replace the Battery Pack with a new or confirmed Alcatel-Lucent Battery pack. Any non-Alcatel-Lucent Battery Packs will not work.
Battery Failed	Battery Pack is damaged or incompatible with handset.	Replace the Battery Pack with a new or confirmed Alcatel-Lucent Battery Pack. Only Alcatel-Lucent Battery Packs will work.
CalSig Addr Bad	Gatekeeper rejected registration request from the handset	Check the H.323 gatekeeper configuration in the handset. Verify the gatekeeper or PCX's configuration Verify the phone has been assigned the correct extension and that no other H.323 devices share that extension.
Can't Renew DHCP yyy.yyy.yyy.yyy	y…y = DHCP server IP address. DHCP server is not responding to initial renewal attempt	Configuration problem. Check the IP address configuration in the DHCP server.
Charging …	The handset is charging in the Desktop Charger	No action needed
Charge Complete	The handset is now fully charged	No action needed
Checking Code	handset is contacting the Download Master to determine if it has a newer version of software that should be downloaded.	None, this message should only last for approximately one second. If message remains displayed, power off and contact customer support for a replacement phone.
Checking DHCP IP	The handset is retrieving DHCP information from the DHCP server	None. This is informational only.
Code Mismatch!	The software loaded into the handset is incorrect for this model handset.	Verify the Licence Management value is correct. Replace the software image on the TFTP server with software that is correct for the handset model.

Message	Description	Action
Connect Timeout	Wireless telephone is not provisioned on the system. Message will display if no CONNECT message is received from the PCX within 30 seconds of the start of initialization.	Handset will restart after 20 seconds. If unsuccessful, check PCX configuration.
CRC Code Error	The software which has been TFTP downloaded has a bad redundancy code check	Try the download again, it is possible the software was corrupted during download. If the error repeats, check that the download image on the TFTP server is not corrupted.
Code Mismatch!	The software loaded into the handset is incorrect for this model phone	Replace the software image on the TFTP server with software that is correct for the phone model.
DCA Timeout	The handset has detected a fault for which it cannot recover, possibly due to a failure to acquire any network.	Turn the handset off then on again. If error persists, contact Alcatel-Lucent Technical Support and report the error.
Dest Unreachable	Unable to establish network connectivity with the gatekeeper	Verify gatekeeper is running and has network connectivity to WLAN infrastructure.
DHCP Error (1-4)	DHCP Error 1	The handset cannot locate a DHCP server. It will try every 4 seconds until a server is located.
	DHCP Error 2	The handset has not received a response from the server for a request for an IP address. It will retry until a server is found.
	DHCP Error 3	The server refuses to lease the handset an IP address. It will keep trying.
	DHCP Error 4	The server offered the handset a lease that is too short. The minimum lease time is 10 minutes but Alcatel-Lucent recommends at least one-hour minimum lease time. The handset will stop trying. Reconfigure the server and power cycle the handset.
	DHCP Error 5	Failure during WEP Key rotation process (proprietary feature).
DHCP Lease Exp yyy.yyy.yyy.yyy	. DHCP is not responding to renewal attempts (at least one renewal succeeded). y…y = DHCP Server IP address	The handset failed to renew its DHCP lease, either because the DHCP server is not running, or because the configuration has been changed by the administrator. The handset will attempt to negotiate a new lease, which will either work, or it will change to one of the above DHCP errors (1 through 4).
DHCP NACK error yyy.yyy.yyy.yyy	y…y = DHCP server IP address DHCP server explicitly refused renewal.	The DHCP lease currently in use by the Wireless Telephone is no longer valid, which forces the Wireless Telephone to restart. This problem should resolve itself on the restart. If it does not, the problem is in the DHCP server.
DL Not On Sector	eHandset software download files are incorrect or corrupted	Download new software from the Alcatel-Lucent website per Software Maintenance.

Message	Description	Action
DO NOT POWER OFF	The Wireless Telephone is in a critical section of the software update	None. Do not remove the battery or attempt to power off the phone while this is displayed. . Doing so may require the handset inoperable
Duplicate IP	The handset has detected another device with its same IP address.	If using DHCP, check that the DHCP server is properly configured to avoid duplicate addresses. If using Static IP, check that the handset was assigned a unique address.
		Verify the phone has been assigned the correct extension and that no other H.323 devices share that extension.
Erase Failed	Download process failed to erase the memory in the handset	Operation will retry but may eventually report the error "int. error: 0F". Power cycle the phone.
Erasing Memory	Handset has determined that a download should occur and is erasing the current software from memory.	None. When the progress bar fills the display line the erase operation is complete. Do not turn the handset off during this operation.
Error in Config	Indicates an error in one of the static IP addresses set in the Admin menu.	Correct static IP addresses in the Admin menu.
Files Too Big	Handset software download files are incorrect or corrupted	Download new software from the Alcatel-Lucent website per Software Maintenance.
Flash Config Error	Handset internal configuration is corrupt.	Perform "Restore Defaults" operation via administrator menus [or re-program with Configuration Cradle].
Initializing …	The handset is performing power on initialization	None. This is informational only.
Internal Err. # #	The handset has detected a fault from which it cannot recover.	Record the error code so it can be reported. Turn the Wireless Telephone off then on again. If error still persists, contact Alcatel-Lucent Technical Support and report the error.
Multiple GW regs	More than one SVP Server has responded.	Caused by two or more handsets sharing the same IP address. Assign unique IP addresses to each handset.
Multiple SVP Reg yyy.yyy.yyy.yyy	y…y = SVP IP address Handset received responses from multiple SVP Servers; displays IP address of one responding SVP Server.	This can happen if the handset has been reconfigured to use a different SVP Server and then powered up before the previous SVP Server has had time to determine that the handset is no longer connected to it. The problem should go away after about 30 seconds.
Must Upgrade SW!	Handset software is incompatible with hardware.	Download new software from the Alcatel-Lucent website per Software Maintenance.
Network Busy xxxxxxxxxxxxxx	x…x = AP MAC address. Handset cannot obtain sufficient bandwidth to support a call; displays MAC of failing AP.	Try the call again later.

Message	Description	Action
No DHCP Server	Handset is unable to contact the DHCP server.	Check that DNCP is operational and connected to WLAN or use Static IP configuration in the handset.
No ESSID	Attempted to run Site Survey application without an ESSID set.	Let handset come completely up. Statically configure an ESSID in the Admin menu..
No Func Code	Handset software download files are incorrect or corrupted.	Reconfigure the handset to gain access to the WLAN and download new code.
	No LAN connection at the AP or Telephony Gateway	Verify Telephony Gateway connection to LAN and all APs.
No Host IP	The handset is configured for “static IP” (as opposed to “use DHCP”) and no valid host IP Address (the Wireless Telephone’s IP Address) has been entered.	Enter a valid IP Address in the configuration settings or change to “use DHCP”.
No IP Address	Invalid IP	Check the IP address of the handset and re-configure if required.
No NOE DHCP	DHCP is configured but no valid NOE option 43 was found.	Check DHCP configuration for option 43 and reconfigure if required.
No Net Access	Cannot authenticate / associate with AP	Verify the AP configuration. Verify that all the WEP settings in the handset match those in the APs.
No Net Found No APs	Handset cannot find any Access Points This indicates any of the following:	
	No radio link	Verify that the AP is turned on.
	No ESSID – Auto-learn not supported (or) Incorrect ESSID	Verify the ESSID of the wireless LAN and enter or Auto-learn it again if required.
	AP does not support 1 or 2 Mb/s	Check the AP using vendor tests. Consult the AP Configuration Note.
	AP does not support appropriate data rates	Check the AP configuration against Configuration Note for AP.
	Out of range	Try getting closer to an AP. Check to see if other hansets are working within the same range of an AP. If so, check the ESSID of this handset.
	Incorrect WEP settings	Verify that all the WEP settings in the handset match those in the APs.
	Incorrect Security settings	Verify that all the Security settings in the handset match those in the APs.
No Net Found xxxxxxxxxxxx yy	x…x = AP MAC address. yy = AP signal strength. Handset cannot find a suitable access point; displays MAC and signal strength of “best” non-suitable AP found.	Check AP and handset network settings such as ESSID, Security, Reg domain and Tx power. Ensure APs are configured per Configuration Note. Try Site Survey mode to determine a more specific cause.

Message	Description	Action
No PBX Response	The handset has exceeded its retransmission limit with no ACK response from proxy server.	Verify that proxy server IP address and port are properly configured
No Reg Domain	Regulatory Domain not set	Configure the Regulatory Domain of the hansdset.
No SVP IP	The handset is configured for “static IP” (as opposed to “use DHCP”) and no valid SVP Server address has been entered.	Enter a valid SVP server IP address in the configuration setting or change to “use DHCP.”
No SVP Response yyy.yyy.yyy.yyy	y…y = SVP Server IP address. Handset has lost contact with the SVP Server.	This may be caused by bad radio reception or a problem with the SVP Server. The Wireless Telephone will keep trying to fix the problem for 20 seconds, and the message may clear by itself. If it does not, the handset will restart. Report this problem to the system administrator if it keeps happening.
No SVP Server	Wireless Telephone can’t locate SVP Server	IP address configuration of SVP Server is wrong or missing.
	SVP Server is not working	Check error status screen on SVP Server.
	No LAN connection at the SVP Server	Verify SVP Server connection to LAN.
No SVP Server No DNS Entry	Handset unable to perform DNS lookup for SVP Server, server had no entry for SVP Server.	The network administrator must verify that a proper IP address has been entered for the SVP Server DHCP option.
No SVP Server No DNS IP	Handset unable to perform DNS lookup for SVP Server, no IP address for DNS server.	The network administrator must verify proper DHCP server operation.
No SW Found	A required software component has not been identified.	A required software component has not been identified. Check that the handset licence type has a corresponding entry in the slnk_cfg.cfg file. Check that the pd11ald.bin and pi110004.bin entries exist under this licence type in the slnk_cfg.cfg file.
Not Installed!	A required software component is missing	Check that all required software files are on the TFTP server, if over-the-air downloading is being used. If the error repeats, contact Alcatel-Lucent Technical Support.
Phone Restarting	If the handset is not able to register at first try, the message is displayed for 20 seconds while it restarts. It also displays if the PCX causes the handset to restart.	None. If the handset does not register after a restart, check the configuration in the Admin menu and the PCX.
Press End Call	The far end of a call has hung up.	Hang up the near end.
Registration REJ	Gatekeeper rejected registration request from the Wireless Telephone	Check the H.323 gatekeeper configuration in the Wireless Telephone.

Message	Description	Action
Select Licence	The correct protocol has not been selected from the licence set.	Using the administrative menus, select one licence from the set to allow the phone to download the appropriate software.
Server Busy	Handset is attempting to download from a TFTP Server that is busy downloading other devices and refusing additional downloads.	None, the handset will automatically retry the download every few seconds.
Service Rej.	The SVP Server has rejected a request from the handset	The handset will restart and attempt to re-register with the SVP Server, which should fix the problem. Report to your administrator if it keeps happening.
System Busy yyy.yyy.yyy.yyy	y…y = SVP Server IP Address. SVP Server has reached call capacity.	All call paths are in use, try the call again in a few minutes.
System Locked (with Busy Tone)	SVP Server is locked	Try call again later, system has been locked for maintenance
	System is locked	Try the call again, system has been locked for maintenance
TFTP ERROR(x):yy	A failure has occurred during a TFTP software download. (x) = The file number which was being downloaded; yy is an error code describing the particular failure. Possible error codes are:	Error code 01, 02 or 07 - check the TFTP server configuration.
	01 = TFTP server did not find the requested file.	Error code 81, the Wireless Telephone will attempt to download the file again.
	02 = Access violation (reported from TFTP server).	For other messages, power off the handset, then turn it on again to retry the download. If the error repeats, note it and contact Alcatel-Lucent Technical Support.
	07 = TFTP server reported "No such user" error.	
	81 = File put into memory did not CRC.	
	FF = Timeout error. TFTP server did not respond within a specified period of time.	
Too Many Errors	The handset continues to reset and cannot be recovered.	Fatal error. Return handset to Alcatel-Lucent.
Unknown xx:yy:zz	A phrase is missing from the phintl file.	Download new software from the Alcatel-Lucent website per Software Maintenance.
Unsupported Codec	The proxy server has requested using a codec not supported by the handset.	Check proxy server configuration for supported codecs and reconfigure if necessary.

Message	Description	Action
Unsupp Transport	Gatekeeper rejected registration request from the Wireless Telephone	Verify the gatekeeper or PCX's configuration. Ensure the gatekeeper and PCX will support version 2 of the H.323 protocol.
Updating …	The handset is internally updating its software images	None. The handset may do this briefly after a download. This is informational only.
Updating Code	Handset is downloading new software into memory. The number icons at the bottom of the display indicate which file number is currently being downloaded. This message also displays a progress bar. When the progress bar fills the display line the update operation is complete on that file.	None. When the progress bar fills the display line the update operation is complete on that file. Do not turn the Wireless Telephone off during this operation.
Waiting...	Handset has attempted some operation several times and failed.	None. The handset is waiting for a specified period of time before attempting that operation again.
Wrong Code Type	The software loaded into the handset is incorrect for this model handset.	Verify the licence type is set correctly.
		If the licence type is correct, replace the software image on the TFTP server with the software that is correct for the handset model.
(No message shown)	There is no voice path.	Verify that the CODEC is G.711.

5.2.4 SVP Server

5.2.4.1 Detailed description

The SVP Server is an Ethernet LAN device that works with Access Points (APs) to provide QoS on the wireless LAN. Voice packets to and from the Alcatel-Lucent IP Touch WLAN handsets are intercepted by the SVP Server and encapsulated for prioritization as they are routed to and from the PCX.

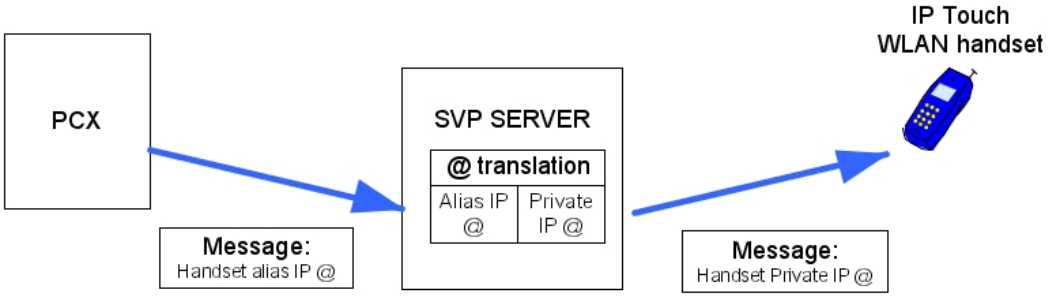
5.2.4.1.1 Conversion Protocol

Between a PCX and an SVP server, the UDP protocol is used. Between the SVP server and an IP Touch WLAN handset, the SRP protocol is used. All voice packets have to transit via the SVP server for conversion. There is no direct communication between the PCX and the handset.

5.2.4.1.2 IP Address Translation

When a handset is switched on, it registers at the SVP server. An IP address alias is assigned to the handset. The SVP server builds a NAT (Network Address Translation) for current/alias IP address translation.

The alias IP address is used for communication between PCX and SVP server. The private IP address is used for communication between SVP server and the handset. This can be displayed on the SVP server.



5.2.4.1.3 Call Admission Control (CAC)

The SVP Server provides Call Admission Control (CAC), which limits the maximum number of simultaneous calls per AP. This feature guarantees good audio quality for simultaneous voice over WLAN communications in the AP.

CAC mechanism:

During configuration of the SVP Server, the system administrator defines the maximum number of simultaneous calls per AP. When the SVP Server is starting, the handset transmits the MAC address of the AP with which it is associated. During a call establishment between the handset and the SVP server, the handset sends the AP's MAC address. This means that the SVP server maintains a table including a list of APs with the on-going calls. Each time the handset roams to a new AP, this table is updated.

When an AP is congested by a new incoming call, the SVP Server asks the handset for an AP change. If it is not possible, the call is rejected (or released in case of roaming).

5.2.4.1.4 SVP Server Models

The SVP server is available in three models:

- SVP100: serves 80 calls simultaneously
- SVP020: serves 20 power-on handsets
- SVP010: serves 10 power-on handsets

5.2.4.1.5 Cascading SVP Servers

In order to increase the number of handsets available on the WLAN, it is possible to add one or more SVP servers. As a result, the number of available simultaneous communications is increased.

One SVP server is declared master and must have a static IP address, the others are slave SVP servers. All SVP servers must be in the same subnetwork.

The master SVP server distributes handsets and APs between the SVP servers. The distribution is done according to MAC addresses.

Each SVP server performs conversion protocol and IP address translation for its attached handsets.

Each SVP server performs management and CAC functions for its attached APs..

5.2.4.1.6 Capacities

A subnetwork can have up to four SVP010 models, or up to two SVP020 models, or up to sixteen SVP100 models. All SVP servers must be the same model type within one subnetwork.

The following tables show the capacities for each SVP server model.

table 5.70 : WLAN Network Resources According to the Number of SVP010 and SVP020 Server

Number of SVP Servers	Number of Handsets SVP010	Number of Handsets SVP020
1	10	20
2	20	40
3	30	N/A
4	40	N/A

table 5.71 : WLAN Network Resources according to the Number of SVP100 Servers

SVP Server	Calls per Server	Total Calls	Erlangs (1% loss)	Max. Users Num. 10% Use	Max. Users Num. 15% use	Max. Users Num. 20% use
1	80	80	65	500	433	325
2	64	128	111	1000	740	555
3	60	180	160	1500	1067	800
4	58	232	211	2000	1407	1055
5	57	285	262	2500	1747	1310
6	56	336	312	3000	2080	1560
7	56	392	367	3500	2447	1835
8	55	440	415	4000	2767	2075
9	55	495	469	4500	3127	2345
10	55	550	524	5000	3493	2620
11	55	605	578	5500	3853	2890
12	54	648	621	6000	4140	3105
13	54	702	674	6500	4493	3370
14	54	756	728	7000	4853	3640
15	54	810	782	7500	5213	3910
16	54	864	836	8000	5573	4180

5.2.4.1.7 Call Roaming with Cascading SVP Servers

The following figure gives an example of call roaming with cascading SVP servers.

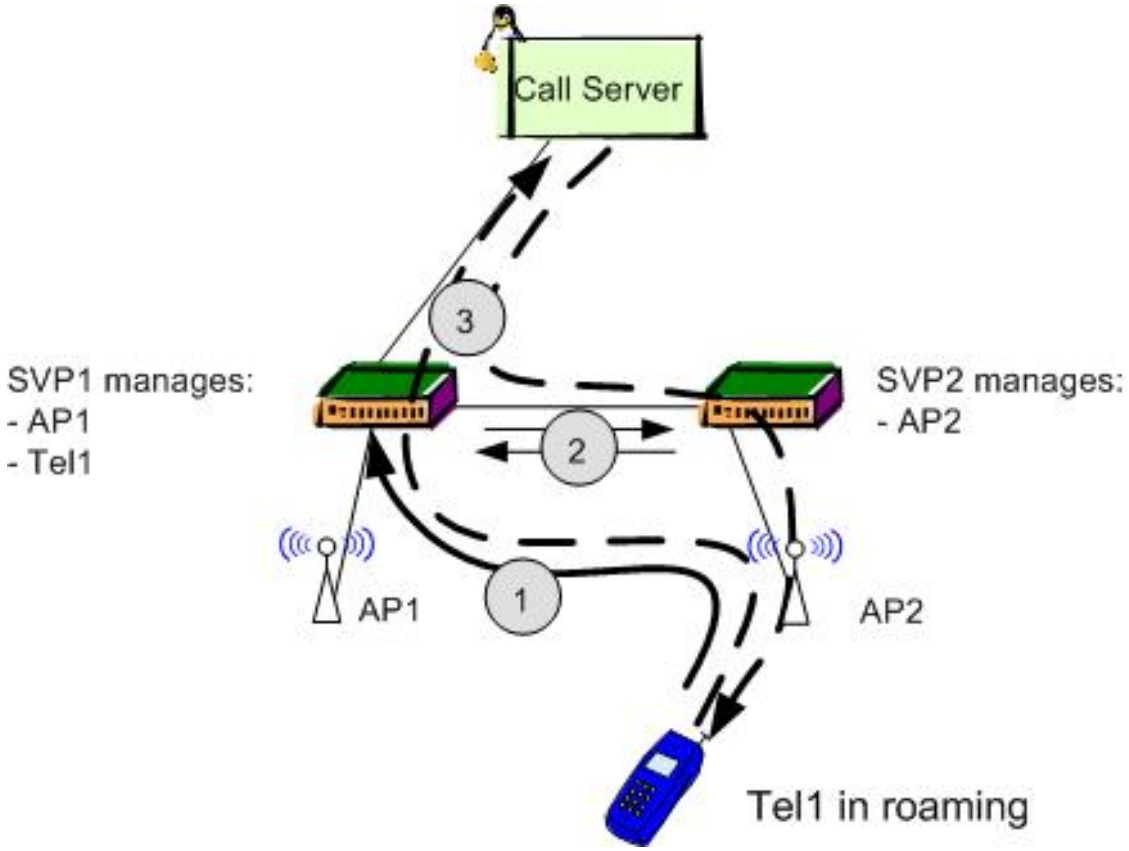


Figure 5.121 : Call roaming with cascading SVP Servers

A roaming handset can initiate a communication as follows:

1. The handset connects to its assigned SVP1 server through the nearest AP2
2. The assigned SVP1 server asks SVP2 permission to use AP2 (CAC feature)
3. The uplink voice path goes through the SVP1 server. The downlink audio path goes through SVP1 and SVP2 servers

5.2.4.2 Installation procedure

This document presents the SVP Server installation. The SVP Server is connected to the Alcatel-Lucent OmniAccess Wireless Switch (AOS-W). For information on installing and configuring the WLAN Switch, see module Voice over Wireless LAN - WLAN Switch Configuration with AOS-W R3.1 and Later .

The specifications covered here allow for great flexibility in physical placement of the components within stated guidelines. See the Configuration and Administration document for your vendor's IP system for information on LAN requirements, network infrastructure and IP addressing.

5.2.4.2.1 SVP Server Front Panel

The following figure and list describe the ports and LED status indicators on the front panel of the SVP Server.

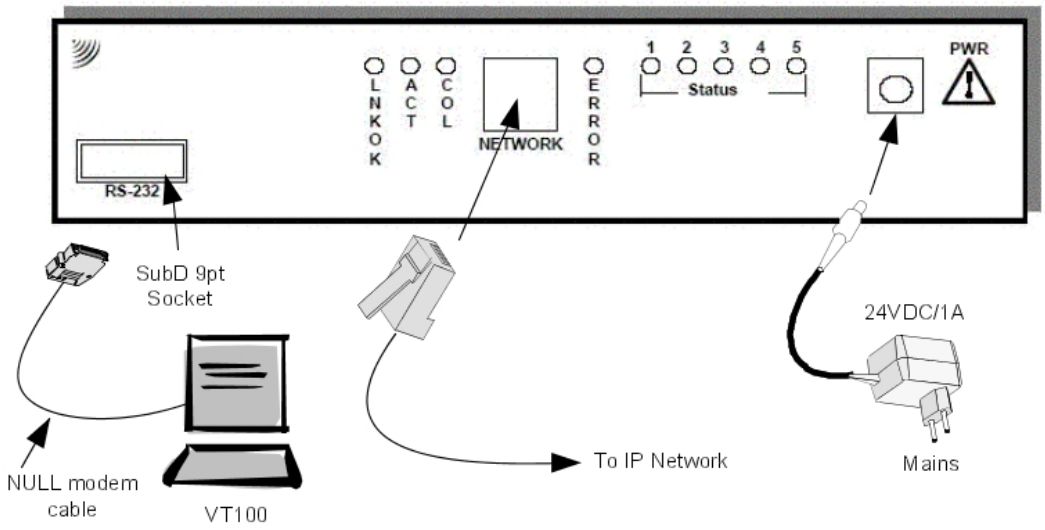


Figure 5.122 : SVP Server front panel

- **RS-232** port: DB-9 male connector (DTE) used for RS-232 connection to a terminal, terminal emulator, or modem for system administration
- **Link LEDs:**
  - **LNKOK**: lit when there is a network connection
  - **ACT**: lit when there is system activity
  - **COL**: lit when there are network collisions
- **NETWORK**: port to wired (Ethernet) LAN
- **ERROR**: lit when the system has detected an error
- **STATUS**: indicate system error messages and status
  - **1**: heartbeat, indicates gateway is running
  - **2**: when active calls
  - **3, 4, 5:** currently unused
- **PWR** (power jack): connects to the AC adapter supplying power to the system

Notes:

Only use the Alcatel-Lucent provided Class II AC Adapter with output 24VDC, 1A

The model designation can be found on the label on the side of the SVP Server.

5.2.4.2.2 Required Materials

The following equipment must be provided by the customer.

- Power Outlet: Must accept Alcatel-Lucent provided AC adapter.
- Backboard space: The SVP Server is designed to be wall mounted to ¾" plywood securely screwed to the wall.
- Screws: Required to mount the SVP Server to the wall. Four #8 - ¾" panhead wood screws (or similar device) are required

- Cat. 5 Cable: RJ-45 connector at the SVP Server. Connection to Ethernet switch.

5.2.4.2.3 Locate the SVP Server

The SVP Server measures approximately 4 x 12.5 x 7 inches, and weighs about five pounds. The unit can be wall mounted, vertically or horizontally, over ¾" plywood. The SVP Server can also be rack mounted using a rack mount kit (sold separately).

Locate the SVP Server in a space with:

- Sufficient backboard mounting space (for wall mount) and proximity to the LAN access device (switched Ethernet hub) and power source.
- Easy access to the front panel, which is used for cabling
- A maximum distance of 325 feet (100 meters) from the Ethernet switch.

5.2.4.2.4 Install the SVP Server

The SVP Server may be mounted on a rack or to a wall.

Mount the SVP Server on a rack

The rack mount kit is designed for mounting equipment in a standard 19 inch rack and should contain the following equipment:

1. Mounting plates: Two for each SVP Server to be mounted
2. Screws: Four rack mount screws for each SVP Server to be mounted

To rack mount the SVP Server:

1. Remove the corner screws from the SVP Server
2. Screw the U-shaped end (round screw holes) of the two mounting plates to the SVP Server
3. Screw the other end of the two mounting plates (oblong screw holes) to the rack
4. Repeat steps 1-3 for each additional SVP Server. The mounting plate is designed to provide the correct minimum spacing between units. When mounting multiple units, stack the units in the rack as closely as possible.

Mount the SVP Server to a wall

The SVP Server can be mounted either horizontally or vertically.

To mount the SVP Server to a wall:

1. Using a 1/8 inch drill bit, drill four pilot holes, on 1.84 by 12.1 inch centres (approximately equivalent to 1-13/16 inch by 12-1/8 inch)
2. Insert the #8 x 3/4 inch screws in the pilot holes and tighten, leaving a 1/8 to 1/4 inch gap from the wall

Connect SVP Server to LAN

Using a Cat. 5 cable, connect the NETWORK port on the SVP Server to the connecting port on the Ethernet switch.

Connect Power

1. Connect the power plug from the AC adapter to the jack labelled PWR on the SVP Server

   Note:
   Use only the provided Class II AC Adapter with output 24VDC, 1A

2. Plug the AC adapter into a 110VAC outlet to apply power to the SVP Server
3. The system will cycle through diagnostic testing and the LEDs will blink for about one minute. When the system is ready for use:
   - The **ERROR** LED should be off
   - **Status 1** should be blinking

5.2.4.3 Configuration procedure

During initial setup of the SVP Server, the IP address is established and the maximum number of active calls per access point is set. Optionally, you may enter a hostname and a location for software updates via TFTP.

Note:

The SVP Server, all WLAN handsets, and all Access Points (APs) must be on the same subnet.

5.2.4.3.1 Connecting to the SVP Server

The initial connection to the SVP Server must be made via a serial connection to establish the SVP Server's IP address. After the IP address is established, set connection to the SVP Server may be done via the network using Telnet. It is recommended that the basic setup actions occur while the serial connection is made.

Connect via the Serial Port

1. Using a DB-9 female, null-modem cable, connect the SVP Server to the serial port of a terminal or PC.
2. Run a terminal emulation program (such as HyperTerminal™) or use a VT-100 terminal with the following configuration:
   Bits per second: 9600
   Data bits: 8
   Parity: None
   Stop bits: 1
   Flow control: None
3. Press Enter to display the SVP Server login screen.
4. Enter the default login: **admin** and default password: **admin**. These are case sensitive.
5. The **SVP-II System** menu will display.

Connecting Via Telnet

Note:

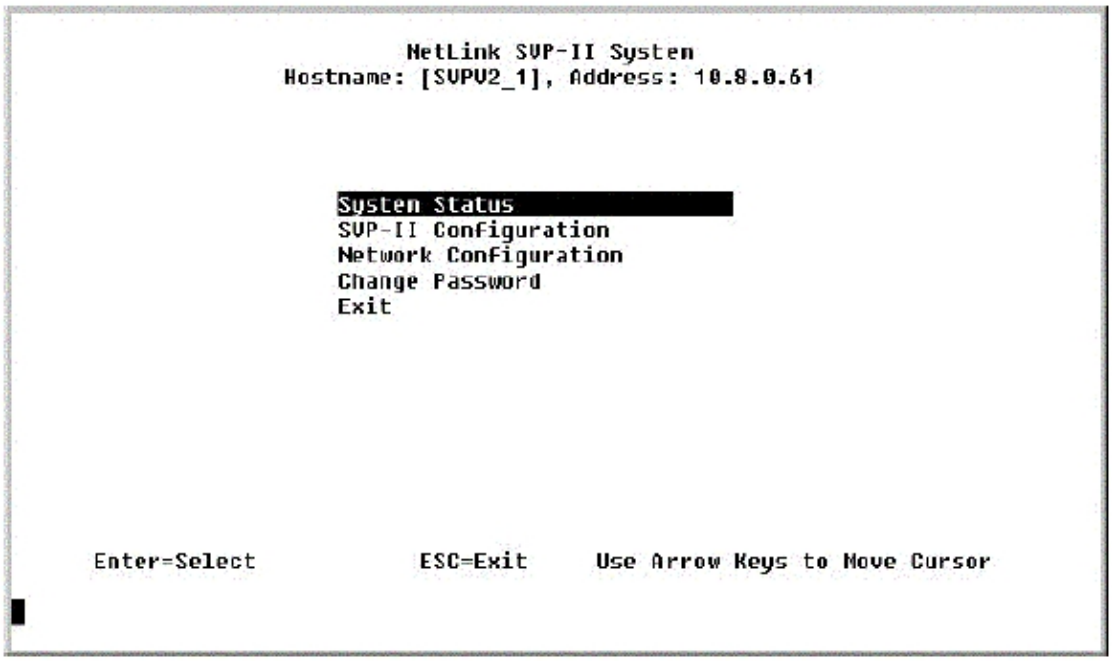
Telnet can only be used after the SVP Server IP address has been configured.

The Telnet method of connection is used for routine maintenance of the Server for both local and remote administration, depending on your network.

To connect via Telnet, run a Telnet session to the IP address of the SVP Server. Once you connect and log in, the **SVP-II System** menu displays.

5.2.4.3.2 The SVP-II System Menu

The main menu displays as shown here:



System Status – menu for viewing error messages, status of operation, software code version.

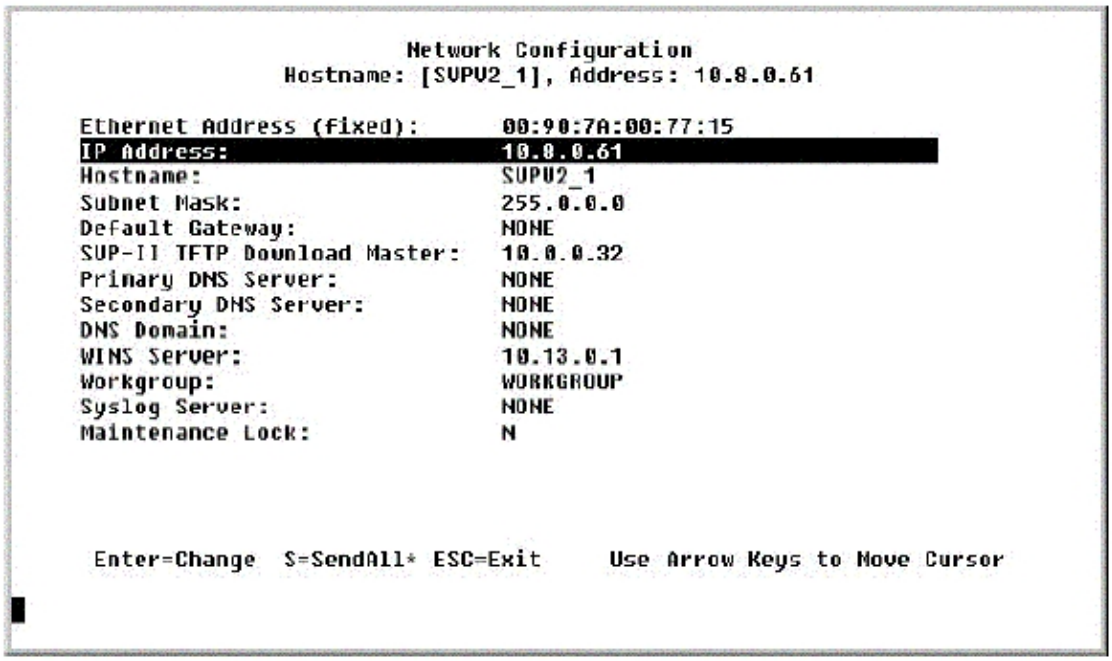
SVP-II Configuration – allows you to set the mode and reset the system.

Network Configuration – allows you to set network configuration options, including IP address and hostname.

Change Password – allows you to change the password for SVP Server access.

5.2.4.3.3 Network Configuration

The IP address and other network settings are established via the **Network Configuration** screen. This is also where you may optionally establish a hostname and enter the IP address of the location of any software updates you may obtain from Alcatel-Lucent. Scroll to **Network Configuration** and select by pressing Enter. A screen similar to the following appears:



Note the navigation options at the bottom of the screen. Press Enter to change a value, ESC to exit the screen, and the arrow keys to move the cursor.

Send All

In an IP system with multiple SVP Servers, the SendAll option is provided to speed configuration and ensure identical settings. The **S=SendAll** option allows you to send that configuration parameter to every SVP Server on the LAN. **SendAll** can only be used after the IP address is established on EACH SVP Server via the serial connection. If you anticipate identical settings across the LAN, set just the IP address and custom hostname (if desired) for each SVP Server using the initial serial connection. Then connect via the LAN and use **SendAll** to set identical configuration options for all SVP Servers.

If **SendAll** is to be utilised in your system, all passwords must be identical. DO NOT CHANGE THE PASSWORD AT THE INITIAL CONFIGURATION IF THE SEND ALL OPTION IS DESIRED. Use the default password and change it globally if desired after a LAN connection is established for all SVP Servers.

If independent administration of each SVP Server is desired, the passwords may be set at initial configuration.

Note 1:

To change the IP address of the master SVP Server, change it in this menu and reboot the system. Then you may change alias IP addresses in each of the other SVP Servers without error.

The following options must be configured:

- **IP Address** – enter the IP address of the SVP Server, defined by your network administrator. Enter the complete address including digits and periods.
  Important: A master SVP Server must have a static IP address.

Note 2:
The SVP Server will automatically lock for maintenance if the IP address is changed. When this Maintenance Lock occurs, the SVP Server must be reset upon exit. All active calls are terminated during a reset.

- **Hostname** -(optional) change the default host name, if desired. This is the name of the SVP Server to which you are connected, for identification purposes only. You cannot enter spaces in this field.
- **SVP-II TFTP Download Master** – this entry indicates the source of software updates for the SVP Server. Valid source location entries are:
  - **NONE** – TFTP request disables. This option allows to start faster after a reboot.
  - **IP Address** – the IP address of a network TFTP server that will be used to transfer software updates to the SVP Server.
- **DNS server and DNS domain** – These settings are used to configure Domain Name services. Consult your system administrator for the correct settings. These can also be set to **DHCP**. This will cause the DHCP client in the SVP Server to attempt to automatically get the correct setting from the DHCP server. The DHCP setting is only valid when the IP address is also acquired using DHCP.
- **WINS servers** – These setting are used for Windows Name Services. Consult your system administrator for the correct settings. These can also be set to DHCP. This will cause the DHCP client in the SVP Server to attempt to automatically get the correct setting from the DHCP server. The DHCP setting is only valid when the IP address is also acquired using DHCP.

When the name services are set up correctly, the SVP Server can translate hostnames to IP addresses. Using Telnet, it is also possible to access the SVP Server using its hostname instead of the IP address.

- **Workgroup** – as set in WINS.
- **Syslog Server** – Logging can be set to Syslog or NONE. If Syslog is set, a message is sent to the syslog server when an alarm is triggered.

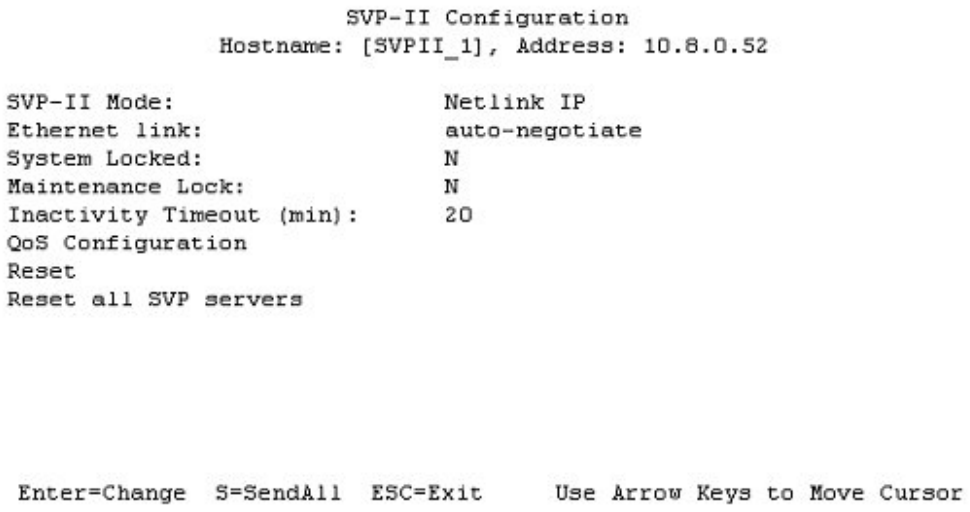
The SVP Server must be reset in order to set the configuration options. If the SVP Server is in **Maintenance Lock**, you will be prompted to reset the SVP Server upon pressing Esc. Respond with a **Y** to the reset prompt.

The SVP Server may be manually reset by selecting the **Reset** option in the **SVP-II Configuration** screen and then pressing **Y** (Yes).

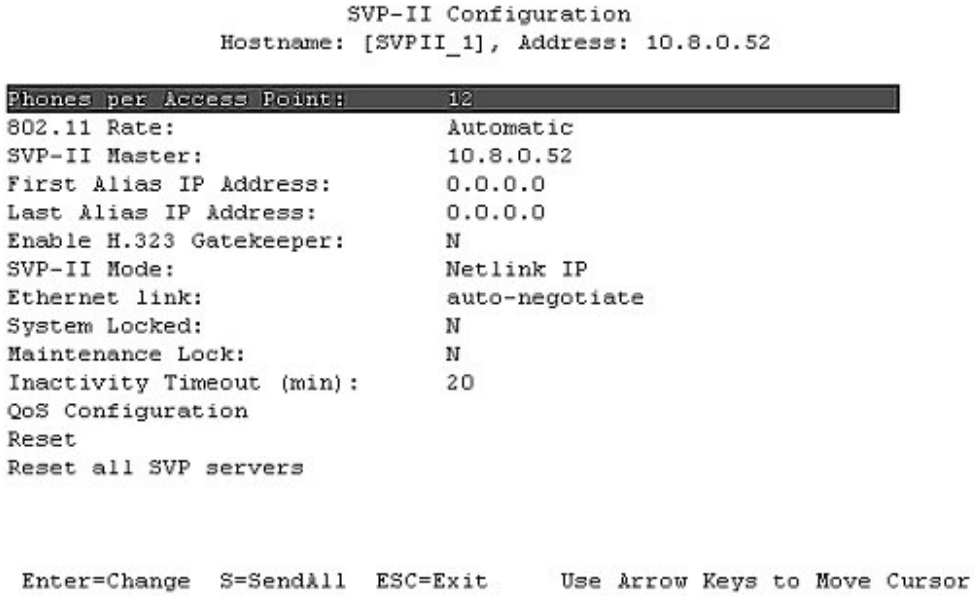
5.2.4.3.4 SVP Server Configuration

The **SVP-II Configuration** screen is where you set the SVP Server mode. This is also where you can lock the SVP Server for maintenance and reset the SVP Server after maintenance. The type of gateway you are using determines the SVP Server mode.

From the main menu, scroll to **SVP-II Configuration** and select by pressing Enter.



SVP-II Mode: The default value "NetLink IP" must be kept for an IP environment. Use the Enter key to select any item. The screen refreshes with additional options for the IP environment.



The following options must be configured:

- **Phones per Access Point**: access point specifications are detailed in the Configuration Notes. Refer to these notes when entering the number of simultaneous calls supported. Alcatel-Lucent recommends configuring 11 phones per Access Point.

- **802.11 Rate**: select 1MB/2MB to limit the transmission rate between the IP Touch WLAN handsets and Access Points. Select **Automatic** to allow the handset to determine its rate (up to 11 Mb/s).
- **SVP-II Master**:
  - The local SVP server is the master SVP server. Enter the IP address of the local server.
  - The local SVP server is a slave SVP server. Enter the IP address of the master SVP server.
- **First Alias IP Address/Last Alias IP Address**: enter the range of IP addresses this SVP Server may use when acting as proxy for the IP Touch WLAN handset.
  All alias addresses must be on the same subnet as the SVP Server and cannot be duplicated on other subnets or SVP Servers. There is no limit to the number of addresses that can be assigned, but the capacity of each SVP Server is 500 handsets.
- **Enable H.323 Gatekeeper**: as of R2.0, the gatekeeper is no longer used. This parameter must be set to N (no).
- **Ethernet link**: the SVP Server will auto-negotiate unless there is a need to specify a link speed.
- **System Locked**: this option is used to take the system down for maintenance. The default entry is N (No). Set it at Y (Yes) to prevent any new calls from starting. Return to N to restore normal operation.
- **Maintenance Lock**: the system automatically sets this option to Y (Yes) after certain maintenance activities that require reset, such as changing the IP address. A maintenance lock prevents any new calls from starting. Note that the administrator cannot change this option. It is automatically set by the system. Reset the system at exit to clear the maintenance lock.
- **Inactivity Timeout (min)**: set the number of minutes the administration module can be left unattended before the system closes it. This number can be from 1 to 100. If it is set to zero (0), the administration module will not close due to inactivity.
- **QoS Configuration**: select this option to set the DSCP tags. See: § QoS Configuration .
- **Reset System**: when this option is selected, you are prompted to reset the SVP Server upon exiting this screen.
- **Reset All SVP Servers**: when this option is selected, you are prompted to reset all SVP Servers upon exiting this screen. This is necessary if you have changed configurations on other SVP Servers by using the SendAll option.

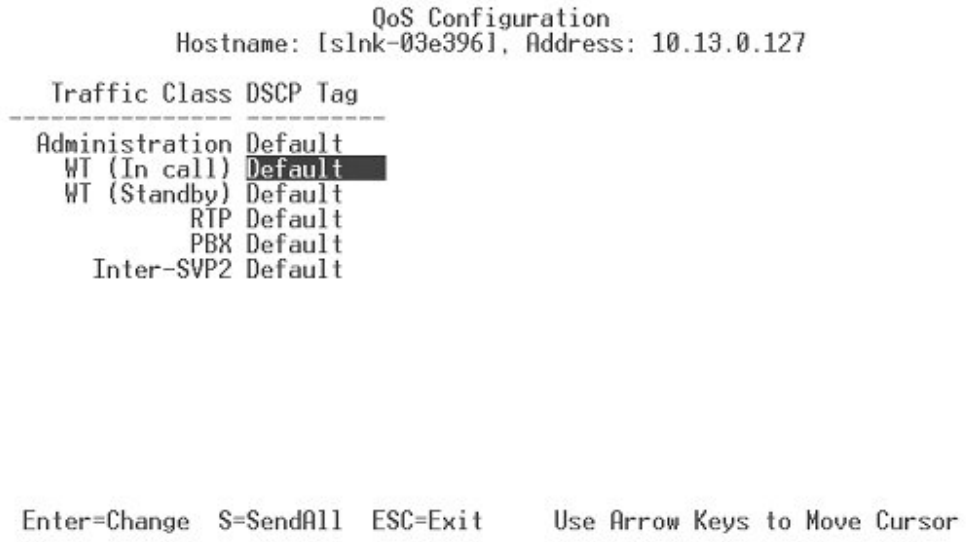
Notes:

The SVP Server should be reset at the end of any maintenance procedure that requires a reset either via Maintenance Lock or manually via Reset System.

Resetting the SVP Server will terminate any calls in progress.

5.2.4.3.5 QoS Configuration

DSCP (Differentiated Services Code Point) tags set packet priorities for QoS:



DSCP Tag: is a QoS mechanism to set relative priorities. Packets are tagged with a DSCP field in the IP header for type of service. The value may be set as a number from 0-255 and may be different for each traffic class listed on the screen. The default for all traffic classes is 16

- **Administration** tags set the priority for telnet, TFTP, and other administration traffic. Administration traffic can have the lowest priority because it does not require voice quality.
- **WT (In call)** traffic requires voice quality and may be set to a higher priority than WT (Standby) traffic.
- **RTP** traffic is the audio traffic to the IP PCX. It requires voice quality.
- **PBX** traffic to the PCX is not audio .
- **Inter-SVP2** traffic is the information transmission protocol SVP Servers use to communicate with each other

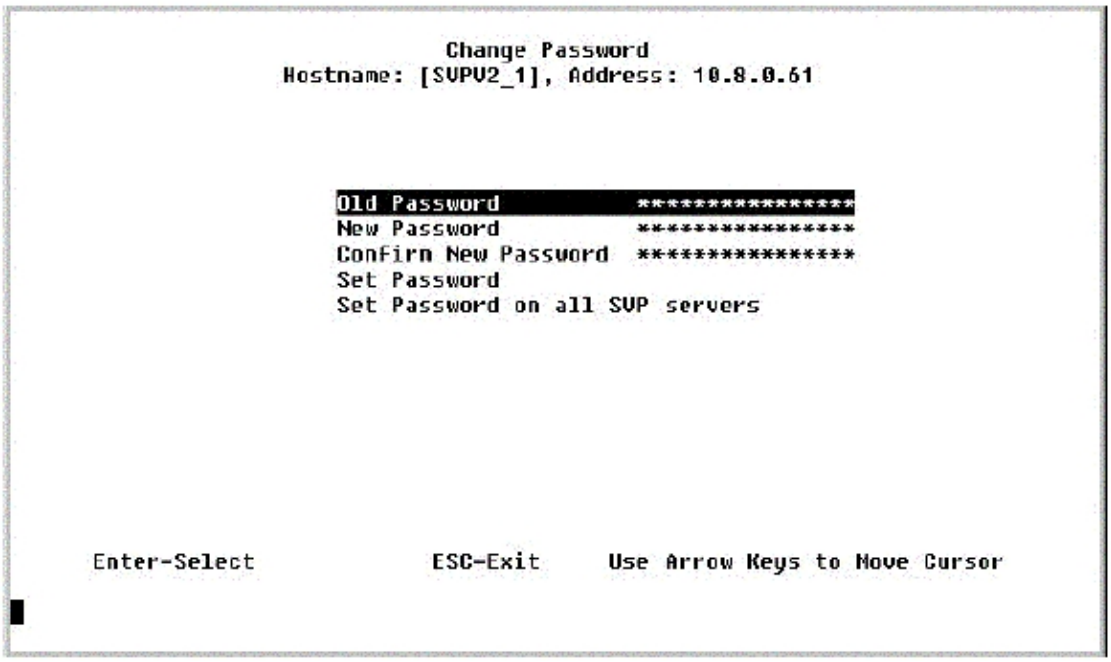
5.2.4.3.6 Change Password:

If desired, the password to access the SVP Server may be changed.

Password parameters:

- More than four characters
- The first character must be a letter
- Other characters may be numbers or letters
- No dashes, spaces, or punctuation marks, or other special characters. (alphanumeric digits only)

Select **Change Password** from the main menu. A screen similar to the following appears:



Enter the information and either select **Set Password** or press the **S** key to set the new password.

If you forget a password, call Alcatel-Lucent Customer Service for assistance.

5.2.4.3.7 Swapping/Adding/Deleting SVP Servers

Whenever an SVP Server is removed from the system, handsets using the SVP Server are affected. If the removal of the SVP Server is intentional, the administrator should lock and stop the system prior to removing an SVP Server.

Adding an SVP Server

A new SVP Server is detected within two seconds of being added to the system (booted/configured/connected). When detected, any handset not active in a call is immediately forced to reboot and check-in again. Any handset in a call immediately switches to the SVP Server which provides its "timing" function. This switch is not noticeable to the user as it is similar to a typical handoff between access points. When the handset ends the call, it is forced to check out and check in again.

Removing an SVP Server

When an SVP Server is removed from the system, it is detected within two seconds. Handsets not in calls are immediately forced to reboot and check in again. For handsets active in calls, two possible scenarios can occur. If the SVP Server that was removed was providing the "gateway" for the handset, then the call is lost and the handset is forced to check in again. If the SVP Server that was removed was providing the "timing" for the call, the call switches to the SVP Server that now provides the "timing". Note that during the two seconds while the loss of the SVP Server is being detected, the audio for the call is lost.

Changing the Master SVP Server

In the event the master SVP Server loses communication with the network, the handset system fails. All SVP Servers lock, all calls are lost and no calls can be placed. Therefore, if the master SVP Server needs to be replaced, ensure the system can be brought down with

minimal call interruption. Reset all SVP Servers after the master has been replaced. If the IP address of the master is changed, it must be changed in all SVP Servers.

5.2.4.3.8 Software Maintenance

The SVP Server uses proprietary software programs written and maintained by Alcatel-Lucent. The software versions that are running on the system components can be displayed via the **System Status** screen.

Alcatel-Lucent or its authorised dealer will provide information about software updates and how to obtain the software (for example, downloading from a web site).

At startup, the SVP Server uses TFTP to check the software version it is running against the version in the TFTP location. If there is a discrepancy, the SVP Server will download the version in the TFTP location.

Software Updates

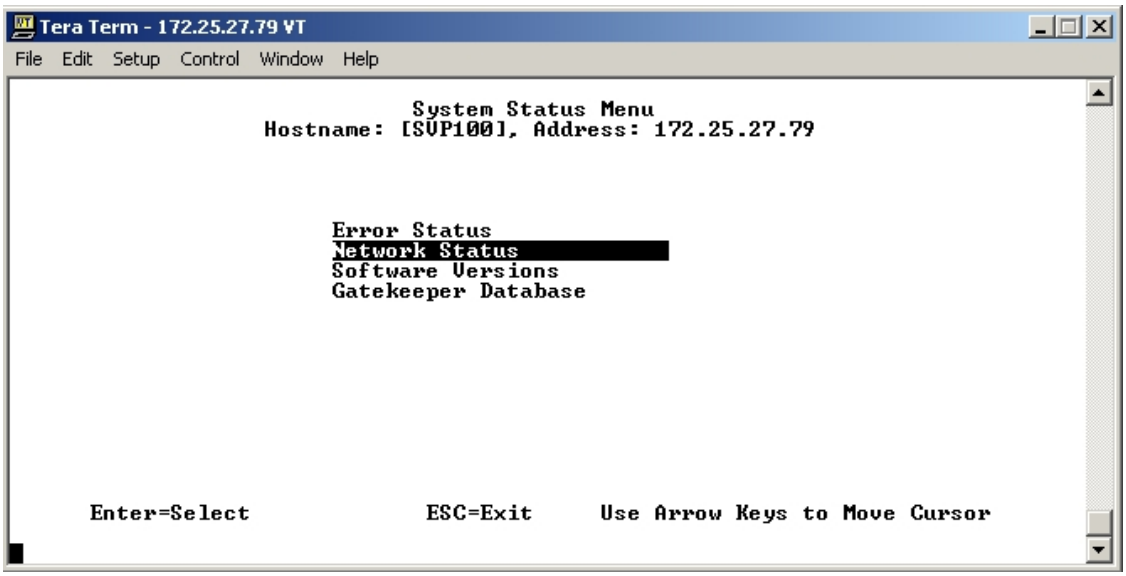
Lock the SVP Server in the **SVP-II Configuration** screen prior to updating the software.

After software updates are obtained from Alcatel-Lucent, they must be transferred to the TFTP location in the LAN to update the code used by the SVP Server.

Note that locking the SVP Server will prevent new calls from starting. All calls in progress will be terminated when the SVP Server is reset.

5.2.4.3.9 Troubleshooting via System Status Menu

Information about system alarms, and network status displays on various screens accessed through the **System Status Menu** screen, opened from the main menu of the SVP Server. See the previous sections for directions on how to connect to the SVP Server and navigate to the **System Status Menu**.



Error Status – displays alarm and error message information.

Network Status – displays information about the Ethernet network to which the SVP Server is connected.

Software Versions – lists the software version for each component.

Gatekeeper Database – as of R2.0, the gatekeeper is no longer used.

Options on the System Status Menu provide a window into the real time operation of the components of the system. Use this data to determine system function and to troubleshoot areas that may be experiencing trouble.

Error Status

The **Error Status** screen displays any alarms that indicate some system malfunction. Some of these alarms are easily remedied and others require a call to Alcatel-Lucent support.

From the **System Status Menu**, select **Error Status**. The screen displays active alarms on the SVP Server. The SVP server does not record the history of alarms. To record the alarm history, a Syslog server must be used. Its IP address must be declared in § Network Configuration .

The following table displays the list of alarms and a description of the action to take to eliminate the alarm.

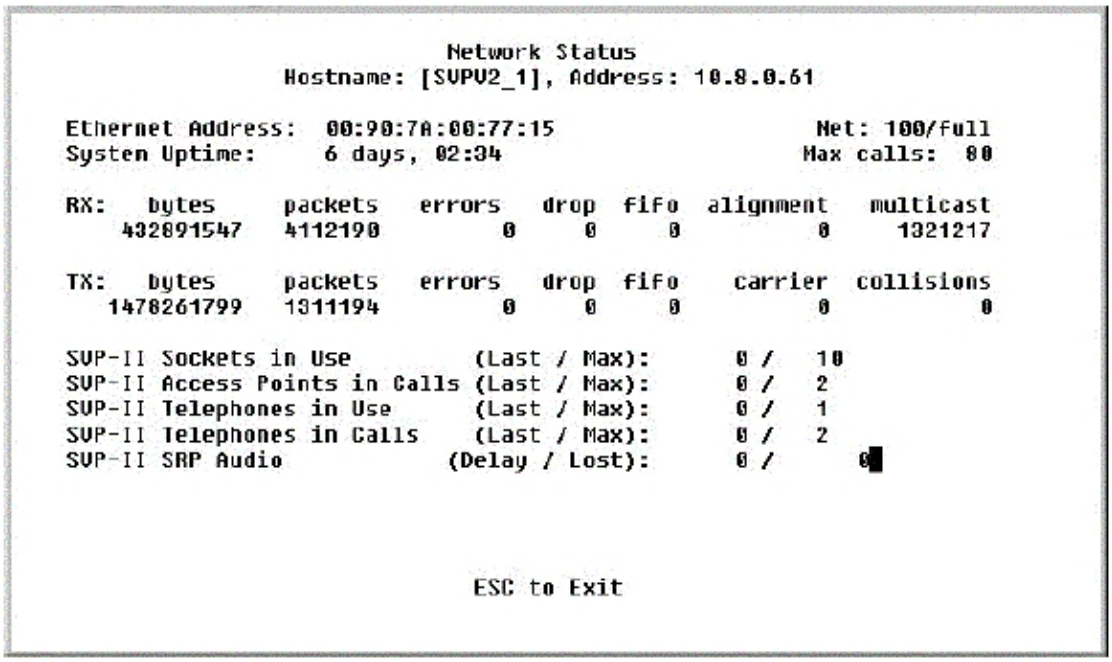
Alarm Text	Action
Maximum payload usage reached	Reduce usage, clear alarm
Maximum telephone usage reached	Reduce usage, clear alarm
Maximum access point usage reached	Reduce usage, clear alarm
Maximum call usage reached	Reduce usage, clear alarm
SRP audio delayed	Reduce usage, clear alarm
SRP audio lost	Reduce usage, clear alarm
No IP address	Configure an IP address

Press C to clear all clearable alarms.

Network Status

The SVP Server is connected to the Ethernet network, referred to as the LAN or Local Area Network. The information about that connection is provided through the **Network Status** screen.

From the **System Status Menu**, select **Network Status**. The screen displays information about the Ethernet network. This information can help troubleshoot network problems. A sample screen is displayed here.



Ethernet Address – MAC address of the SVP Server (hexadecimal).

System Uptime – the number of days, hours and minutes since the SVP Server was last reset.

Net – the type of connection to the Ethernet switch currently utilised. See SVP100 Capacity for more information.

Data is transmitted over Alcatel-Lucentcomponents by proprietary technology developed by Alcatel-Lucent. The Spectralink Radio Protocol (SRP) packets and bytes can be differentiated from other types of transmissions and are used to evaluate system functioning by Alcatel-Lucent customer support and engineering personnel.

RX – Ethernet statistics concerning the received packets during System Uptime.

bytes – bytes received

packets – packets received

errors – sum of all receive errors (long packet, short packet, CRC, overrun, alignment)

drop – packets dropped due to insufficient memory

fifo – overrun occurred during reception

alignment – nonoctet-aligned packets (number of bits NOT divisible by eight)

multicast – packets received with a broadcast or multicast destination address

TX – Ethernet statistics concerning the transmitted packets during System Uptime.

bytes – bytes transmitted

packets – packets transmitted

errors – sum of all transmit errors (heartbeat, late collision, repeated collision, underrun, carrier)

drop – packets dropped due to insufficient memory

fifo – underrun occurred during transmission

carrier – carrier lost during transmission

collisions – packets deferred (delayed) due to collision

SVP-II Access Points in Use – access points in use by WLAN handsets, either in standby or in a call 'Last' is current, 'Max' is the maximum number in use at one time.

SVP-II Access Points in Calls – Access Points with handsets in a call

SVP-II Telephones in Use – Handsets in standby or in a call

SVP-II Telephones in Calls – Handsets in a call

SVP-II SRP Audio (Delay) – SRP audio packets whose transmission was momentarily delayed

SVP-II SRP Audio (Lost) – SRP audio packets dropped due to insufficient memory resources

Software Version

The SVP Server and IP Touch WLAN handsets use an Alcatel-Lucent proprietary software controlled and maintained through versioning. The **Software Version** screen provides information about the version currently running on the SVP Server. This information helps you determine if you are running the most recent version and assists Alcatel-Lucent engineering and/or customer support in troubleshooting software problems.

This screen also displays the model type.

From the **System Status Menu**, **select Software Version**. A sample screen is displayed here.

```
                    Software Version Numbers
Hostname: [slnk-03e396], Address: 10.13.0.127


SVP Type:                 010
Hardware Versions:        33/02
Factory Page:             230.009
Downloader:               71.002 (2a644ba2)
Table of Contents:        213.002 (9fb4e4ca)
Functional Code:          213.001 (ba8f6119)
File System:              213.002 (b896c80f)


                          ESC to Exit
```

Note that the software versions on your system are different from the versions displayed in the above sample screen.

5.3 Advanced Cellular Extension

5.3.1 Overview

5.3.1.1 Overview

The Advanced Cellular Extension service (ACE) is a feature of the Alcatel-Lucent OmniPCX Office Communication Server, providing corporate telephony services to authorized mobile users.

The Advanced Cellular Extension operates in association with a software client application hosted on a mobile phone. This software client provides a menu driven interface to access Alcatel-Lucent OmniPCX Office Communication Server services.

The software client can be either:

- The Ace client R2.3

  Note 1:
  The mobile device must be compliant with the Ace application. The list of compatible mobile devices is available on the BPWS (Business Partner Web Site).

- The Nokia Intellisync Call Connect (ICC) v2.1 for Alcatel-Lucent software

  Note 2:
  The list of compatible mobile devices and more information on Nokia Intellisync Call Connect for Alcatel-Lucent can be found on the Nokia web site:

  http://europe.nokia.com/A4195042

Note 3:
*In this document, **Advanced Cellular Extension** (**ACE**) refers to the feature of the Alcatel-Lucent OmniPCX Enterprise CS. **Ace** refers to the client software hosted on a mobile phone.*

5.3.1.2 Implementation

The ACE mobile phone is associated with local set of the PCX.

The telephony services provided by the ACE are the same as those provided by remote customization. On the mobile device, the improved graphical user interface provides easy to use ACE features.

Incoming calls directed to the user's local set are rerouted to the mobile phone by the nomadic feature.

In ACE mode, mobile phone users dial as if they were internal users of the PCX: the call is routed to the PCX through remote substitution (DISA) and sent to its destination. When the called set is an internal set, ARS is used to avoid going through public network.

Caution:
Numbers corresponding to emergency numbers are not treated as internal PCX numbers by the mobile phone, even in ACE mode. The emergency centre is called, whatever the mobile mode: ACE or private.

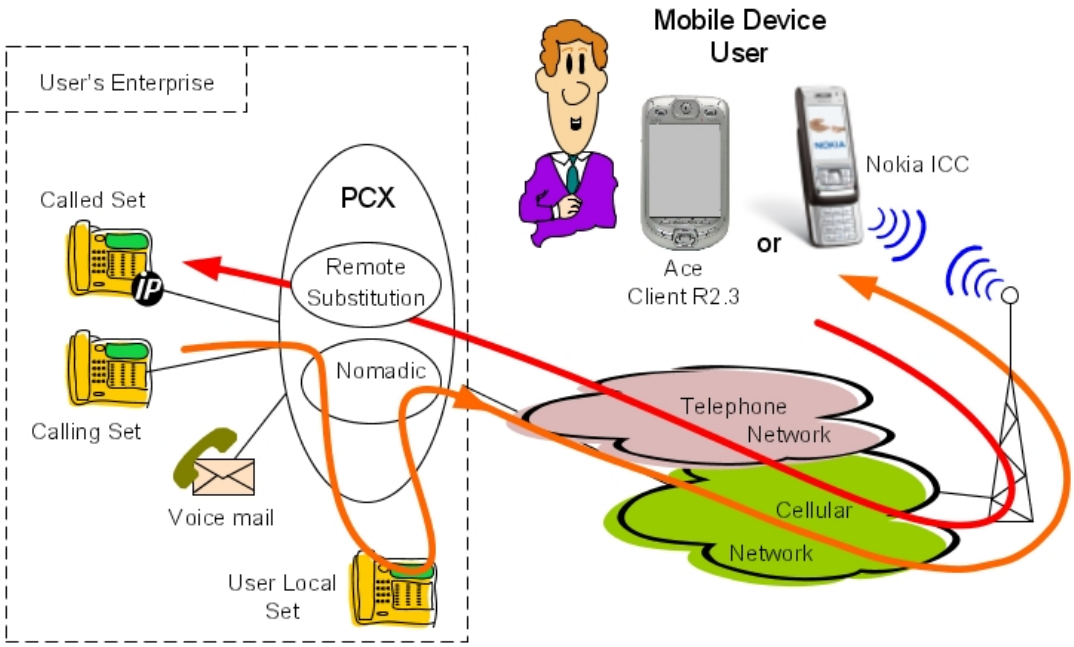


Figure 5.126 : ACE Cellular Mode Architecture

5.3.2 Configuration procedure

This chapter details the configuration on Alcatel-Lucent OmniPCX Office Communication Server to implement Advanced Cellular Extension.

5.3.2.1 Configuration Example Values

The configuration example described below is based on the following values:

- DDI number for remote substitution: 0388553790
- DDI number for remote customization: 0388408370
- User's local desktop:
  - Internal number: 1165
  - DDI number: 0390671165
- Mobile phone:
  - Public number: 0611223344
- Range of local user numbers: 1000-1999
- Operator call number: 9

5.3.2.2 Pre-requisites:

The Advanced Cellular Extension implementation requires:

- An Alcatel-Lucent OmniPCX Office Communication Server R7.0 (or later version)

- An ISDN trunk group to the public network
- The **DISA / DISA Transit** licence
- The **Voice Mail Remote Customization** licence
- A **Nomadic user** licence per ACE subscriber
- A DDI number for remote substitution (DISA)
- A DDI number for remote customization
- One DDI number per ACE subscriber (local user set number)

5.3.2.2.1 Checking Licences

1. In OMC (Expert View), select **Modification Typical** > **System** > **Software key**
2. Click **Details**
3. In the **System features** tab, check that **DISA / DISA Transit** is enabled
4. In the **Call Facilities** tab, check that **Voice Mail Remote Customization** is enabled
5. In the **CTI** tab, check the **Nomadic users** value: a licence is necessary for each virtual nomadic terminal, including ACE subscribers.

5.3.2.2.2 Configuring DDI Numbers

If necessary, create DDI numbers:

1. In OMC (Expert View), select **Dialling** > **Dialling Plans** > **Public Numbering Plan**
2. Define a DDI number for remote substitution
3. Define a DDI number for remote customization

   Note:
   The remote customization number corresponds to the directory number of the hunting group containing the voice mail ports.
4. Define a DDI number for each ACE subscriber (local user set number)

5.3.2.3 PCX Configuration

5.3.2.3.1 Configuring the Numbering Plan

It is necessary to create secondary trunk groups corresponding to the internal numbers that can be dialled on the mobile phone. In our example, this corresponds to the internal user numbers (1000-1999) and the operator call number (9)

1. In OMC (Expert View), select **Dialling** > **Dialling Plans** > **Internal Dialling Plan**
2. Create a **Secondary Trunk Group** corresponding to internal user numbers:
   - **Start**: #1000
   - **End**: #1999
   - **Base**: **ARS**
   - **NMT**: **Yes**
3. Create a **Secondary Trunk Group** corresponding to the attendant call number:
   - **Start**: #9
   - **End**: #9

- **Base**: **ARS**
- **NMT**: **Yes**

4. Confirm your entries

Caution:
There should be no internal number corresponding to emergency numbers (e.g. 112). Indeed it is not possible for a mobile subscriber to call an internal user whose directory number corresponds to an emergency number. Whether in ACE mode or not, the emergency centre is always called: this operation mode cannot be modified on the mobile phone.

5.3.2.3.2 Configuring a Local Trunk Group

A local trunk group is used by the ARS to route local calls. If necessary, create a local trunk group:

1. In OMC (Expert View), select **Numbering** > **Automatic Routing Selection** > **Trunk Group Lists**
2. Right-click and select **Add**
3. Review/modify the following attributes:
   - **List ID**: 6
   - **Index**: **Local**
   - **No.**: leave blank

5.3.2.3.3 Configuring ARS

The ARS must be configured to route local calls to a local trunk group.

1. In OMC (Expert View), select **Numbering** > **Automatic Routing Selection** > **Automatic Routing: Prefixes**
2. Add a prefix corresponding to the internal subscriber number range
   - **Activation**: **Yes**
   - **Network**: **Priv**
   - **Prefix**: #1
   - **Ranges**: 000-999
   - **Substitute**: 1
   - **TrGpList**: 6
3. Add a prefix corresponding to the attendant call number:
   - **Activation**: **Yes**
   - **Network**: **Priv**
   - **Prefix**: #9
   - **Ranges**: leave blank
   - **Substitute**: 9
   - **TrGpList**: 6 (local trunk group number)

5.3.2.3.4 Configuring an ACE Subscriber

To configure an ACE subscriber, perform any of the following:

- Basic configuration: the local user set is assigned the right to the nomadic feature: in this

case, the local set cannot be used when ACE is activated on the mobile set.

- Twin-set configuration: the local user set is associated to a virtual set in a multi-set configuration and only the virtual set is assigned the nomadic right. In this case, the user's local set can still be used when ACE is activated on the mobile set.

Basic Configuration

1. In OMC (Expert View), in the **Users/Base stations List**, select the user's local number (1165)
2. Click **Details**
3. Click **Features**
4. Enable the **Remote Substitution**
5. Confirm your entries
6. Click **Cent Serv**.
7. Enable the **Nomadic Right**
8. Confirm your entries

Multi-Set Configuration

To create a virtual terminal:

1. In OMC, in the **Users/Base stations List**, click **Add**
2. Check the **Virtual Terminal** radio button and select the virtual set **No.**
3. Click **OK**.
4. In the **Users/Base stations List**, select the new virtual terminal and click **Details**
5. Click **Cent Serv**.
6. Enable the **Nomadic Right**
7. Confirm your entries

To configure the user's local set:

1. In OMC (Expert View), in the **Users/Base stations List**, select the local user (1165)
2. Click **Details**
3. Create a multi-set association with the new virtual set
4. Click **Features**
5. Enable the **Remote Substitution**
6. Confirm your entries

Note:
In this configuration, the nomadic right must not be enabled on the user's local set.

5.3.2.4 Client Installation and Configuration

To install and configure the Ace client software on a mobile set, refer to the Ace R2.3 Installation Manual.

To install and configure the Nokia ICC client software on a mobile set, refer to the **Nokia Intellisync Call Connect Administration Guide**.

5.3.2.5 Nomadic Activation

Once the Alcatel-Lucent OmniPCX Office Communication Server is configured and the software client is installed and configured on the mobile phone, it is necessary to activate manually (one time) the nomadic mode to register the mobile number in the system.

This manual activation can be performed from any set except the user's local set. If the activation is performed from a mobile set, ACE must not be activated.

1. Dial the remote customization number
   A voice guide requests your local phone number
2. Dial your local phone number (1165) and your password
3. Press 9 to enter the remote customization main menu
4. Press 6 to enter the nomadic mode settings
5. Press 2 to activate the nomadic mode
6. Dial the mobile number (trunk seizure prefix + mobile number) example: 00611223344
7. Press # to validate

Chapter 6

VoIP Services

6.1 General Presentation

6.1.1 Services

6.1.1.1 Overview

Alcatel-Lucent OmniPCX Office Communication Server provides 2 services that can be combined:

- Voice over IP is based on the Integrated H.323/SIP Gateway, the core of Voice over IP (VoIP), which allows communication between the conventional telephony world and the data world.
- IP telephony enables an enterprise to share its data infrastructure (local IP network) between the data world and the telephone world by means of IP terminals which connect to the LAN and/or a Windows application on a Multimedia PC (PIMphony IP Edition) to simulate a LAN PC station. For more information about PIMphony IP Edition, consult the "Installation - configuration" file in the "Voice over IP" section.

Remark:

IP terminals can be:

- *Alcatel-Lucent 8 series sets*
- *Alcatel-Lucent IP Touch 310/610 WLAN Handsets*
- *Alcatel-Lucent Mobile IP Touch 300/600*

The Voice over IP services are provided by a daughter board VoIPx-1 on the main CPU and/or several (max. 6) CoCPU/CoCPU-1/CoCPU-2 (CoProcessing Unit) boards. This VoIPx-1 board integrates an H.323/SIP gateway which has the following main characteristics:

- from 4 to 96 DSP channels for the H.323/SIP gateway and IP Telephony services (DSP channels for coding / decoding the audio signal)
- supports the audio compression algorithms G711, G729a and G723.1
- IP communications in Full Duplex mode
- use of RTP/RTCP to send audio signals in real time
- supports the T38 protocol (Fax over IP): a Fax type call can be routed over IP through a T38 fax channel
- echo suppression
- gain improvement
- tone generation and detection
- silence suppression (VAD). Note: do not activate voice detection on an IP station with Codec G711

Additional characteristics applicable to the SIP gateway:

- direct RTP , reducing DSP channel allocation
- SIP option for (remote) gateway Keep Alive

Note:

All communications and VoIP signals transit via the CoCPU VoIP board, except in the case of communications between a PC with PIMphony IP and an IP terminal, between IP terminals, or between IP terminals and IP trunks when direct RTP is activated. In all these cases only signalling transits via the CoCPU.

6.1.1.1.1 Quality of Service (QoS)

Mechanisms in the system's ARS determine whether a VoIP call to a remote H.323/SIP gateway can be made without degradation of bandwidth (see "Installation - Configuration" File).

The aim is to provide an "end-to-end" QoS for all audio IP packets.

To achieve this, the system supports IP ToS (IP Type of Service): each IP VoIP packet contains a 3-bit precedence field indicating a level of priority. This information can be used by network elements (routers, gateways, etc.) to assign a level of priority to IP voice packets with respect to IP data packets. Alcatel-Lucent OmniPCX Office Communication Server also supports "DiffServ" (RFC 2475) and VLAN (since R5.0).

Note:

End-to-end quality of service can only be guaranteed if all network elements are IP ToS, DiffServ, or VLAN compatible.

6.1.1.1.2 Environment tests

The H.323/SIP gateway (CoCPU board equipped with VoIPx daughter board) is connected either to a 10 Mbps Ethernet LAN or to a 100 Mbps Fast Ethernet LAN via an RJ45 cable (category 5).

6.1.1.1.3 RTP proxy services

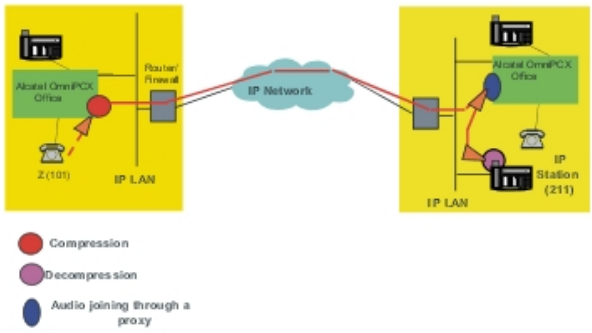
In the case of a call from an IP terminal to a remote H.323/SIP gateway via an IP H.323/SIP network, this service optimises the call audio quality.

It avoids any unnecessary compression/decompression of voice packets. In previous releases, the mechanism used to include the decompression of incoming packets, switching via the PCM bus, and a new PCM/IP compression in the outgoing channel.

This mechanism applies to calls from a handset (IP or not) connected to an Alcatel-Lucent OmniPCX Office Communication Server system, to an IP terminal (remote or local) connected to another Alcatel-Lucent OmniPCX Office Communication Server system.

Note:

The "RTP Proxy" function only applies if the Codecs are identical (for instance, same Codec for IP handsets and IP trunks). In the case of a Alcatel-Lucent 8 series IP Touch set, the Codec between the set and the Alcatel-Lucent OmniPCX Office Communication Server adapts itself to the Codec between the Alcatel-Lucent OmniPCX Office Communication Server and the IP trunk (Note: IP Touch Alcatel-Lucent 8 series does not support 90ms and 120ms framing and therefore IP trunk codecs should not use them). If the codecs are different, the former mechanism will be applied, namely: "incoming" call on the gateway, IP/PCM decompression and PCM/IP recompression for the "outgoing" call with a different codec.



6.1.1.1.4 Direct RTP

The direct RTP service provides direct RTP and RTPC flow exchange between IP endpoints (IP sets, DSP channels on VoIP or CoCPU boards, distant gateways..).

From Alcatel-Lucent OmniPCX Office Communication Server R6.0, the direct RTP feature is offered for SIP trunking and applies to private and public SIP trunking, provided that:

- The remote SIP proxies that the system is connected to are compatible with the transfer optimization method (support of Re-INVITE without SDP). Most of the SIP proxies support this method; Alcatel-Lucent OmniPCX Office Communication Server R5.0 and higher supports this method in reception.
- IP phones connected to the system support RFC2833 for DTMF sending.

The main advantages of direct RTP are:

- Audio path optimization, resulting in bandwidth use reduction in routers and network, better audio quality by delay reduction.
  - In addition to the proxy RTP and SIP optimization features, from R6.0 of Alcatel-Lucent OmniPCX Office Communication Server, direct RTP can be used for Transfer and Forwarding services in a heterogenous environment (need for configuration of the ARS table). For other services such as Hold (with music on hold), Record on line and Conference, the audio path is optimized by direct RTP on the distant side.
- Cost (and resource) reduction:
  - Thanks to direct flow between IP sets and **distant** gateways or IP sets it is no longer necessary to allocate DSP channels of the VoIP subscribers channel pool to basic external calls. Reduction of DSP channel needs result in cost optimization by the reduction of DSP daughterboards and CoCPU.

For more information about reduction of DSP daughterboards and CoCPU, refer to the Dimensioning section in the VoIP services chapter.

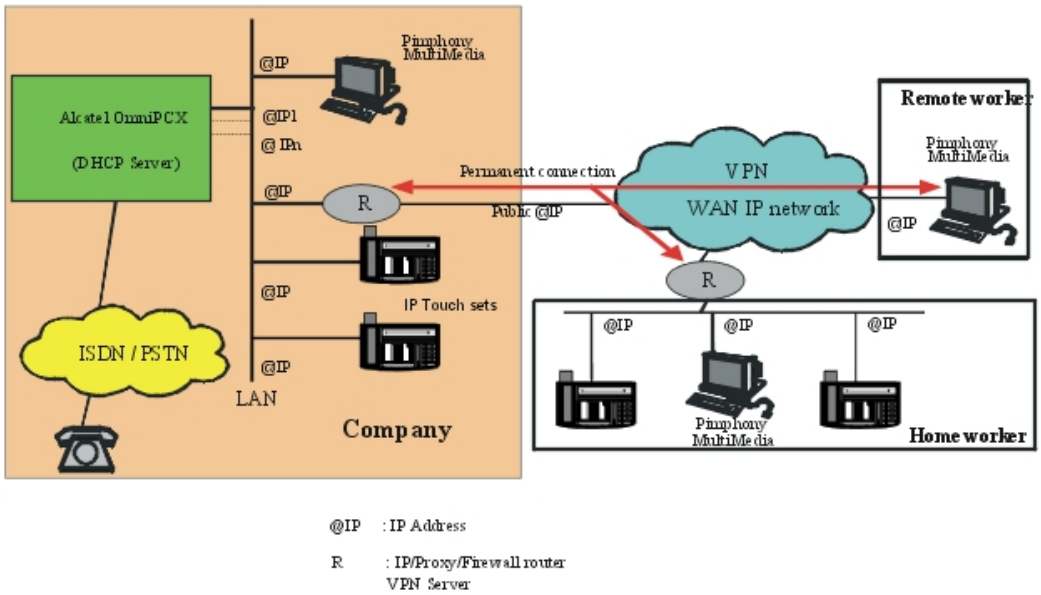
6.2 IP Telephony

6.2.1 Overview

The purpose of this section is to show how Alcatel OmniPCX Office can be connected to VLANs.

This service does not require any specific external equipment (IP and/or Proxy/Firewall

Router), unless it is provided for Remote/Home workers.



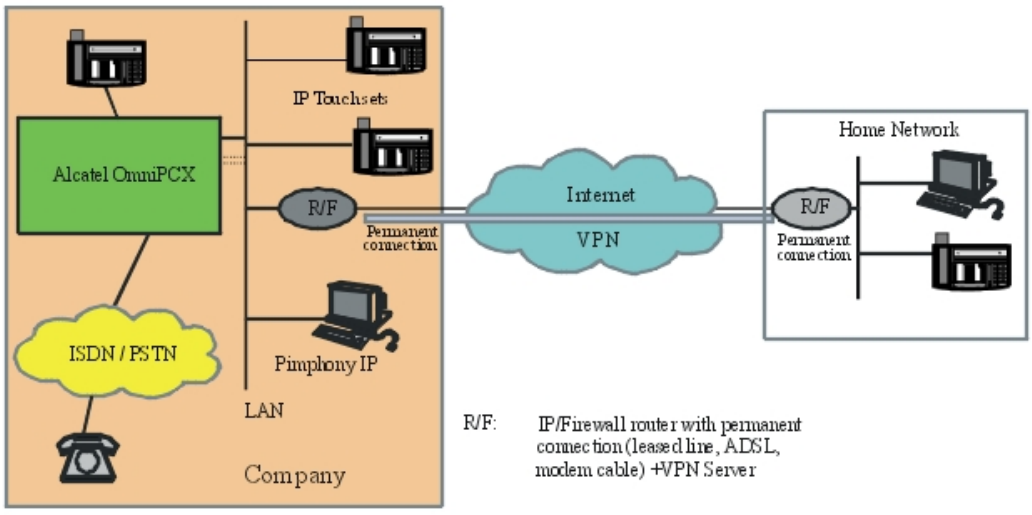
The IP router (R) connected to the Intranet can be a simple IP router. The reservation of bandwidth is "guaranteed" if this router supports IP ToS (DiffServ).

The number of remote IP Touch or PIMphony IP subscribers depends on the line bandwidth (no more than 2 simultaneous calls for 64 Kbps, 5 for 128 Kbps).

6.2.2 Home Worker

6.2.2.1 Detailed description

6.2.2.1.1 HOME WORKER (remote IP Telephony via a VPN)



The connection between the Home worker and the Internet must be "always-on" (ADSL, cable,

etc.). It is indispensable to have an IP/Proxy/Firewall router or a VPN server on the Home worker side.

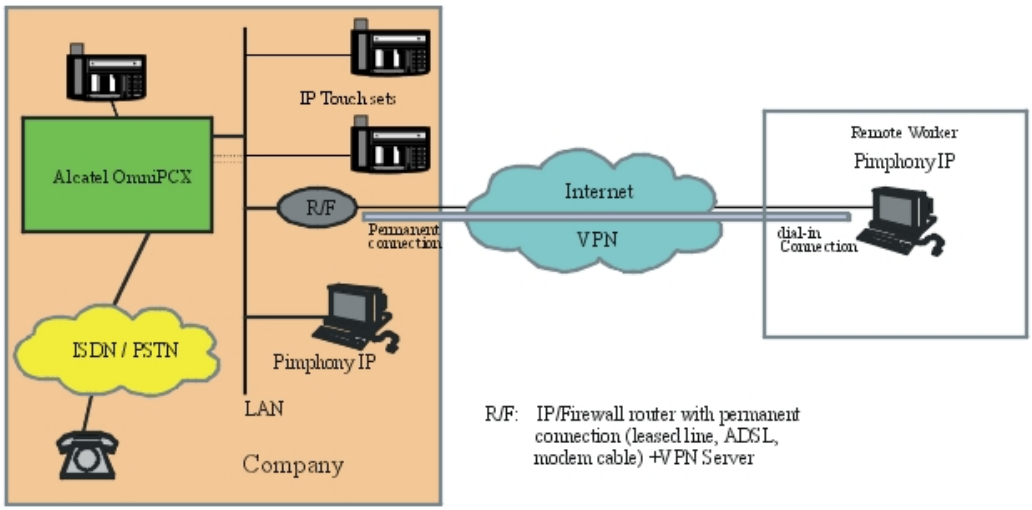
The IP router (R/F) at the front end of the VPN must offer Proxy/Firewall and VPN server functionality (IPSec with 3DES encryption for interoperability with the system's built-in router).

The number of remote IP Touch or PIMphony IP sets depends on the line bandwidth (no more than 2 simultaneous calls for 64 Kbps, 5 for 128 Kbps).

6.2.3 Remote Worker

6.2.3.1 Detailed description

6.2.3.1.1 REMOTE WORKER (PIMphony IP via a VPN)



The connection between the remote PC (PIMphony IP Edition) and the Internet is of the "dial-on-demand" type (V90 analogue, ISDN or ADSL modem). The remote PC first establishes a connection to the nearest access provider, then a PPTP connection to the company's VPN server.

PC with Microsoft NetMeeting®

The remote NetMeeting PC establishes a PPTP connection to the company's VPN server.

6.2.4 Configuring from an External DHCP

6.2.4.1 Overview

The following minimum parameters must be configured for **e-Reflexes stations:**

- IP address
- Subnet mask
- Router address

- TFTP address (DHCP option code 066)
- "Vendor Specific Information" option:
  - If the e-Reflexes station is configured in DHCP Alcatel-Lucent only, this option's value must be set to "a4200.0"
  - <Recommended> If the e-Reflexes station is configured in DHCP non-Alcatel-Lucent, this option must not be configured

6.2.5 Configuring Pimphony IP

6.2.5.1 Overview

6.2.5.1.1 Creating an IP user

A PC equipped with PIMphony IP is considered by the system as an IP user, in the same way as an IP set.

- For PIMphony you must create an IP user (of type "Multimedia PC") before installing PIMphony. This is done in the OMC tool, as follows:
  1. In the OMC tool, navigate to the screen **Subscribers/Basestations List** and click **Add**. This displays the **Add Subscriber** screen.
  2. Select **IP Terminal** and choose the EDN number in the **No.** field according to the numbering plan, then click **OK**.
  3. In the **Subscribers/Basestations List** screen, change the terminal type for the new subscriber to "PC Multimedia" in the **Terminal/Basestat.** field.

6.2.5.1.2 Registering the IP address

Unlike IP sets, Alcatel-Lucent OmniPCX Office Communication Server does not manage the IP address of a Multimedia PC; only its MAC address is registered at first connection. No software (firmware) is transferred between the system and PIMphony IP during the registration procedure.

Registration is an open operation based upon the IP protocol: the PC generates a Multicast request and waits for the reply from a VoIP CoCPU/CoCPU-1/CoCPU-2 board. During the reply/registration phase, the VoIP CoCPU/CoCPU-1/CoCPU-2 board indicates its IP address to the PC and the PC transmits its Ethernet address (MAC Address) to the PBX.

If there is no reply (e.g. IP routing problems), the PC generates the Multicast request several times, and if no reply is obtained, PIMphony IP enters into a "failure". The user is then asked to indicate the IP address of the master VoIP CoCPU/CoCPU-1/CoCPU-2 board; if the address is incorrect, another request is made.

Once registration has been performed, the IP address of the VoIP CoCPU/CoCPU-1/CoCPU-2 board is stored in the Windows registry and will be used for all future connections. If a problem arises, such as a change in the IP address of the VoIP CoCPU/CoCPU-1/CoCPU-2 board, a new registration sequence (Multicast request) is initiated.

After initialising PIMphony IP, IP connectivity must be permanent, otherwise the system considers the PC to be out of service.

Note:

A "Multimedia PC" in the subscribers list is a PC equipped with PIMphony IP Edition.

A "netmeeting PC" does not appear in the subscribers list; it is considered as an "external private num-

ber" and requires an entry in the ARS table.

6.2.5.1.3 Choosing the codec to be used

Three different codecs are available:

- G711
- G723.1
- G729A with framing of 30ms, 40 ms, 50 ms, 60 ms 90 ms or 120 ms(default value is 30 ms)

Note:
You cannot use framing value 90ms and 120ms for codecs G.723.1 and G.729a if IP Touch sets are connected to Alcatel-Lucent OmniPCX Office Communication Server.

With no compression mode, the G711 codec has the highest bandwidth requirements. The two other codecs (G729A and G723.1) support compressed speech, and you can reduce VoIP bandwidth by 35% by enabling the voice activity detection (check the box **With silence detection (VAD)**).

The Quality of Service applies to all codecs.

To enable your preferred codec:

1. Select the PIMphony menu **Configuration / Options.**
2. Click the **VoIP** tab.
3. Choose a VoIP Application board name or address, or automatically detect the VoIP board by clicking the **Auto-detect** button.
4. Select your preferred codec among the 3 options (G711 is the default preferred codec).

6.3 H.323 Gateway

6.3.1 H.323 Gateway Services

6.3.1.1 Detailed description

This service can be implemented in the following 2 ways:

- Using the IA board of the Alcatel-Lucent OmniPCX Office Communication Server as a router to the Internet with built-in VPN and Firewall
- Using an external router to the Internet or to a dedicated link

Note:
In the following diagrams, Alcatel-Lucent OmniPCX Office Communication Server is used for the Internet connection configuration and the external router is used for other types of connections (leased line, ADSL, etc.).

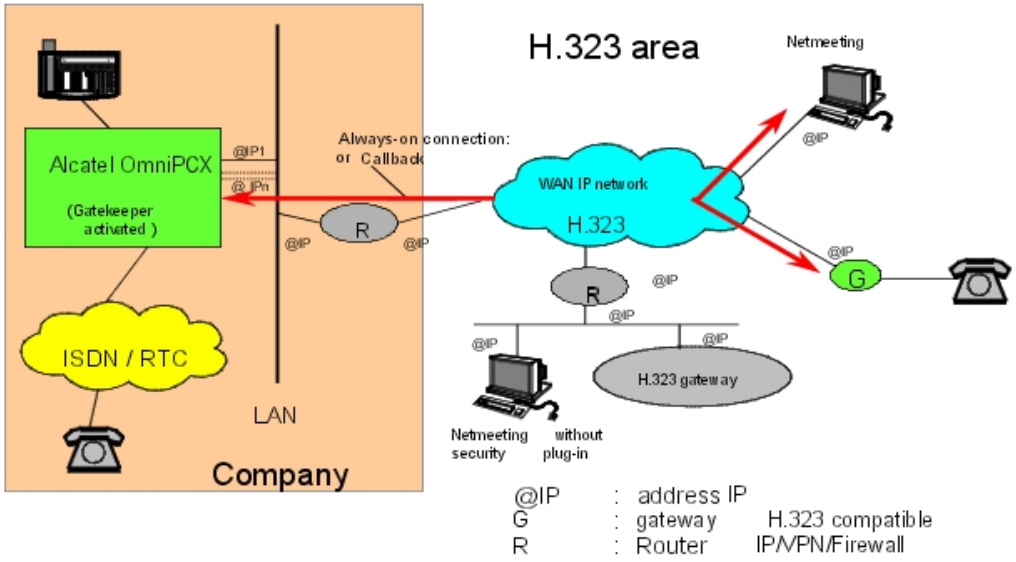
The Alcatel-Lucent OmniPCX Office Communication Server H.323 Gateway service can be implemented in the following 3 contexts:

- H.323 gateway integrated into a standalone configuration
- H.323 gateway integrated into an H.323 area

- Gateway managed from another Alcatel-Lucent OmniPCX Office Communication Server system

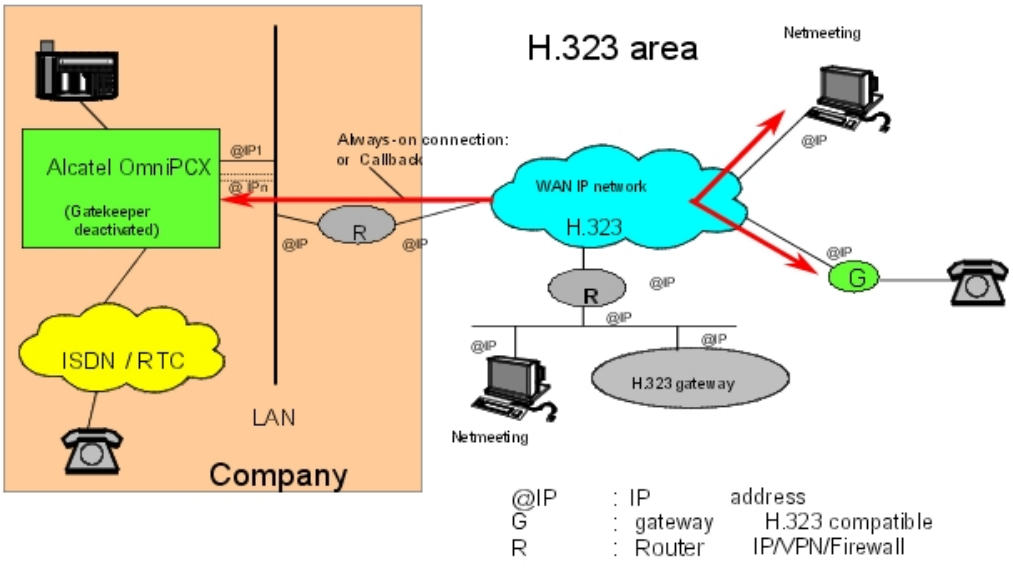
6.3.1.1.1 H.323 gateway integrated into a standalone configuration

In a standalone configuration, the integrated gatekeeper is alive; it is masked to the exterior and cannot be managed from the LAN.



6.3.1.1.2 Gateway in a H.323 area

In a network topology like the one below, the H.323 gateway of Alcatel-Lucent OmniPCX Office Communication Server can be integrated into an H.323 area managed by an external gatekeeper.

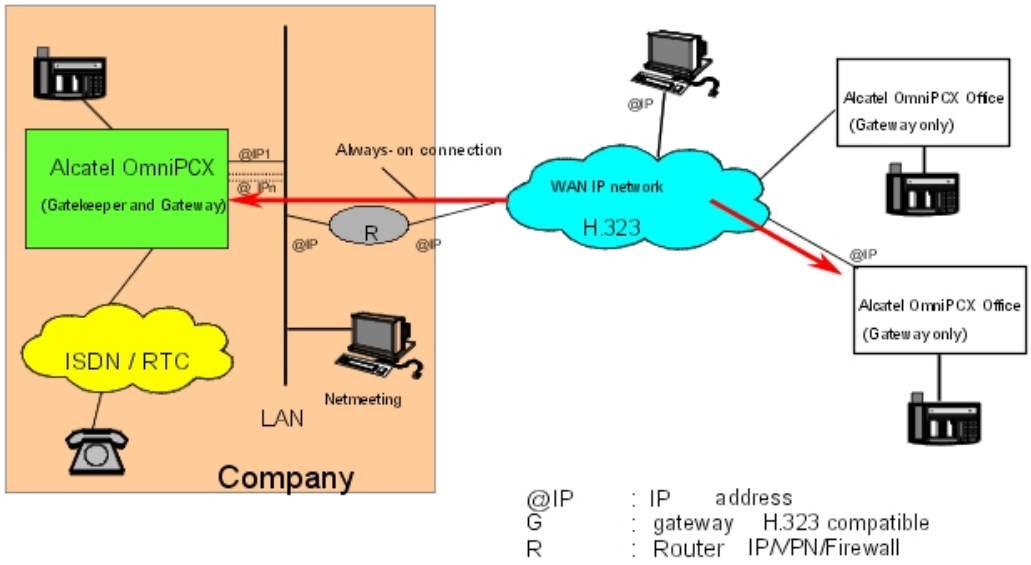


In this configuration, the gatekeeper integrated into Alcatel-Lucent OmniPCX Office Communication Server must be deactivated and the network administrator must supply the IP address of the external gatekeeper.

Note:

The ARS table must always contain all the IP addresses.

6.3.1.1.3 Gateway managed from another Alcatel-Lucent OmniPCX Office Communication Server system



In this configuration, the H.323 gateway is managed by a Gatekeeper which is integrated into another Alcatel-Lucent OmniPCX Office Communication Server system and which therefore has its own gateway. This configuration is suitable for small installations (less than 10 gateways and 50 PC/H.323 terminals).

This requires configuration of numbering plans in full for all systems. All the H.323 items (remote system, PC, H.323 terminals) should be defined in the ARS tables of all systems. The Gatekeepers integrated into other Alcatel-Lucent OmniPCX Office Communication Server systems should be inhibited and the IP address of these systems' external Gatekeeper should be the same as the master system's.

6.3.1.1.4 Fax over IP (FoIP)

The Fax over IP services are available when a Fax is detected in an H.323 call. When this happens, the Audio channels are closed and T38 sessions are initialised to transmit or receive Fax packets (IFP - Internet Fax Packet).

Alcatel-Lucent OmniPCX Office Communication Server only allows T38 sessions over UDP. In order to ensure the reliability of the UDP transmission, the packets are sent several times to ensure that the information reaches its destination; this operation is called "UDP Redundancy".

In order to reduce bandwidth use, an operation (framing) allows the concatenation of packets of the same type.

The Fax over IP (FoIP) service does not require any particular configuration of the ARS table. A Fax call is considered as a transparent H.323 call to the ARS operations.

6.3.2 Service H.450

6.3.2.1 Detailed description

The following services are supported:

H.450 Service	Supported level
H.450.1: Generic functional protocol for additional H.323 services	Supported
H.450.2: Call transfer	Supervised transfer: supported Unsupervised transfer: - if the destination is an Alcatel-Lucent OmniPCX Office Communication Server: supported - if the destination does not support this feature, a transfer by joining is made by forwarding Alcatel-Lucent OmniPCX Office Communication Server
H.450.3: Call forwarding	Immediate diversion: supported (including PO forwarding) Other forwarding: not supported
H.450.4: Warning	Not supported
H.450.5: Call parking/pick-up	Not supported
H.450.6: Call signalling on the called station	Not supported
H.450.7: Camped-on call signalling	Not supported
H.450.8: Advanced display and information	Not supported

Optimising resources

The H450 protocol allows not to use the voice coding resources on Alcatel-Lucent OmniPCX Office Communication Server. In the case of a transfer or a forwarding request, the two initial calls are released and replaced with a single direct call between the two parties. Thus, the bandwidth consumption is decreased and all the DSP resources used for the initial calls are released on the Alcatel-Lucent OmniPCX Office Communication Server performing the forwarding or the transfer.

Note:

Alcatel-Lucent OmniPCX Office Communication Server cannot fully optimise a three-node transfer. In this case, the transfer is made by joining.

6.3.3 Topologies

6.3.3.1 Architecture

This section describes typical IP network architecture for implementing the Alcatel-Lucent

OmniPCX Office Communication Server Voice over IP services.

A V4-compatible H.323 gateway complies with recommendations to provide support for:

- Q.931/Q932 signalling
- H.225 v4 protocol for establishing signalling channels between H.323 gateways (including Fast Connect)
- H.245 v7 protocol to monitor communications: establishing channels, negotiating the Codec, etc.
- RAS signalling for communications with the H.225 internal gatekeeper (H.225 v4) or to the outside (authentication, authorisation, bandwidth management)
- H.450.1, H.450.2, H.450.3: additional services (transfer, forwarding)

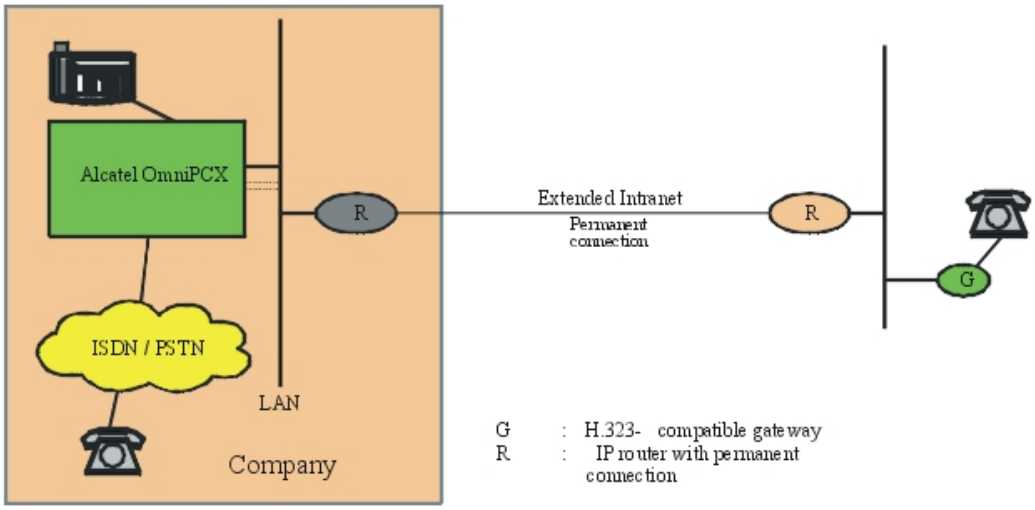
The gateway also integrates an H.323 v4 gatekeeper that provides the following functions:

- RAS (Registration Admission Status) server
- Testing the presence of remote H.323 gateways (ICMP or H.323 packets)

6.3.3.1.1 Multi-site configurations

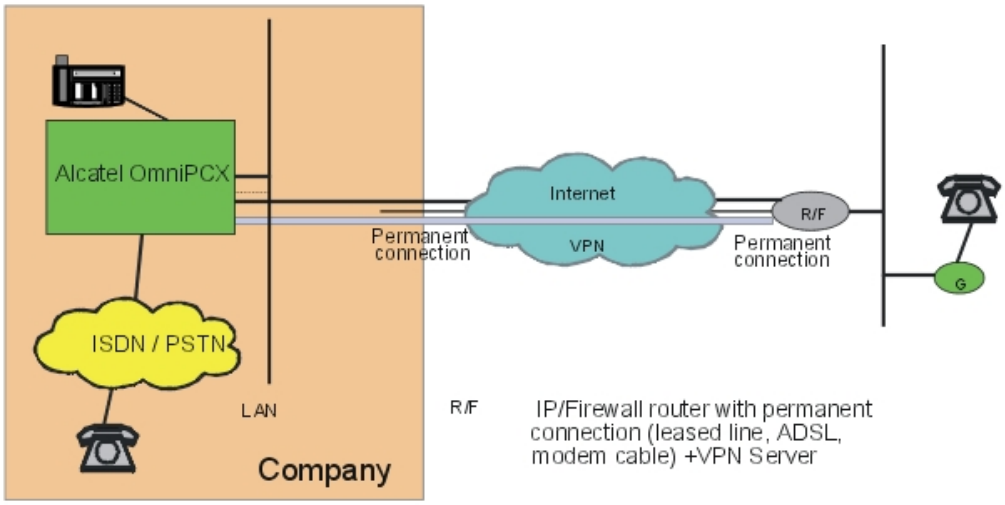
A multi-site configuration is possible via an extended Intranet or an Internet VPN.

6.3.3.1.2 *H.323 gateway integrated into an extended Intranet*



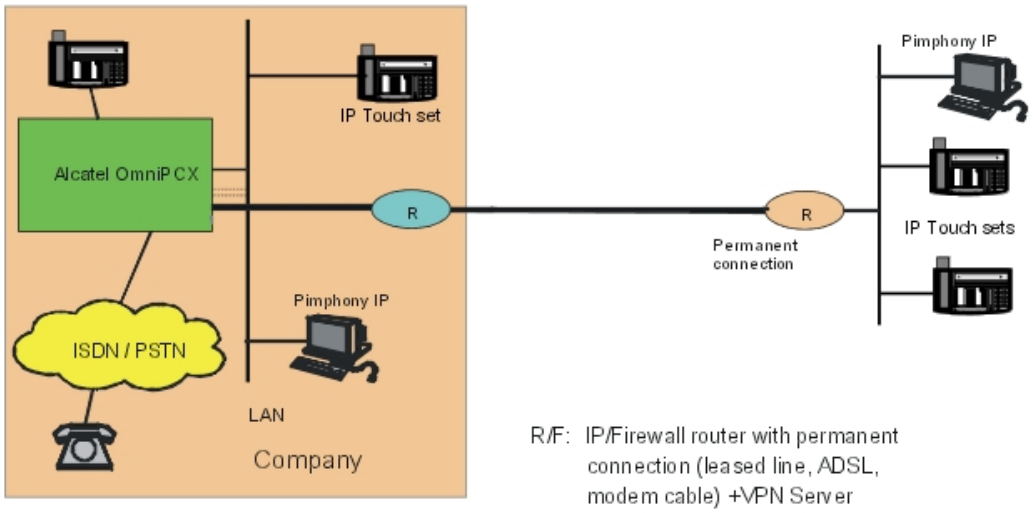
The IP router (R) connected to the Intranet can be a simple IP router. The reservation of bandwidth is "guaranteed" if this router supports Ipv4 ToS (DiffServ).

6.3.3.1.3 *H.323 gateway integrated into a VPN*



The IP router (R/F) at the front end of the VPN must offer Proxy/Firewall and VPN server functionality (IPSec with 3DES encryption for interoperability with the system's built-in router).

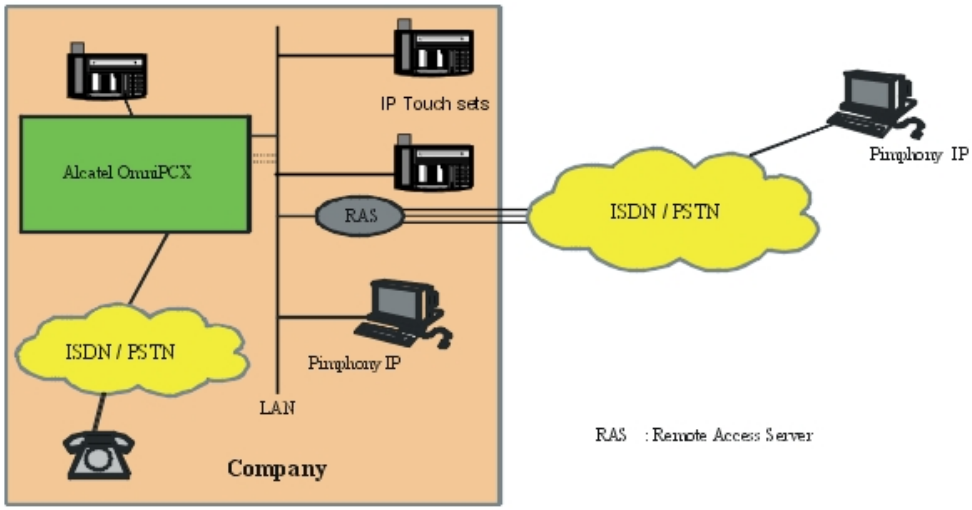
6.3.3.1.4 *IP telephony in an extended Intranet*



Note:

See also the Home Worker and Remote Worker topologies described earlier.

6.3.3.1.5 *PIMphony IP through RAS (Remote Access Server)*



The RAS is equipped with a pool of modems or a T0/T2. The RAS client PC is authenticated by a PAP/CHAP authentication procedure, then is called back by the RAS (callback).

6.3.3.1.6 *PC with Microsoft NetMeeting®*

A NetMeeting PC can connect to the company via the VPN (PPTP connection on Internet) or directly by a RAS connection via the telephone network (PSTN/ISDN).

6.3.4 Configuring H.323 Gateway

6.3.4.1 Hardware configuration

H.323 Gateway: This application layer forms the interface between the IP telephony (H.323 stack) and switched telephony worlds (Alcatel-Lucent OmniPCX Office Communication Server PBX call manager).

6.3.4.1.1 Configuring the system as the H.323 gateway

By default, after initialisation, all the DSPs are assigned to the pool of VoIP subscriber channels (IP telephony).

In a pure H.323 gateway configuration, all the DSPs of the system VoIP daughter boards will be used for "IP network" accesses.

By OMC (Expert View): **System -> Voice on IP -> VoIP: Parameters -> General** tab

Number of VoIP access channels (IP trunks): Number of channels for VoIP IP access, i.e. 1 DSP channel for 1 "network access".

Quality of IP service: Selection of the type of QoS used for the remote H.323 gateway VoIP calls.

If all the network equipment items support the IP ToS, one can choose an IP priority from 1 to 7.

If all the network equipment items are "DiffServ" compatible, one can choose from:

- DiffServ PHB Best Effort Forwarding (BE) (priority bits: 00000000)

- DiffServ PHB Expedited Forwarding (EF) (priority bits: 10111000)

Note:
Each DSP placed in the "VoIP access" pool is considered as a "network access" by the PBX, i.e. 1 VoIP DSP = 1 B-channel. As there can be a maximum of 6 VoIP daughter boards, each with 16 DSPs, there can be no more than 96 VoIP access DSPs, i.e. 96 "IP" B-channels.

Network accesses (T0, T2, analogue TL, DLT0, DLT2) + VoIP Accesses = 120 Max.

6.3.4.1.2 Configuring the gatekeeper (optional)

By OMC (Expert View): **System -> Voice on IP -> VoIP: Parameters -> Gatekeeper** tab

- **Integrated gatekeeper:** By default, the Gatekeeper is integrated into the PBX (box is selected); if not, fill in the Gatekeeper's identification
- **IP Address:** If the PBX is a gateway in an H.323 area, one must use an external gatekeeper that is the manager of the H.323 area it covers, indicating its IP Address provided by the network administrator
- **Reset Code:** Allows the resetting of a password on NetMeeting PCs that have a safety Plug-in

6.3.4.1.3 Configuring the Gateway timeouts (optional)

By OMC (Expert View): **System -> Voice on IP -> VoIP: Parameters -> Gateway** tab

NB: The parameters have standardized values, do not change them without prior analysis.

- **RAS Request Timeout:** Maximum authorised response time for a RAS request ("Registration, Admission, Status") made to the gatekeeper; between 10 and 180; default value = 20
- **Gateway Presence Timeout :** Determines the presence of a remote Gateway; value between 10 and 600; default value = 50
- **Connect Timeout:** Maximum authorised time interval between initialisation and connection; value between 10 and 1200; default value = 500
- **H.245 Request Timeout:** Maximum authorised response time for an H.245 request; value between 10 and 60; default value = 40
- **H323: End of dialling timeout**: Default value = 5

6.3.4.1.4 Configuration of T38 parameters for Fax over IP (optional)

By OMC (Expert View): **System -> Voice on IP -> VoIP: Parameters -> Fax** tab

- **UDP Redundancy:** Number of forwardings of Fax data packets; value between 0 and 2; default value = 1
- **Framing:** Number of data packets in the same frame; value between 0 and 5; default value = 0. In fact, the number of packets is equal to the number in this field + 1

Note:
***a**) Only T38 traffic is supported: modem, V90, V24, etc., are not available via H323/SIP connection. **b**) If the UDP redundancy is set to 0, any framing value (0 to 5) can be used. If the UDP redundancy is set to*

1, the framing value must not be higher than 1.

6.3.5 Configuring a Remote H.323 Gateway

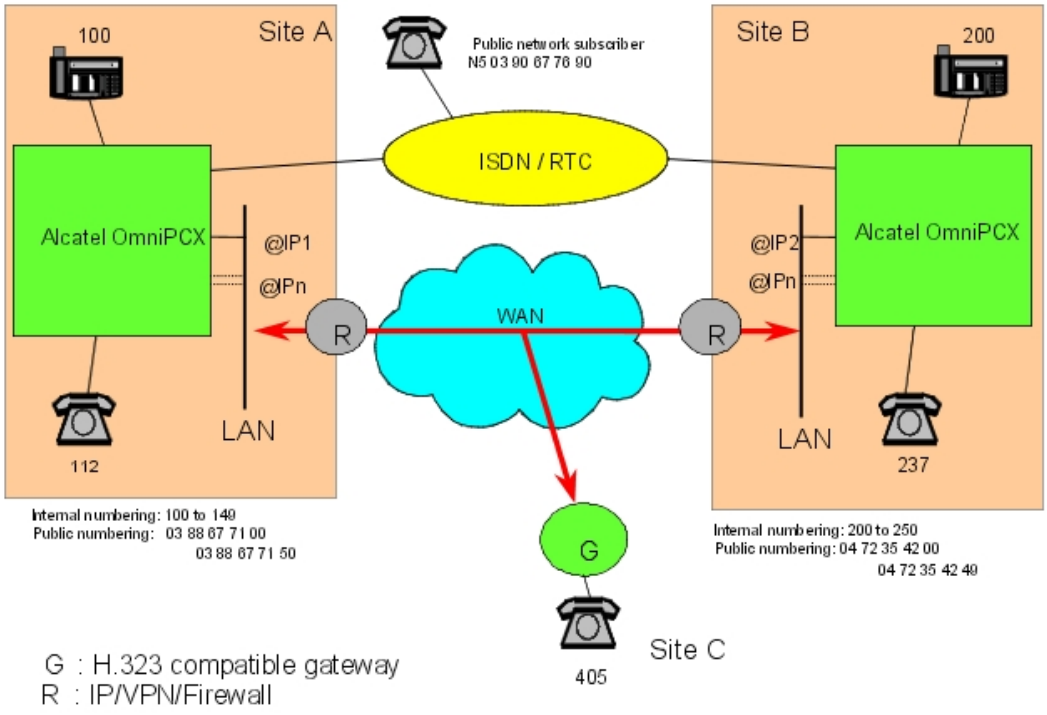
6.3.5.1 Configuration examples

6.3.5.1.1 Configuring outgoing communication (ARS table)

The choice of routing a telephone communication between a public network access or a VoIP access and the busy trunk overflow feature are defined in the ARS table.

Like conventional outgoing telephone calls, a VoIP call is subject to the ARS mechanisms: link categories, ARS time slot management, overflow on busy, etc.

In the diagram below sites A and B are Alcatel-Lucent OmniPCX Office Communication Servers. Site C is a remote system integrating an H.323 gateway.



- @IP1: IP address of the master VoIP CoCPU/CoCPU-1/CoCPU-2 board at site A
- @IP2 : IP address of the master VoIP CoCPU/CoCPU-1/CoCPU-2 board at site B. For example: 192.189.50.120
- @IPn: IP address of slave board(s)

6.3.5.1.2 Basic call

The site A stations call the site B stations by dialling their internal numbers:

Internal numbering plan (site A):

Function	Start	End	Base	NMT	Priv
Secondary trunk group	2	2	ARS	Keep	Yes

ARS Table:

Network	Access	Range	Substitute	List. Trunk group list	Called Party (ISVPN/H450)	Comment
Priv	2	00-49	2	4	Het	H.323 to site B

- The "Called(ISVPN/H450)" field has the value "Heterogeneous" by default. The notions of ISVPN do not apply to VoIP calls. This field is used for H450. If the remote is known to manage H450 transfer and/or forwarding services, this parameter can be set to "Homogenous"
- The "User Comment" field enables a comment to be associated with the ARS input (20 characters maximum)

Note 1:

The IP parameters in the ARS table are accessed by right-clicking and selecting "IP parameters".

Destination	IP Type	IP address	Hostname	Gateway Alive Protocol	Gateway Alive Timeout	Bandwidth	Gateway Alive Status
Gateway	Static	192.189.50.120	option	ICMP	300	128 Kbits (5 calls)	Enabled

- The "Destination" field of an ARS input to VoIP accesses must be of the "Gateway" type (H.323 gateway)
- For a "Gateway" destination, the "IP Type" must be a static IP address (non-modifiable field)
- The "IP Address" field must be that of the remote H.323 gateway. In the example, this value corresponds to the IP address of the master VoIP CoCPU/CoCPU-1/CoCPU-2 board at site B
- The "Host name" can be used instead of the IP address of the remote gateway's Gatekeeper. Requires a DNS server
- Gateway Alive Protocol / Gateway Alive Timeout:
  The integrated gateway tests the presence of the remote gateway every 300 seconds (Gateway Alive Timeout, from 0 to 3600 seconds). The test protocol (Gateway Alive Protocol) used by default is ICMP: the H.323 test protocol can only be used if the remote gateway is H.323 V4-compatible

Note 2:

Gateway Alive Timeout: If this field is at 0, the "Gateway Alive Protocol " mechanism is inhibited. This option is to be used in the specific situation where it is impossible to use ICMP or H.323 to test for the presence of the remote gateway; but in this case, there is no means whatsoever of knowing whether the remote gateway is alive or out of service.

- Gateway Bandwidth / QoS: For each ARS input to a remote H.323 gateway, a bandwidth must be reserved for the Voice over IP to the remote H.323 gateway. The number of simultaneous communications that can be held depends on this value:

Bandwidth	Number of simultaneous communications possible
None	No communication possible (Default value)
55.6 Kbps	1
64 Kbps	2
128 Kbps	5
256 Kbps	10
512 Kbps	20
= 1024 Kbps	> 20

For example, if the total bandwidth corresponding to the data rate to a remote gateway is 256 Kbps and the mean traffic level is 50%, it is wise to define a bandwidth of 128 Kbps for Voice over IP.

6.3.5.1.3 Remark concerning the quality of service (QoS)

If we take our example, site A can make H.323 calls to sites B and C. One assumes that the bandwidths reserved for Voice over IP at the LAN/WAN gateways of each site are:

- Bandwidth reserved for VoIP on site A: 1024 Kbps (20 calls or more)
- Bandwidth reserved for VoIP on site B: 128 Kbps (5 simultaneous calls)
- Bandwidth reserved for VoIP on site C: 64 Kbps (2 simultaneous calls)

In this configuration one sees that it is possible to make 7 simultaneous calls from site A to the remote H.323 gateways: 5 to site B and 2 to site C.

7 DSPs can therefore be assigned in the "VoIP access" pool for site A (7 being the number of DSPs needed to call sites B and C simultaneously).

However, let us assume that there is no ongoing communication between sites A and C, and that 5 calls are established between A and B. The total number of VoIP network access DSPs consumed in PBX A is 5: therefore 2 DSPs remain available to establish two other calls to site B.

Yet in this example we exceed the bandwidth reserved for Voice over IP at the LAN/WAN gateway of site B. The quality of service is no longer guaranteed.

To avoid downgrading the VoIP service, the system uses the "Gateway Bandwidth" field of the ARS table associated with the input to the remote H.323 gateway of site B, which will be configured at 128 Kbps (5 calls), as quality indicator (QoS). Although there are still 2 DSPs available, the PBX will refuse a 6th call to site B.

Note 1:

This service is not available if an external gatekeeper is used.

Note 2:

To optimise management of this ARS table parameter, it is vital to have information about the bandwidth available (reserved) for VoIP calls that is as precise as possible.

- Gateway Alive Status: this regularly updated read-only field indicates the status of the remote gateway:
  - Alive: Remote gateway present

- Deactivated: Remote gateway absent / out of service

It can, however, turn out to be judicious to deactivate the mechanism if one is sure of network reliability, in order to reduce the traffic.

6.3.5.1.4 Incoming call

An incoming "VoIP access" call is analysed in the private numbering plan. In our example:

Private numbering plan of site B:

Function	Start	End	Base	NMT	Priv
Local call	200	249	200		No

6.3.5.1.5 Forcing a public call to the H.323 gateway

LCR : Least Cost Routing

When a site A subscriber dials the public number of the site B station, the call can be forced to the VoIP network accesses:

Internal numbering plan of site A:

Function	Start	End	Base	NMT	Priv
Main trunk group	0	0	ARS	Drop	No

ARS Table:

Network	Access	Range	Substitute	List. Trunk group list	Called Party (ISVPN/H450)	Comment
Pub.	04723542	00-49	2	4	Het	H.323 to site B

6.3.5.1.6 Overflow

When a site A subscriber calls a site B station by its internal number, ARS routing enables the calls to be re-routed to the public network when it is no longer possible to call via the VoIP accesses. The following criteria render a "VoIP access" trunk group inaccessible:

- The VoIP CoCPU/CoCPU-1/CoCPU-2 board of site A is out of service
- No more DSPs associated with the VoIP accesses are available
- The remote H.323 gateway is out of service (VoIP CoCPU/CoCPU-1/CoCPU-2 board of site B is out of service).
- The quality of service (QoS) to the remote gateway is poor (exceeding of the possible simultaneous communication threshold for the bandwidth reserved for Voice over IP for this remote H.323 gateway)

ARS table of site A: Network

Calling the site B station by its internal number:

Network	Access	Range	Substitute	List. Trunk group list	Called Party (ISVPN/H450)	Comment	Destination
Priv	2	00-49	2	4	Het	H.323 to site B	Gateway

			04723542	1	Het	ISDN Access	No IP

Calling the site B station using its public number:

Network	Access	Range	Substitute	List. Trunk group list	Called Party (ISVPN/H450)	Comment	Destination	
Pub.	04723542	00-49	2 04723542	4 1	Het Het	H.323 to site B ISDN Access	Gateway No IP	
Pub.	04723542	50-99	04723542	1	Het	ISDN Access	No IP	*

* : As the public numbers 04723542 50 to 99 do not belong to site B, they must be routed to the public network.

6.3.5.1.7 Break In

The break-in service enables the PBX to re-route a public number from site A to site B. In our example, the public network subscriber dials the number 03 88 67 71 50 which is routed to station 250 on site B:

Public numbering plan (site A):

Function	Start	End	Base	NMT	Priv
Secondary trunk group	7150	7150	ARS	Keep	No

ARS Table:

Network	Access	Range	Substitute	List. Trunk group list	Called Party (ISVPN/H450)	Comment
Pub.	0388677150		250	4	Het	H.323 to site B

Reminder: It is vital for the PBX "Installation number" field to be configured; e.g. for site A: 388677100.

6.3.5.1.8 Break Out

The break-out service enables proximity calls to be made. In our example, a site A station dials a public number starting with 04, the call is routed to site B via the H.323 gateway, then routed to the public network from site B, configuration:

Internal numbering plan of site A:

Function	Start	End	Base	NMT	Priv
Main trunk group	0	0	ARS	Drop	No

ARS table of site A: Network

Network	Access	Range	Substitute	List. Trunk group list	Called Party (ISVPN/H450)	Comment	Destination	
Pub.	04		004	4	Het	H.323 to site B	Gateway	*
			04	1	Het	ISDN Access	No IP	**

* : As the prefix 0 is dropped in the internal numbering plan, 004 must be substituted for 04,

** : This sub-line allows overflow to the public network lines of site A if the VoIP access calls are inaccessible.

As an incoming VoIP access call is analysed in the private numbering plan, the following must be programmed in the private numbering plan of site B:

Function	Start	End	Base	NMT	Priv
Main trunk group	0	0	0	Drop	No

6.4 SIP

6.4.1 Overview

6.4.1.1 SIP Protocol

SIP (Session Initiation Protocol) is an IP signalling protocol designed to establish, to maintain and to end multimedia sessions between different parties. It operates on a client-server mode. It is based on the exchange of text messages with a syntax similar to that of *HyperText Transport Protocol* (HTTP) messages. Elements of the SIP world are identified by SIP *Uniform Resource Locators* (URLs) similar to e-mail addresses.

It is important to note that SIP does not provide an integrated communication system. SIP is only in charge of initiating a dialog between interlocutors and of negotiating communication parameters, in particular those concerning the media involved (audio, video). Media characteristics are described by the *Session Description Protocol* (SDP). SIP uses the other standard communication protocols on IP: for example, for voice channels on IP, Real-time Transport Protocol (RTP) and Real-time Transport Control Protocol (RTCP). In turn, RTP uses G7xx audio codecs for voice coding and compression.

Unlike H.323, the SIP protocol can rely on the IP network transport protocol in datagram mode *User Datagram Protocol* (UDP) in addition to the IP network transport protocol in *Transmission Control Protocol* (TCP) connected mode: see figure : H.323 and SIP in the OSI Model . UDP has the advantage of being an unconnected protocol that facilitates swift exchanges. It does not guarantee datagram reception and transmission sequence preservation. Thus, SIP carries out these functions, using retransmission, acknowledgement and sequencing mechanisms.

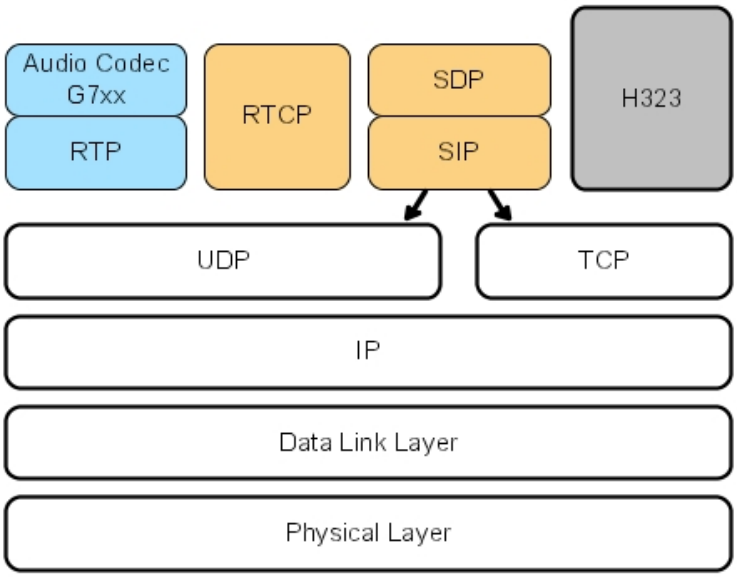


Figure 6.6 : H.323 and SIP in the OSI Model

SIP introduces the concept of user mobility. A call is made by entering the "logical" address of a user (as a URL). This address is used to identify the user, but not to detect his/her location.

To execute a conversion between the logical address and the actual location, an entity called a location server, which provides the user's actual address at the time of the call (URL of the device to be called), is consulted. The location server knows the addresses of the users because it has their registrations.

This operating mode also enables a user to receive his calls simultaneously on several terminals if the latter are registered with the same logical address.

6.4.1.2 Addressing

The SIP protocol uses URLs. They are constructed from:

- A number (to the left of the "@"), which can take on the form of standard numbers (canonical form), for example **+497118245000**
- A domain part (to the right of the "@") which can be an IP address, the name of a machine, or a *Fully Qualified Domain Name* (FQDN), i.e. the name of a domain.

Example:

sip:5000@192.168.5.10, ***sip:+497118245000@sip.mycompany.com***

6.4.1.3 Exchanging Messages

Like HTTP, SIP is constituted by transactions. A transaction is made up of a request sent by a client and of 0 to n responses to this request sent by a server. Unlike HTTP, a client (who transmits requests and waits for answers) can also be a server (which receives requests and sends back answers). All transactions are independent from each other. However, some can be used to set up a "dialog". Transactions within a dialog are linked. For example, a phone call is a dialog: in addition to calling, one must hold, or hang up.

The main types of requests (which initiate transactions) are:

- **INVITE**: message sent systematically by the client for any connection request. The **INVITE** message can also be used to update an established session. In this case, it is also called **Re-INVITE**.
- **ACK**: message sent by the client to end and to confirm the connection request.
- **BYE**: terminates a call, RTP packet exchange is stopped.
- **CANCEL**: terminates a call currently being set up.
- **REGISTER**: message sent by an agent to indicate his actual address. This information can be stored in the location server and is used for call routing.
- **OPTION**: message used to perform capability query (and keep-alive mechanism by the Alcatel-Lucent OmniPCX Office Communication Server).

Responses are characterized by a code which is an integer:

- **1xx**: informational (transaction in progress).
- **2xx**: success (transaction completed successfully).
- **3xx**: forward (the transaction is terminated and prompts the user to try again in other conditions).
- **4xx, 5xx, 6xx**: errors (the transaction is unsuccessfully terminated).

Certain transactions completed successfully establish a dialog within which other transactions can be exchanged (parameter negotiations, inter-interlocutor signalling data transport, etc.). Please note that the path followed by the initial transaction is not necessarily the one that other transactions within the dialog will follow. Indeed, the initial transaction will be sent to the interlocutor's logical address, and can pass through SIP entities in charge of finding his actual location. Once the final called party has been found and the initial transaction has established a dialog, the next transactions within the dialog are exchanged directly between interlocutors. Certain SIP entities through which the initial transaction is transmitted, can however remain in the signalling path. A specific transaction is used to terminate the dialog. In the case of a dialog initiated by an INVITE request, BYE terminates the dialog.

6.4.1.4 Message Formats

Requests and responses include two parts: A heading (mandatory) and, in certain cases, a second part called the *body*. The heading includes several fields called *headers*.

table 6.20 : Example of an INVITE Message:

```
INVITE sip:3481545074@172.25.41.10;user=phone SIP/2.0
Supported: 100rel
User-Agent: OxO GW
P-Asserted-Identity: sip:+0810021883@mycompany.com;user=phone
To: <sip:3481545074@mycompany.com;user=phone>
From: <sip:+0810021883@mycompany.com;user=phone
;tag=50ea3fbbbf41236cf7cc145b963a9140>
Contact: <sip:+0810021883@62.97.50.243;user=phone>
Content-Type: application/sdp
Call-ID: 78fa3caba1338e93dc50e8262f5ccd13@62.97.50.243
CSeq: 1453537030 INVITE Via: SIP/2.0/udp 62.97.50.243
;branch=z9hG4bKc43959f162a7bc2699f6f86425bf0899
Max-Forwards: 70
Content-Length: 215
** Body not Show **
```

For greater clarity, the body of the above message is not shown.

Some of these fields (or field parts) identify transactions and dialogs. Certain fields provide caller and called party data:

- Request-URI **sip:3481545074@172.25.41.10**: routable address of the destination
- **To: sip:3481545074@mycompany.com**: address of the final called party of the request. This is a logical address: it does not allow sending of the request directly; the location step is required to determine the actual address of the called party at the time of the call. SIP entities called proxies are in charge of transporting requests to the final location of the called party.
- **From: sip:+0810021883@mycompany.com**: address of initial request sender (logical address).

Certain fields indicate which path the next requests must follow within a dialog (Contact, Route, Record-Route fields). Unless requested by the SIP entities used during dialog initiation, the next requests are directly exchanged by terminal entities.

- **Contact: sip:+0810021883@62.97.50.243**: physical address of each interlocutor.

Other fields describe the format and the size of the message body (in this example, an SDP description). Finally, optional fields can be added, depending on selected transaction functions.

A SIP entity can send a message body containing an SDP description of the media it chooses to use (IP transport, compression algorithms). The remote entity responds with a SIP message containing an SDP description of the media selected in the initial offer. This negotiation phase can also take place again once the call is established.

6.4.1.5 Example of a Dialog

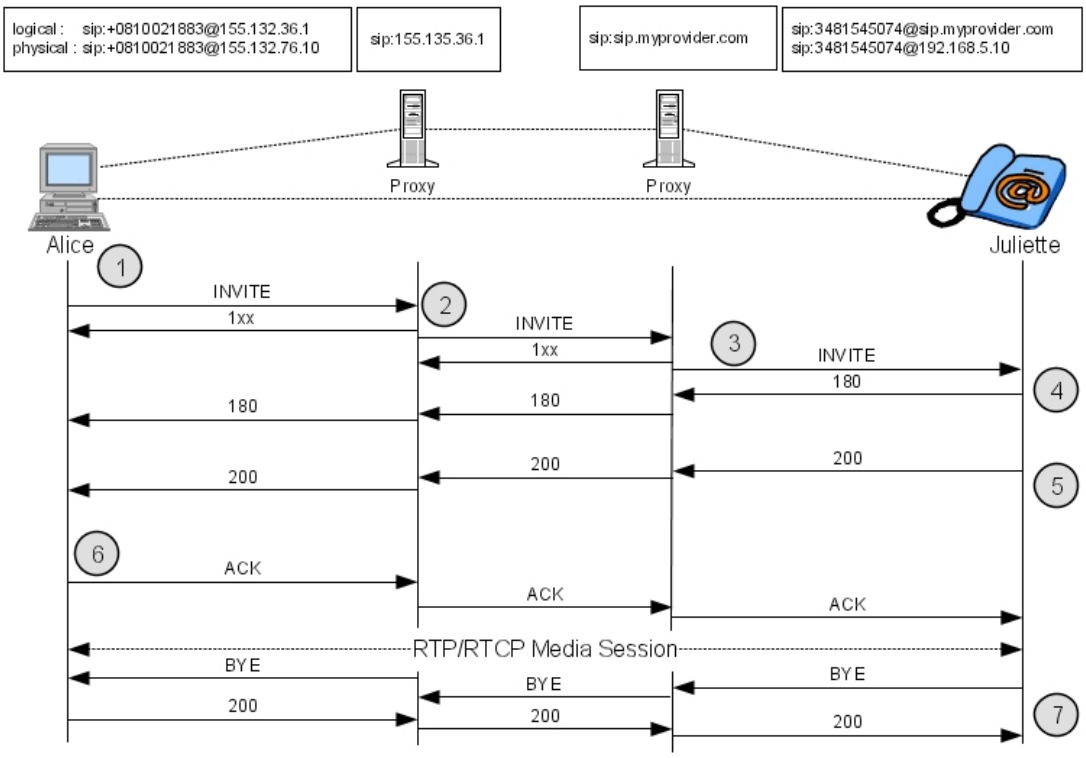


Figure 6.7 : Example of a dialog

The exchange shown in figure : Example of a dialog includes 2 *transactions*.

The first transaction begins with the *INVITE* request from Alice to Juliette and ends with a non 1xx response; in the example, the *OK* response from Juliette:

1. Alice sends an *INVITE* request to her proxy server for a call to Juliette. This request contains an SDP description of the media that Alice wishes to use,
2. The proxy server determines Juliette's proxy server address, for example by consulting a DNS server, transmits an *INVITE* request to this server and a *100 Trying* response to Alice,
3. The second proxy server transmits a *100 Trying* response to the first server and consults its location server to find Juliette's actual address. Once this address is identified, the *INVITE* request is sent to Juliette's SIP terminal,
4. Juliette is informed of the call when her terminal rings and a *180 Ringing* response is sent to Alice's terminal. This response contains, in the *Contact* field, Juliette's current address (where she can be contacted directly without transiting via the proxy server),
5. When Juliette off-hooks, a *200 OK* response is sent to Alice's terminal. This response ends the transaction. It can contain an SDP description of the media that Juliet wants to use in relation to Alice's suggestion,
6. The second transaction begins with Alice's acknowledgement *ACK*. The *ACK* request is transmitted to Juliette's URL, contained in the *200 OK* contact field.
   RTP/RTCP voice channels on IP are established between the two terminals, in compliance with the results of SDP negotiation,

7. Two messages (*BYE* and *200 OK*) end the dialog. RTP/RTCP channels are also released.

6.4.1.6 *Media Negotiation*

Media negotiation consists in an offer/answer dialog allowing to select the media that will be used for a communication between two user agents. The SDP protocol is used (defined in RFC 2327).

For a voice communication, media negotiation applies to the compression algorithm, to VAD, to the quantization law (A or µ law) and to the framing.

Media negotiation takes place at call setup. There are two cases:

- The offer is given by the calling user agent in the INVITE message. In this case, the called user agent gives an answer in the 200 OK message.

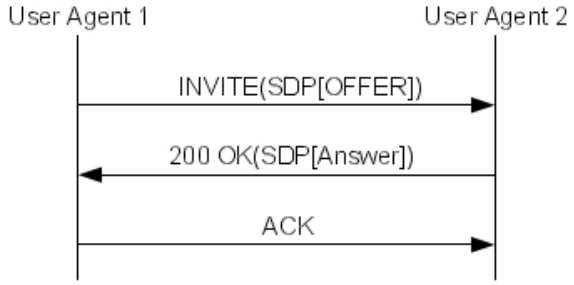


Figure 6.8 : Media Negotiation with an Offer in the INVITE Message

- The offer is not given by the calling user agent in the INVITE message. In this case, the called user agent makes an offer in the 200 OK message and the calling user agent makes an answer in the ACK message.

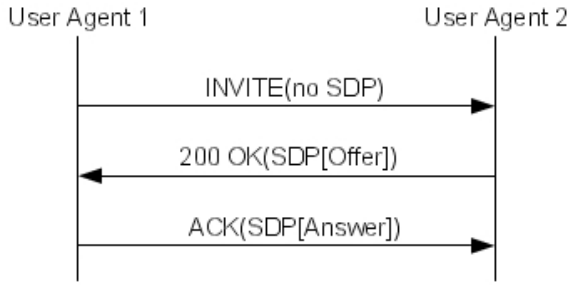


Figure 6.9 : Media Negotiation with no Offer in the INVITE Message

6.4.1.6.1 Offer Description for Voice Communications

table 6.21 : Example of Offer

```
v=0
o=default 1149510698 1149510698 IN IP4 62.97.50.243
s=-
c=IN IP4 62.97.50.243
t=0 0
m=audio 32082 RTP/AVP 0 8 106
a=sendrecv
a=ptime:30
a=maxptime:120
a=rtpmap:106 telephone-event/8000
a=fmtp:106 0-15
```

table 6.22 : Offer Description

v	Version of the offer
c	Address of the media gateway that will send and receive media flows
m	Media description - audio: media type - 32082: port number - RTP/AVP: transport type - 0 8 106: payload type proposed • 0: G711 µ law • 8: G711 A law • 106: dynamic payload (telephone-event)
a	Media description attributes: - sendrecv: the media is bidirectional (other value are: recvonly and sendonly) - ptime: framing - rtpmap: media associated to the specified payload - fmtp: parameters for the specified payload

6.4.1.6.2 Answer Description for Voice Communications

The answer is similar to the offer. It acknowledges the media given in the offer. In the example below, the chosen codec is G711 A law.

table 6.23 : Example of Answer

```
v=0
o=default 1149510698 1149510698 IN IP4 62.97.50.243
s=-
c=IN IP4 62.97.50.243
t=0 0
m=audio 32000 RTP/AVP 8 106
a=sendrecv
a=ptime:30
a=maxptime:120
a=rtpmap:106 telephone-event/8000
a=fmtp:106 0-15
```

table 6.24 : Answer Description

m	Media attributes: - audio: media type - 32000: port number - RTP/AVP: transport type - 8 106: payload type proposed • 8: G711 A law • 106: dynamic payload (telephone-event)

6.4.1.6.3 Offer Description for Fax Communications

The table below shows an example of offer for a fax communication.

table 6.25 : Example of Offer for a Fax Communication

```
v=0
o=default 1149510698 1149510698 IN IP4 62.97.50.243
s=-
c=IN IP4 62.97.50.243
t=0 0
m=image 32000 udptl t38
a=T38FaxVersion:0
a=T38MaxBitRate:14400
a=T38FaxRateManagement:transferredTCF
a=T38FaxMaxBuffer:72
a=T38FaxMaxDatagram:316
a=T38FaxUdpEC:t38UDPFEC
a=T38FaxUdpEC:t38UDPRedundancy
```

table 6.26 : Fax Offer Description

m	Media description - image: media type - 32000: port number - udptl: transport type: fax over UDP - t38: protocol used
a	Fax attributes

6.4.1.7 SIP Network Elements

6.4.1.7.1 Terminals

A SIP terminal may be either a SIP phone or a SIP application on a PC equipped with a microphone and loudspeakers (softphone).

In SIP terminology, terminals are sometimes referred to as *User Agents* (UAs).

6.4.1.7.2 Location Entities

Several logical functions are used to locate request recipients.

- **Registrar**

The registrar is in charge of collecting SIP set registration requests, and then of transmitting the data to the location server.
For a SIP user, the registration consists in sending a REGISTER request to the server. This request contains its actual address at a given time as well as the period of validity of this address.
A user can register under several addresses at the same time. In this case, the call will be routed to all his physical URLs (forking feature).

- **Location Server**
  The location server contains the database of "logical" URL - "physical" URL (current address to be actually called) relations. This database can be entered from terminal registrations, or using other means chosen by the manager.
  When a call is established, the INVITE request contains the logical URL of the recipient user. This URL cannot be used to route the call. On receiving the request, the proxy server consults the location server to identify the user's actual URL, then routes the request to this URL.
- **Proxy**
  The proxy is an intermediate entity that operates as a client or a server by transmitting requests for a User Agent.
  The main function of the proxy is routing. On receiving an INVITE request, it transmits the request either to the recipient set, or to another proxy, which is "closer" to the set.
- **Redirect Server**
  A *redirect server* is a *User Agent* that generates 3xx responses to the requests it receives, supplying the client with new addresses to contact.
  Unlike the proxy, the redirect server does not transmit requests.

6.4.1.7.3 Gateways

Gateways are used to ensure the SIP interface with other signalling protocols and with other voice transport protocols.

Gateways are identified as SIP User Agents. Alcatel-Lucent OmniPCX Office Communication Server is a User Agent.

6.4.1.7.4 DNS (Domain Name System)

The DNS is a directory system distributed on Internet.

The basic function of a DNS server is to convert domain names into IP addresses. This is done:

- Through a DNS A request to convert a name into an ipv4 IP address
- Through a DNS AAAA request to convert an name into an ipv6 IP address.

Any SIP entity can use the DNS if the domain part of a URL appears as a name, in order to convert it into an IP address.

For SIP, the DNS can also be used to resolve protocol type, address and the port number where requests relating to a given SIP address must be sent. This is done through NAPTR and DNS SRV requests.

6.4.1.7.5 NAPTR and DNS SRV

An answer to a NAPTR (Naming Authority Pointer) request for a given domain name consists of one or several NAPTR records. A NAPTR record contains the supported transport protocol (UDP, TCP, TLS over TCP, ...) and the replacement name to be used for DNS SRV requests.

The example below shows NAPTR records which could be obtained for a NAPTR request for the domain "mydomain.com".

Example:

```
      Order  pref  flags  service   regexp   replacement
IN NAPTR 50  50    "s"    "SIP+D2T" ""       _sip._tcp.mydomain.com
IN NAPTR 90  50    "s"    "SIP+D2U" ""       _sip._udp.mydomain.com
```

The records indicate that the server supports TCP and UDP in that order of preference. `Order` specifies the order in which the NAPTR records must be processed to ensure the correct ordering of rules. `Pref` specifies the order in which NAPTR records with equal `Order` values should be processed, low numbers being processed before high numbers.

Then, the system must make a TCP lookup to get SRV records for "_sip._tcp.mydomain.com". An SRV RR answer may be:

```
       Priority  Weight  Port  Target
IN SRV 0         1       5060  server1.mydomain.com
IN SRV 0         2       5060  server2.mydomain.com
```

The records indicate that the system should send its request to server1. If there is no answer, server2 should be used. Note that the domain name "mydomain" can change between NAPTR records and SRV records.

Once the protocol, the port and the domain have been resolved, the system should determine the IP address of the server. The system performs DNS A query (or AAAA for IPV6) related to "server1.mydomain.com" to get a list of IP addresses.

The system should try the first SRV RR record. If no answer, the next in the list should be queried until the end of the list.

If no SRV records were found, the system has to perform DNS A query (or AAAA for IPV6) on the domain name.

If a port is specified in the URI (example : 1234@mydomain.com:5060), then the system has to perform a DNS A query (or AAAA for IPV6) for this domain.

6.4.2 Public SIP Trunking

6.4.2.1 Overview

The following chapters describe the Alcatel-Lucent OmniPCX Office Communication Server connection to a public provider through SIP trunking.

Public SIP trunking allows connection to a SIP provider with a level of service similar to ISDN. This includes for example ISDN services such as CLIP/CLIR or fax transport.

The following chapters detail:

- Typical network topologies
- The main features of public SIP trunking
- The public SIP trunking configuration procedure

6.4.2.2 Topologies

6.4.2.2.1 Overview

The following section describes several topologies for public SIP trunking.

The described topologies differ in the way the customer private IP network (including the Alcatel-Lucent OmniPCX Office Communication Server and other telephony IP devices) is connected to the provider network. This can be through:

- A Multi Protocol Label Switching (MPLS) based IP-VPN network
- The Internet
- A managed IP network

6.4.2.2.2 Deployment Constraints

The type of connection between the customer IP network and the provider network has an impact on:

- **NAT (Network Address Translation)**

  NAT is necessary to translate private IP addresses into public IP addresses. Typically, a router performs level 3 NAT. This means that only IP addresses of IP Packets headers are translated. SIP requires level 5 NAT so that IP addresses in SIP messages are also translated. Alcatel-Lucent OmniPCX Office Communication Server does not perform level 5 NAT. According to the network topology, level 5 NAT is performed by the provider Session Border Controller (SBC) or must be performed by the customer border element.

- **Outbound proxy**

  The outbound proxy is the first SIP aware equipment reached by outgoing SIP messages. According to the network topology, the provider SBC or the customer border element must operate as outbound proxy.

- **DNS server location**

  According to the network topology, the DNS server for service and port resolution must be either in the private network or in the public network.

6.4.2.2.3 SIP Trunking through an MPLS Network

In this configuration, the customer network is connected to the SIP provider through an MPLS (Multi Protocol Label Switching) based IP-VPN network.

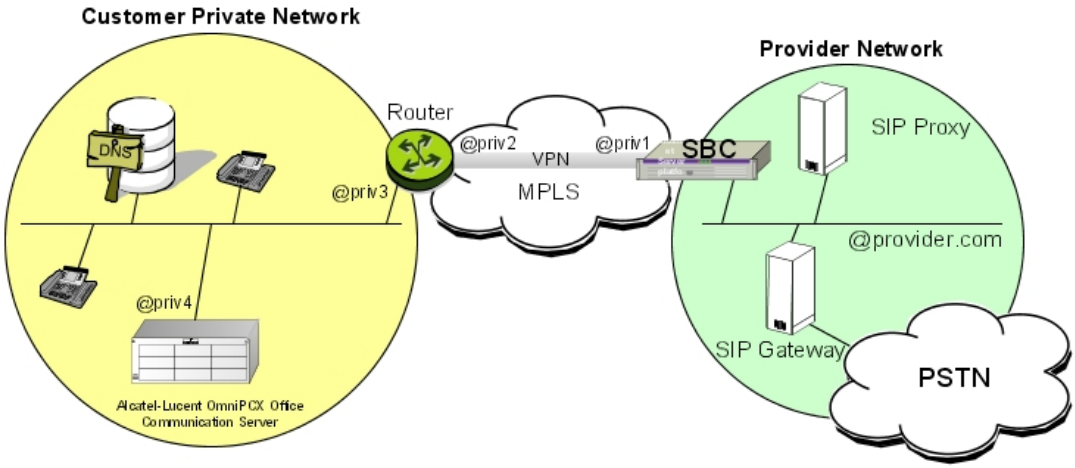


Figure 6.10 : SIP Trunking on an MPLS Network

The SIP provider Session Border Controller (SBC) has a private IP address in the customer network. This topology requires no equipment performing level 5 NAT in the customer network.

The SIP SBC operates as an outbound proxy for Alcatel-Lucent OmniPCX Office Communication Server.

If DNS SRV is used, DNS resolution consists in resolving the service/name of the SBC. DNS servers must belong to the private addressing plan.

6.4.2.2.4 SIP Trunking through the Internet

In this configuration, the customer network is connected to the SIP provider through the Internet.

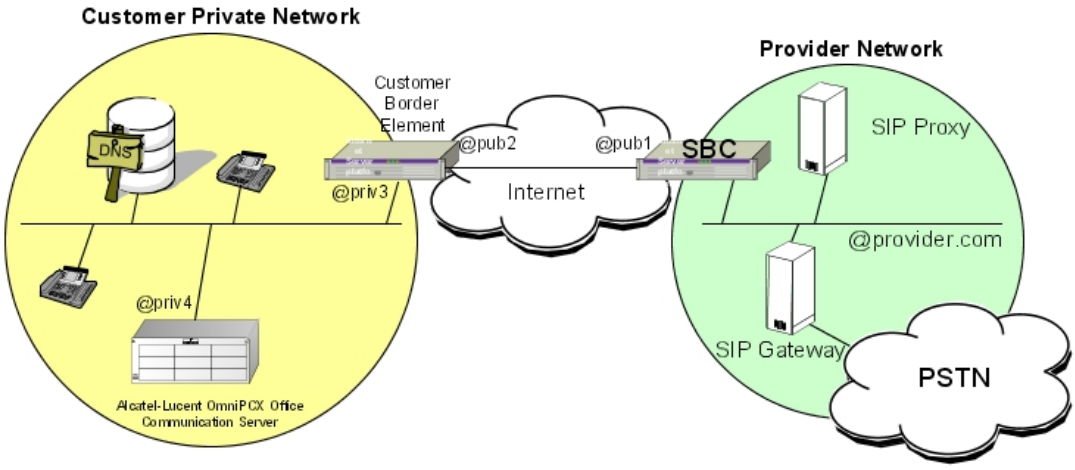


Figure 6.11 : SIP Trunking on the Internet

The SIP provider SBC has a public address (and no private address in the customer network). This topology requires a customer border element performing level 5 NAT.

The customer border element operates as outbound proxy for Alcatel-Lucent OmniPCX Office Communication Server.

If DNS SRV is used, DNS resolution consists in resolving the service/name of the customer border element. DNS servers must belong to customer network.

6.4.2.2.5 SIP Trunking in a Managed IP Network

In this configuration, the customer network is connected to the SIP provider through a trusted managed IP network.

In this case, there are two possibilities:

- A customer border element is a SIP aware equipment: it performs level 5 NAT and operates as outbound proxy. The configuration is then equivalent to the topology described: § SIP Trunking through the Internet .

- The piece of equipment on customer premises is a simple router/firewall performing level 3 and 4 NAT.
  - The provider SBC processes SIP signalling and level 5 NAT.
  - The provider SBC operates as an outbound proxy.
  - If DNS SRV is used, DNS resolution consists in resolving the service/name of the provider SBC. DNS servers belong to the public numbering plan.

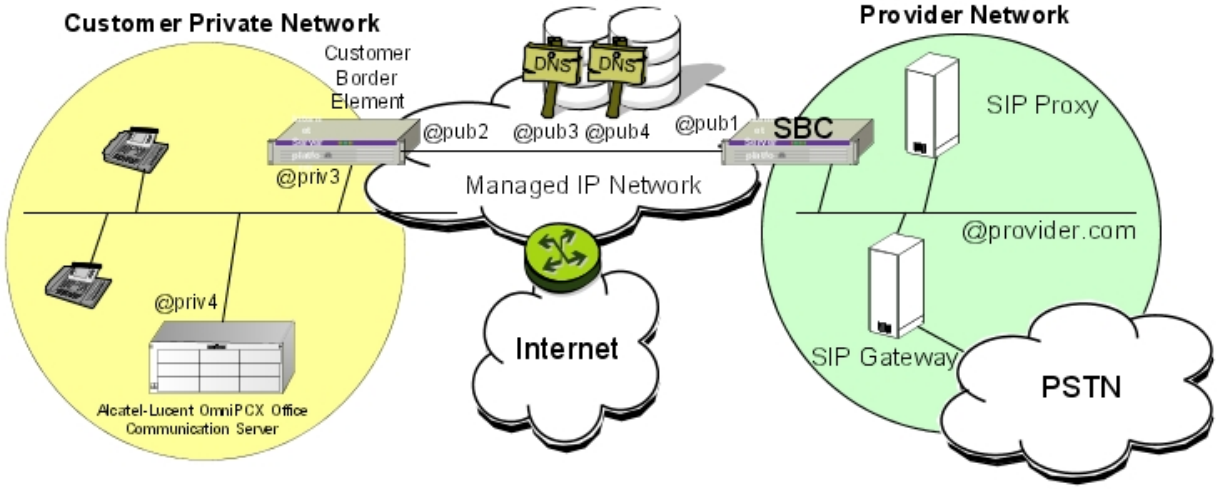


Figure 6.12 : SIP Trunking in a Managed IP Network

6.4.2.3 Feature Description

6.4.2.3.1 SIP Trunking Features in a Public Networking Context

The table below contains the features available on public SIP trunking.

table 6.27 : Available Features on Public SIP Trunking

Feature	Public Networking through a SIP proxy
Direct end-to-end call	Not applicable
Call through a SIP proxy	Yes
Basic incoming/outgoing voice call	Yes
Block dialling	Yes
CLIP, CNIP	Yes[3]
CLIR, CNIR	Yes [3]
COLP, COLR	Yes [3]
Private/public call differentiation	Yes
DTMF transport	Yes[4]
T38/UDP fax Call	Yes[5]

Feature	Public Networking through a SIP proxy
Call Forwarding (CFR, CFB) with signalling path optimization	No
Call Forwarding (CFR, CFB) by joining the two calls (with or without audio path optimization)	Yes
Call Transfer with signalling path optimization	No
Transfer (consultation, ringing) by joining the two calls (with or without audio path optimization)	Yes
Authentication for incoming calls	No
Authentication for outgoing calls	Yes
Registration (with/without authentication)	Yes
Least cost routing	Yes
Bandwidth limitation on peer-to-peer basis	Yes
Automatic overflow on lack of bandwidth towards a given destination	Yes
VoIP route disabling for some subscribers	Yes
DDI	Yes
Break-in	Yes, if numbering plans are compliant
Break-out	Yes, if numbering plans are compliant
RTP proxy between a SIP trunk and an IP phone	Yes
RTP proxy between two joined SIP trunks	Yes
QoS tickets	Yes
Direct RTP between a SIP trunk and an IP phone	Yes
Direct RTP between two joined SIP trunks	Yes

6.4.2.3.2 Standards

The table below shows the standards used for feature implementation.

table 6.28 : Standards Used for Feature implementation

Feature	Standard Used
Basic Call	RFC 3261, 3264, 2327, 3966

[3] Provided both SIP stacks are RFC 3323, 3324, 3325 compliant and Alcatel-Lucent OmniPCX Office Communication Server is a trusted element

[4] DTMF transport is transparent to the proxy. The SIP end-element must be RFC 2833 compliant.

[5] Fax transport is performed by SIP end-elements and is transparent to the proxy.

Feature	Standard Used
Early Media	RFC 3960, 3262
Media	RFC 3550, 3551
Third Party Call Control	RFC 3725
DNS SRV	RFC 3263, 2782, 1034
Numbering Format	RFC 3261
CLIP	RFC 3323, 3324, 3325
CLIR	RFC 3325, 3261
COLP	RFC 3323, 3324, 3325
Causes (reject and release)	RFC 4497
Authentication of the Alcatel-Lucent OmniPCX Office Communication Server SIP gateway	RFC 3261
Authentication for outgoing calls	RFC 2617, 1321
Forward	RFC 3261
Hold	RFC 3261
Transfer	RFC 3261
Fax	T38 Annex D
DTMF	RFC 2833
Symmetric Response Routing	RFC 3581

6.4.2.3.3 Outbound Proxy

In the case of public SIP trunking, SIP messages are not sent directly to the SIP gateway but are first sent to an outbound proxy, which is in charge of routing SIP messages.

According to the network topology, the outbound proxy can be:

- The provider Session Border Controller (SBC)
- The Customer Border Element

For more information, see: module Public SIP Trunking - Topologies .

6.4.2.3.4 DNS SRV

Up to R6.0, the gateway, outbound proxy and registrar IP addresses and port numbers must be provided statically in **Automatic Routing** and **VoIP Parameters**. If there are several proxies (for example a primary and a secondary proxy), the overflow must be configured through ARS.

As of R6.1, DNS SRV enables a resolution of service/name.

For an INVITE message, the service/name to resolve is the very next SIP equipment, that is the outbound proxy.

For example, if the To header of the INVITE message is sip:1234@provider.com, the service/name to resolve is _sip._udp.provider.com.

A DNS SRV answer may contain several records ordered by priority. Each record contains a proxy name. If a proxy is unavailable, requests are sent to the second proxy and so on. There

is no need to configure the overflow through ARS.

DNS SRV can also be used for registration. The service/name to resolve is the registrar name.

Note 1:
Alcatel-Lucent OmniPCX Office Communication Server does not perform the DNS A request alone. A DNS A request is always performed following a DNS SRV request.

The figure : Process for Locating a SIP Server describes the process followed to locate a SIP server starting from a given URI.

Note 2:
Since only UDP transport protocol is supported, Alcatel-Lucent OmniPCX Office Communication Server does not perform NAPTR requests. For example, if "domain.com" is the domain name to resolve, a DNS SRV request for "_sip._udp_domain.com" is sent.

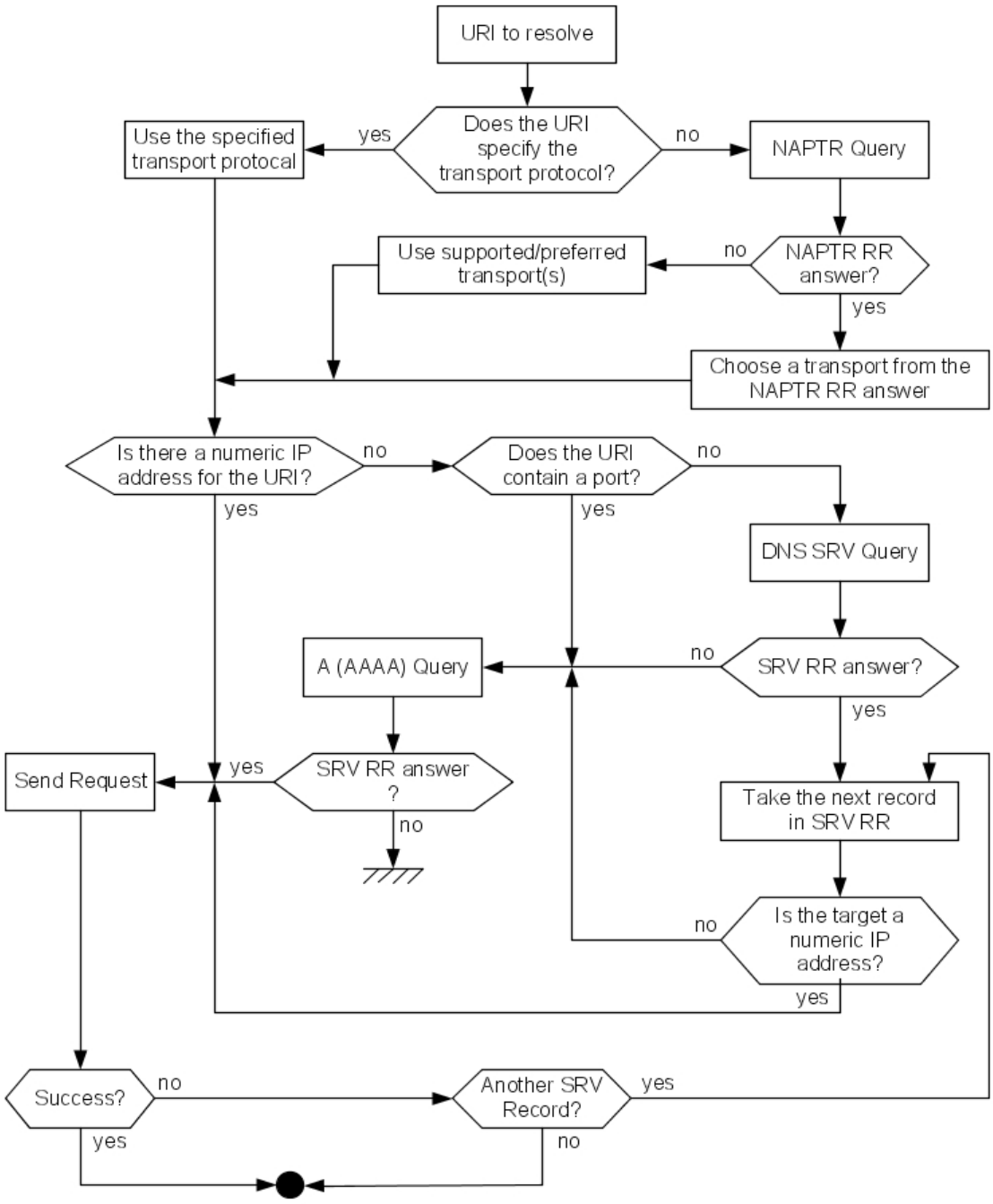


Figure 6.13 : Process for Locating a SIP Server

DNS Cache

To speed up call set up and also to limit exchanges on the IP network, Alcatel-Lucent OmniPCX Office Communication Server holds a cache containing DNS RR (SRV and A) records.

When a service/name to be resolved is present in the cache, the record stored in cache is used and no DNS request is sent.

A record is saved during the Time To Live (TTL) received in the DNS answer. When the TTL timer expires for a record, the record is removed from the cache and a subsequent request for the corresponding service/name results in a DNS request.

If the TTL received in the DNS answer is equal to 0, the corresponding record is not saved in the cache.

figure : Example of Dialogue shows an example of dialogue: INVITE 789@prov, sent after TTL expiration, resulting in a DNS SRV request.

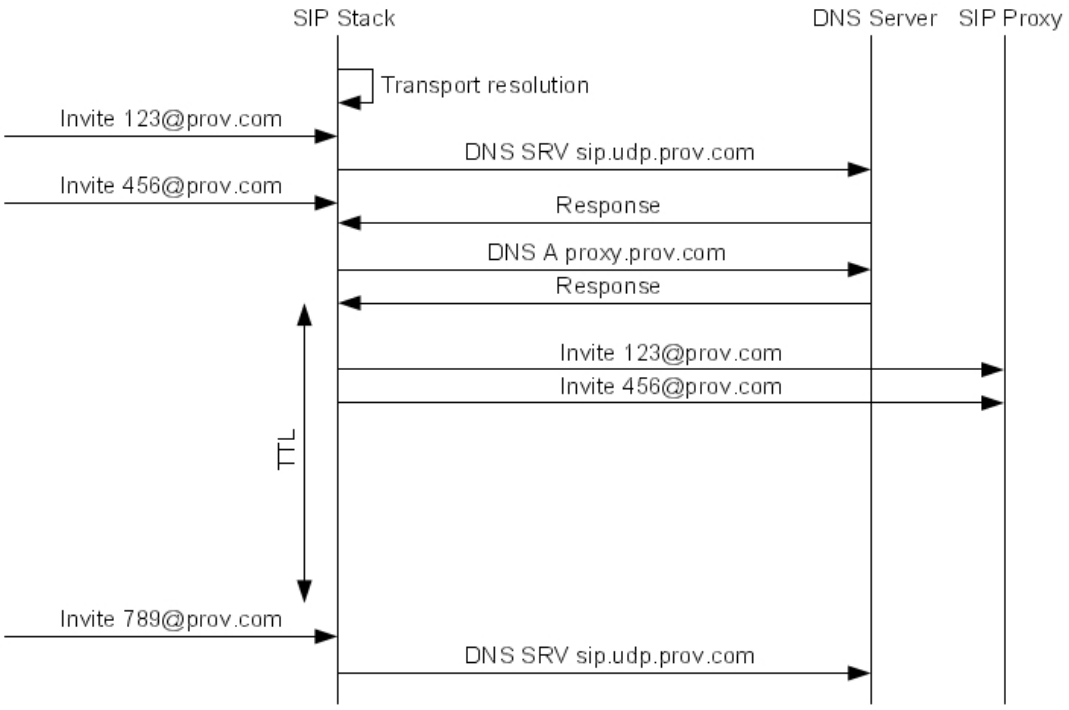


Figure 6.14 : Example of Dialogue

Unavailable Proxy List

To avoid sending useless requests to unreachable proxies, Alcatel-Lucent OmniPCX Office Communication Server can hold a list of unavailable proxies.

An unavailable proxy IP address is stored in the list during a configurable timer. The unavailable proxy list mechanism can be inhibited by setting this timer to 0.

The administrator can consult and reset the unavailable proxy list through **webdiag**.

A proxy IP address is put in the unavailable proxy list when:

- A proxy does not answer an INVITE message before Timer B expiration.
- An ICMP Destination Unreachable message is received.

Timer B = $2^{\text{Number of Retries}}$ * Timer T1

By default, **Number of Retries** = 6, Timer B = 64 * T1

A proxy IP address is removed from the unavailable proxy list when:

- The **Unreachable Proxy List Timer** expires
- All the proxies corresponding to a given SRV request are in the unavailable proxy list: in this case, all the proxies corresponding to this SRV request are removed from the list and messages can be sent again to these proxies after a timer.
- The administrator resets the list through **webdiag**.

To configure the **Unreachable Proxy List Timer**:

1. In OMC (Expert View), select **System** > **Voice over IP**> **VoIP: Parameters** > **SIP** tab
2. Review/modify the following attribute:

Unreachable Proxy List Timer	Enter the time (in minutes) after which an unavailable proxy IP address is automatically removed from the unavailable proxy list. Enter 0 to inhibit the unavailable proxy list mechanism. Default value: 10 Max value: 1440 (1 day)

6.4.2.3.5 Registration

Registration is used for mapping between a Uniform Resource Identifier (URI) and a contact for a user.

The Alcatel-Lucent OmniPCX Office Communication Server can perform registration. There is only one registration for the whole system. There is no registration for each system user. A URI corresponding to a unique system identifier is registered. This unique system identifier must be configured as requested by the provider: it can be for example the installation number.

Registration is necessary if the Alcatel-Lucent OmniPCX Office Communication Server IP address is not statically provisioned in the provider location data base.

The registration URI is: `sip:unique_installation_id@provider_domain`

Example:

`sip:+497114567110@domain.com;user=phone` *where is* `+497114567110` *the installation number.*

The contact header of the registration request is:

`sip:unique_installation_id@IPPPX_IP_address`

Registration is performed at Alcatel-Lucent OmniPCX Office Communication Server startup and then periodically. The **Expiration Time** parameter defines the registration periodicity. The default value is 3600 seconds.

The registrar IP address can be defined statically or can be resolved by DNS SRV.

If requested by the registrar, the Alcatel-Lucent OmniPCX Office Communication Server can authenticate itself. Authentication parameters are sent in a new REGISTER message.

Registration and authentication parameters (**Username**, **Shared Secret** and **Registered Realm**) are configured in OMC (Expert View), in **System** > **Voice over IP**> **VoIP: Parameters** > **SIP** tab.

6.4.2.3.6 Keep Alive Mechanism

The keep alive mechanism is used to check the remote gateway status.

The Alcatel-Lucent OmniPCX Office Communication Server supports two keep-alive mechanisms : ICMP message (ping) and the SIP Option method.

By default, the Alcatel-Lucent OmniPCX Office Communication Server uses ICMP message (ping). A message is sent every 300 s.

Note:

The keep-alive mechanism is inhibited when DNS SRV is enabled.

To configure the keep alive mechanism:

1. In OMC (Expert View), select **Numbering** > **Automatic Routing Selection** > **Automatic Routing: Prefixes**
2. Review/modify the following attributes:

Gateway Alive Protocol	Select **ICMP** or **SIP Option**
Gateway Alive Timeout/s	Enter the periodicity (in seconds) of keep alive message emission. Enter 0 to inhibit the keep alive mechanism.

6.4.2.3.7 Authentication

Incoming Calls

There is no authentication for incoming calls.

Incoming calls are accepted:

- When DNS SRV is not enabled, if the remote gateway IP address matches one **IP Address** in the **Automatic Routing: Prefixes**.
- When DNS SRV is enabled, if the domain part of the From field of the INVITE message matches a **Domain Name** in the **Gateway Parameters**.

Outgoing Calls

If requested by the provider, outgoing calls can authenticate themselves.

The Alcatel-Lucent OmniPCX Office Communication Server supports the Digest authentication scheme (MD5).

Authentication parameters (**Login**, **Password** and **Realm**) are defined in the **Gateway Parameters**.

6.4.2.3.8 Safety

A mechanism based on a quarantine list is used to protect the Alcatel-Lucent OmniPCX Office Communication Server from DOS (Denial Of Service) type attacks.

IP addresses in the quarantine list are the IP addresses whose messages are ignored for the duration of the **Quarantine Time**.

An IP address is automatically placed in the quarantine list when the number of messages received by the Alcatel-Lucent OmniPCX Office Communication Server from this address has reached a configurable maximum threshold (**Message Peak Number**) during a configurable amount of time (**Period Peak Detection**).

To configure quarantine parameters:

1. In OMC (Expert View), select **System** > **Voice over IP** > **VoIP: Parameters** > **SIP** tab
2. Review/modify the following parameters:

Message Peak Number	Enter a integer between 10 and 250. Default value: 90
Period Peak Detection	Enter the detection period in seconds between 1 and 60. Default value: 3
Quarantine Time	Enter the quarantine time in seconds between 1 and 600. Default value: 360

6.4.2.3.9 Numbering Formats

By default, all numbers transmitted by the Alcatel-Lucent OmniPCX Office Communication Server in SIP messages are in the E.164 canonical form, i.e. `+CCnational_number`, where CC is the country code.

International numbers have the advantage of being totally unambiguous whatever the type of call.

Some providers do not use numbers in canonical form.

- The Alcatel-Lucent OmniPCX Office Communication Server can be configured to send calling and called numbers for outgoing calls in the format required by the provider
- The Alcatel-Lucent OmniPCX Office Communication Server can be configured to interpret calling and called numbers for incoming calls received in non-canonical forms

The paragraph below presents the **SIP Public Numbering** configuration for outgoing calls and incoming calls.

The examples shown use the following installation numbers.

table 6.32 : Installation Numbers used in the following examples

Installation Number	4567
International Prefix	00
International Code	49
Intercity Prefix	0
Intercity Code	711
Recall Prefix	0

Outgoing Calls

Calling Number Format

The calling number format for outgoing calls applies to:

- The user part of the FROM and P-asserted-identity headers of outgoing INVITE requests.
- The alerted number in a 180 Ringing
- The connected number in a 200 OK
- The divert number in an INVITE

Two parameters are used to configure the calling number format: **Calling Format (Outgoing)** and **Calling Prefix (Outgoing)**.

Note:
The typical calling number is a concatenation of installation (system) number and DDI set (extension) number. The alternative CLIP/COLP number is used to send a specific CLIP/COLP number instead of the typical CLIP/COLP number, as explained: § Alternative CLIP/COLP Numbers .

The table below shows examples of numbers constructed for the different values of the **Calling Format (Outgoing)** parameter.

table 6.33 : User Part of the From Header according to the **Calling Format (Outgoing)** Value

Calling Format (Outgoing)	Calling Prefix (Outgoing) = "+"	No Calling Prefix (Outgoing)
Canonical (default value)	+497114567110	497114567110
International	+00497114567110	00497114567110
National	+07114567110	07114567110
National without intercity prefix	+7114567110	7114567110
Regional	+4567110	4567110

Alternative CLIP/COLP Numbers

There are several types of alternative numbers:

- Alternative system CLIP number
- Alternative user CLIP/COLP number
- Alternative access CLIP/COLP number

For more information on alternative numbers, see: module Alternative CLIP and COLP Numbers - Overview .

The format type of an alternative number (international, national, ...) can be deduced by comparing the leading digits of that number to the international or national prefixes configured in the installation numbers table. The CLIP/COLP number finally passed within the SIP protocol is the alternative number that has been formatted according to the **ARS Calling Format (Outgoing)** and ARS **Calling Prefix (Outgoing)** parameters.

The table below shows examples of numbers in different cases. In this example, the **Calling Prefix (Outgoing)** is set to **+**. "NOK" means that the configuration is not valid.

table 6.34 : Example of CLIP/COLP Numbers in SIP Messages According to Alternative Numbers and ARS **Calling Format (Outgoing)**

Alternative Number Configured	Format Type Deduced	ARS Calling Format (Outgoing)	ID Number Sent in the SIP Message
0033390671234	International	**Canonical**	+33390671234
		International	0033390671234
		National	**0033390671234 NOK**
		Regional	**33390671234 NOK**
0390671234	National	**Canonical**	+49390671234
		International	0049390671234
		National	0390671234
		Regional	**390671234 NOK**
1234	Other	**Canonical**	+497111234
		International	00497111234
		National	07111234
		Regional	1234

Called Number Format

The called number format for outgoing calls applies to the user part of the Request-URI and the To header of INVITE messages.

Two parameters are used to configure the called number format for outgoing calls: **Called Format (Outgoing)** and **Called Prefix (Outgoing)**.

The table below shows numbers constructed for different dialled number and the different possible values of **Called Format (Outgoing)**. In the example, the **Called Prefix (Outgoing)** is empty.

table 6.35 : Called Number in the To Header According to the **Called Format (Outgoing)** Value

Number dialled:	Called Format (Outgoing) Value				
	Canonical	**International**	**National / International**	**National without intercity prefix**	**Undefined**
3699 (number in the same region)	497113699	00497113699	07113699	7113699	3699
7111234 (number in the same region)	497117111234	004971171112340	7117111234	7117111234	7111234

Number dialled:	Called Format (Outgoing) Value				
	Canonical	International	National / International	National without intercity prefix	Undefined
07111234 (national number in the same region)	497111234	00497111234	07111234	7111234	07111234
06541234 (national number)	496541234	00496541234	06541234	6541234	06541234
0033123456789 (international number)	33123456789	0033123456789	0033123456789	33123456789	0033123456789

Incoming Calls

The format of calling and called numbers for incoming calls can be configured.

The calling (or called) format selected has an impact on the way a received number is interpreted and transformed. The principle is as follows:

- If a received number begins with the **International Prefix** or the **Intercity Prefix** (national prefix), the **Calling Format (Incoming)** (or **Called Format (Incoming)**) is not used
- If a received number does not begin with the international prefix or the national prefix, the number is considered to be of the configured **Calling Format (Incoming)** (or **Called Format (Incoming)**) type.

Calling Number Format

The calling number format for incoming calls concerns the FROM and P-asserted-identity headers.

Two parameters are used to configure the calling number format for incoming calls: **Calling Format (Incoming)** and **Calling Prefix (Incoming)**.

The **Calling Prefix (Incoming)** is used to distinguish private from public calling numbers:

- If the calling number begins with the **Calling Prefix (Incoming)**, it is considered to be public
- If the calling number does not begin with the **Calling Prefix (Incoming)**, it is considered to be private

If the **Calling Prefix (Incoming)** is empty, all calling numbers are considered public.

The calling format selected has an impact on the way a received number is transformed for storage and display on the called set.

- If a received number begins with the international prefix or the national prefix, the **Calling Format (Incoming)** is not used
- If a received number does not begin with the **International Prefix** or the **Intercity Prefix** (national prefix), the number is considered to be of the configured **Calling Format (Incoming)** type. An inconsistency between a received number and the configured **Calling**

Format (Incoming) will result in a wrong interpretation of the number type and a wrong displayed number on the called set.

The table below shows examples of transformation of numbers according to the **Calling Format (Incoming)** selected. "NOK" means that the number is misinterpreted.

table 6.36 : Calling Number Displayed According to the Configuration Choice

Format	Number received in the From header	Calling Format (Incoming) selected			
		Canonical / International	National	Regional	Unknown
Canonical with/without leading prefix	(+)33123456789 (other country)	0033123456789	**033123456789 NOK**	**33123456789 NOK**	**33123456789 NOK**
	(+)497654321 (own country, other region)	07654321	**0497654321 NOK**	**497654321 NOK**	**497654321 NOK**
	(+)497119876 (own country and region)	9876	**0497119876 NOK**	**0497119876 NOK**	**0497119876 NOK**
International with international prefix	0033123456789 (other country)	0033123456789	0033123456789	0033123456789	0033123456789
	00497654321 (own country, other region)	07654321	07654321	07654321	**00497654321 NOK**
	00497119876 (own country and region)	9876	9876	9876	**00497119876 NOK**
National with prefix	07654321 (own country, other region)	07654321	07654321	07654321	07654321
	07119876 (own country and region)	9876	9876	9876	**07119876 NOK**
National without prefix	7654321 (own country, other region)	**007654321 NOK**	07654321	**7654321 NOK**	**7654321 NOK**
	7119876 (own country and region)	**007119876 NOK**	9876	**7119876 NOK**	**7119876 NOK**
Other	987654321	**00987654321 NOK**	**0987654321 NOK**	987654321	987654321

The table below shows the compatibility between called numbers that are likely to be received and the configured **Called Format (Incoming)**.

Example:

If the calling numbers sent by the provider in the From header can be in international with prefix, national

*with prefix or national without prefix formats, the **Called Format (Incoming)** parameter must be set to **National**.*

table 6.37 : Compatibilities Between Format of Number Received in From Header and **Called Format (Incoming)** Value

Called Format (Incoming)	Format or Number in the From Header				
	Canonical or international with/without prefix	**international with prefix**	**National with prefix**	**National without prefix**	**Else**
Canonical / International	OK	OK	OK	NOK	NOK
National	NOK	OK	OK	OK	NOK
Regional	NOK	OK	OK	NOK	OK
DDI	NOK	NOK	NOK	NOK	OK

Called Number Format

The called number format for incoming calls concerns the To header.

Two parameters are used to configure the calling number format for incoming calls: **Called Format (Incoming)** and **Called Prefix (Incoming)**.

The **Called Prefix (Incoming)** is used to distinguish private from public called numbers:

- If the called number begins with the **Called Prefix (Incoming)**, it is considered to be public
- If the called number does not begin with the **Called Prefix (Incoming)**, it is considered to be private

If the **Called Prefix (Incoming)** is empty, all called numbers are considered to be public.

The called format selected has an impact on the way a received number is interpreted and sent to the public numbering plan. If the transformed number does not match any entry in the public numbering plan, the call fails. The principle is as follows:

- If a received number begins with the international prefix or the national prefix, the **Called Format (Incoming)** is not used
- If a received number does not begin with the **International Prefix** or the **Intercity Prefix** (national prefix), the number is considered to be of the configured **Called Format (Incoming)** type. An inconsistency between received number and the configured **Called Format (Incoming)** will result in a wrong interpretation of the number type and a wrong number sent to the public numbering plan.

The table below shows the numbers sent to the public numbering plan according to the number received and the called format configured. NOK means that the number is misinterpreted and that the call fails.

Number received in the From header	Called Format (Incoming)			
	Canonical / International	**National**	**Regional**	**DDI**
(+)49 7114567110	110	NOK	NOK	110
(+)00 49 7114567110	110	110	110	110

Number received in the From header	Called Format (Incoming)			
	Canonical / International	National	Regional	DDI
(+)0 7114567110	110	110	110	110
(+)7114567110	NOK	110	NOK	110
(+)4567110	NOK	NOK	110	110
(+)110	NOK	NOK	NOK	110

6.4.2.3.10 CLIP/CLIR

CLIP/CLIR for Outgoing Calls

CLIP for Outgoing Calls

CLIP is provided in both the From and P-asserted-Identity headers of the INVITE method.

Example:

```
From: "John" <sip:+497114567110@localdomain;user=phone>
P-Asserted-Identity : "John Lennon"
<sip:+497114567110@localdomain;user=phone>
```

CLIR for Outgoing Calls

By default, RFC 3325 is used. If secret identity is required for an outgoing SIP call, the FROM header of the INVITE message takes a particular syntax with anonymous values and the two headers "P_Asserted_Identity" and "Privacy" are added, as shown in the example below.

Example 1:

```
From: <sip:anonymous@anonymous.invalid>
P-Asserted-Identity : "John" <sip:+497114567110@localdomain;user=phone>
Privacy : user,id
```

If the provider does not take the P-Asserted-Identity header into account, the **RFC 3325** parameter of the **Gateway Parameters** must be set to **No**. If secret identity is required for an outgoing SIP call, the calling party identity is provided in the From header and a Privacy header is added, as indicated in the example below.

Example 2:

```
From: "John" <sip:+497114567110@localdomain;user=phone>
Privacy : user,id
```

CLIP/CLIR for Incoming Calls

CLIP for Incoming Calls

The calling party number is retrieved from the user part of the SIP URL of:

- The P-Asserted-Identity header, if present in the INVITE message
- The From header if there is no P-Asserted-Identity header

The corresponding calling name is used for SIP name display.

CLIR for Incoming Calls

CLIR applies to an incoming call if the Privacy header is present in the INVITE method, whatever its value ("id", "user" or "header"). This means that the Privacy header applies,

- To the P-Asserted-Identity header, if present in the INVITE message
- To the From header, if there is no P-Asserted-Identity header

6.4.2.3.11 COLP/COLR

COLP/COLR for Outgoing Calls

COLP for Outgoing Calls

COLP is retrieved from the user part of the SIP URL of:

- the P-Asserted-Identity header, if present in the 200.OK response or 180 Ringing message
- the Contact header, if there is no P-Asserted-Identity header

COLR for Outgoing Calls

COLR applies if the Privacy header is present in the 200.OK answer or the 180 Ringing message, whatever its value ("id", "user" or "header"). This means that the Privacy header applies to the P-Asserted-Identity header, if present, or to the Contact header.

COLP/COLR for Incoming Calls

COLP for Incoming Calls

COLP is provided in the Contact and P-Asserted-Identity headers of the 200.OK and 180.Ringing messages.

Example:

```
Contact : "John" <sip:+497114567110@localdomain;user=phone>
P-Asserted-Identity : "John" <sip:+497114567110@localdomain;user=phone>
```

COLR for Incoming Calls

If COLR is required for an incoming call, the Privacy header value is set to "id".

Example:

```
Contact : "John" <sip:+497114567110@localdomain;user=phone>
P-Asserted-Identity : "John" <sip:+497114567110@localdomain;user=phone>
Privacy : user,id
```

6.4.2.3.12 DTMF

The Alcatel-Lucent OmniPCX Office Communication Server DTMF transmission mode complies with RFC 2833. Payload is negotiated with the provider.

Note:
The Alcatel-Lucent OmniPCX Office Communication Server does not support the in-band and INFO

method DTMF transmission modes.

DTMF for Outgoing Calls

A dynamic payload X (106 by default) is proposed in the SDP part of the INVITE message.

Example:

```
m=audio 32082 RTP/AVP 0 8 106
```

The Alcatel-Lucent OmniPCX Office Communication Server behaviour depends on the contents of the SDP part of the 200.OK response:

- Payload X: use of RFC 2833 with payload X for emission and reception
- Payload Y: use of RFC 2833 with payload Y for DTMF emission and payload X for DTMF reception
- None: no DTMF

By default, the dynamic payload X proposed by Alcatel-Lucent OmniPCX Office Communication Server is 106. A noteworthy address is used to modify this value.

1. In OMC (Expert View), select **System** > **System Miscellaneous** > **Memory Read/Write** > **Other Labels**
2. Select **DtmfDynPL**:

DtmfDynPL	Enter the dynamic payload value in hexadecimal format. For example enter 78 for a decimal value of 120. Default value: 6A (106 dec)

DTMF for Incoming Calls

DTMF transmission depends on the contents of the SDP part of the INVITE method:

- Payload Y: agreement on payload Y in the 200.OK response, use of payload Y
- None: No payload in the 200.OK response, no DTMF

6.4.2.3.13 IP QoS

The Alcatel-Lucent OmniPCX Office Communication Server provides TOS/Diffserv tagging.

The Alcatel-Lucent OmniPCX Office Communication Server does not provide different tagging for signalling and media flows.

6.4.2.3.14 Codec/Framing Negotiation

The Alcatel-Lucent OmniPCX Office Communication Server supports the following codecs: G729A, G723.1, G711 A law, G711 µ law.

The Alcatel-Lucent OmniPCX Office Communication Server supports the following framings: 10, 20, 30, 40, 50, 60, 90, 120 ms, depending on the codec used.

The codec and framing used for a communication are the result of a negotiation between the Alcatel-Lucent OmniPCX Office Communication Server and the remote party.

The Alcatel-Lucent OmniPCX Office Communication Server behaviour depends on the **Codec/Framing** value in the **Automatic Routing: Prefixes** parameters

In a default configuration (**Codec/Framing** set to **default**), there is no preferred codec/framing on the Alcatel-Lucent OmniPCX Office Communication Server side. The selected

codec/framing depends on the remote party.

If the **Codec/Framing** parameter is set to a specific value, Alcatel-Lucent OmniPCX Office Communication Server uses only this configured value. If this codec/framing is not supported by the remote party, the call fails.

Note:

Noteworthy addresses can be used for specific behaviour. For more information, see module Public SIP Trunking - Configuration procedure § Appendix: Noteworthy Addresses for Codec/Framing Negotiation .

Outgoing Calls

Codec/Framing set to **default**

1. The Alcatel-Lucent OmniPCX Office Communication Server sends the list of all supported codec/framing in the SDP part of the INVITE message.
2. The called party answers with one codec/framing in the SDP part of the 200.OK response
3. The Alcatel-Lucent OmniPCX Office Communication Server acknowledges this response

Codec/Framing Set to a Specific Value

1. The Alcatel-Lucent OmniPCX Office Communication Server sends the configured codec/framing (e.g. G723_30) in the SDP part of the INVITE message.
2. The called party either accepts or rejects the call.

Incoming Calls

Codec/Framing Set to **default**

First Case

1. The caller sends a list of codec/framing in the SDP part of the INVITE message.
2. The Alcatel-Lucent OmniPCX Office Communication Server select the first supported codec/framing in the list.

Second Case

1. The caller sends a specific codec/framing in the SDP part of the INVITE message.
2. If the proposed codec/framing is supported by Alcatel-Lucent OmniPCX Office Communication Server, the call is accepted. Otherwise, the call is rejected.

Codec/Framing Set to a Specific Value

First Case

1. The caller sends a list of codec/framing in the SDP part of the INVITE message.
2. If the codec/framing configured for Alcatel-Lucent OmniPCX Office Communication Server is in the list proposed by the caller, the call is accepted. Otherwise, the call is rejected.

Second Case

1. The caller sends a specific codec/framing in the SDP part of the INVITE message.
2. If the proposed codec/framing matches the codec/framing configured for Alcatel-Lucent OmniPCX Office Communication Server, the call is accepted. Otherwise, the call is rejected.

6.4.2.3.15 Fax

T38 Annex D is supported.

G711 transparent fax is not supported.

6.4.2.3.16 Supplementary Services

Hold

A remote party can put on hold a local user through a public SIP trunk group by:

- Sending a Re-INVITE with an IP address set to 0.0.0.0 or media attribute set to "sendonly".

  The local music on hold is played by the Alcatel-Lucent OmniPCX Office Communication Server to the user put on hold.

- Sending a Re-INVITE with a valid IP address.

  The remote party plays its own music on hold. Hold is transparent to the Alcatel-Lucent OmniPCX Office Communication Server.

A local user can put on hold a remote party through a public SIP trunk group. The local music on hold is played by the Alcatel-Lucent OmniPCX Office Communication Server to the remote party put on hold. A Re-INVITE is transmitted with a valid media IP address.

Call Forwarding

Call forwarding is performed by joining the two calls.

Call forwarding with signalling path optimization is not supported.

Media optimization can be performed through the RTP direct mechanism.

The 3xx message is not used:

- The Alcatel-Lucent OmniPCX Office Communication Server does not send a 3xx message.
- The provider must not send a 3xx message. Such a message is rejected with a 503.Service Unavailable message.

Transfer

Transfer is performed by joining the two calls. The Re-INVITE method is used.

Transfer with signalling path optimization is not supported.

Media optimization can be performed through the RTP direct mechanism.

RFC 3515, 3891 and 3892 are not supported on public SIP Trunking.

- The Alcatel-Lucent OmniPCX Office Communication Server does not use the REFER method
- The provider must not send REFER message nor an INVITE message including a Replaces field.

Other Services

Other services requiring a renegotiation of media, such as conference or recording a conversation, are performed by using the Re-INVITE method.

6.4.2.3.17 Symmetric Response Routing

As of R7.0, the Alcatel-Lucent OmniPCX Office Communication Server complies with the RFC 3581 extension to the Session Initiation Protocol (SIP), for symmetric response routing. The

goal is to facilitate interworking with NATs.

Client behaviour: when UDP transport is used, the Alcatel-Lucent OmniPCX Office Communication Server includes the `report` parameter in the top `Via` header, to indicate that the RFC 3581 extension is supported and requested for the associated transaction. The Alcatel-Lucent OmniPCX Office Communication Server is ready to receive responses either to the request's source port, or to the 5060 port.

Server behaviour: the Alcatel-Lucent OmniPCX Office Communication Server examines the topmost `Via` header field. If it finds an `report` parameter, when building the response, it populates the `report` parameter with the source port of the request and adds a `received` parameter with the source IP address of the request. Then, it sends the response back to the `received`/ `report` address (in other words to the source address of the received request), from the same address and port where the request was received.

6.4.2.4 Configuration procedure

6.4.2.4.1 Pre-Requisites

The following must be declared:

- **Installation Numbers**: no SIP specificity
- DDI number range in the **Public Dialling Plan**: no SIP specificity

6.4.2.4.2 Checking Noteworthy Addresses

1. In OMC (Expert View), select **System** > **System Miscellaneous** > **Memory Read/Write** > **Other Labels**
2. Check the **VipPuNuA** value is **00**
3. Check the **ExtNuFoVoi** value is **22**

   Note:
   *The default value of the **ExtNuFoVoi** address is country dependent. Its function and value are the same as **ExtNumForm** for ISDN.*

6.4.2.4.3 Enabling SIP as VoIP Protocol and Setting the Number of VoIP Trunk Channels

By default, H.323 is the VoIP protocol enabled on the Alcatel-Lucent OmniPCX Office Communication Server and the number of DSP channels reserved for VoIP (H.323 or SIP) is equal to 0.

VoIP protocol must be switched to SIP and the number of channels for VoIP trunks must be increased to a non-null value.

1. In OMC (Expert View), select the **System** > **Voice over IP** > **VoIP: Parameters** > **General** tab
2. Review/modify the following attributes:

Number of VoIP-Trunk Channels	Enter the number of channels used for SIP trunking.
VoIP Protocol	Select **SIP**

3. Confirm your entries
4. If the **VoIP Protocol** has been switched from **H323** to **SIP**, you are requested to reset the

VoIP boards

6.4.2.4.4 Configuring the VoIP Trunks and Trunk Group

Configuring VoIP Trunks as Public

The VoIP trunks must be configured as public trunks.

1. In OMC (Expert View), select **System** > **External Lines** > **List of Accesses** > **Details**
2. Check the **Public trunk** box

Creating the VoIP Trunk Group

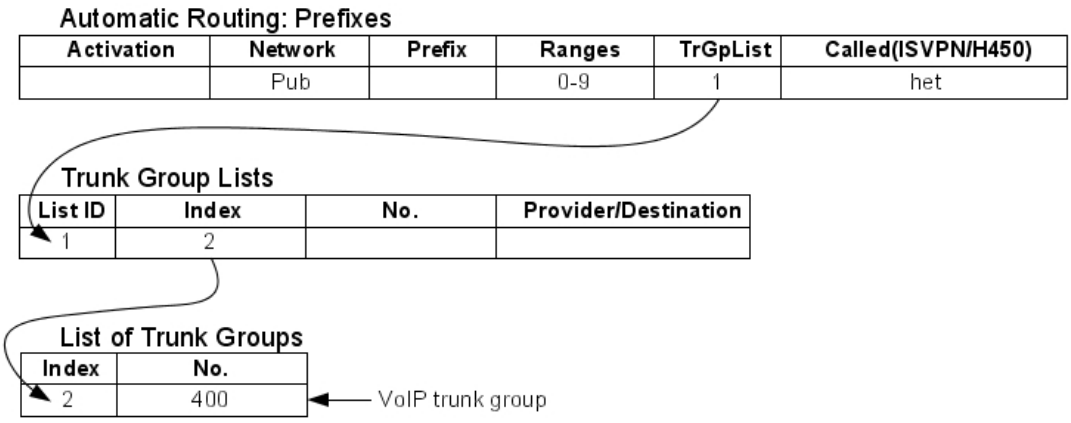
1. In OMC (Expert View), select **System** > **External Lines** > **List of Trunk Groups**
2. Create a trunk group containing the VoIP trunks
3. If necessary, modify the **Link Category** value (**Traffic Sharing**)
4. If necessary, modify the Traffic sharing & barring matrix

Creating a List Index for the VoIP Trunk Group

1. In OMC (Expert View), select **System** > **Numbering** > **Automatic Routing Selection** > **Trunk Group Lists**
2. Create a list index for the VoIP trunk group

Creating the ARS Route

An ARS route must be created to route all numbers to the VoIP trunk group list. The figure below shows the relationship between objects.



1. In OMC (Expert View), select **System** > **Numbering** > **Automatic Routing Selection** > **Automatic Routing: Prefixes**
2. Add a line that routes everything to the VoIP trunk group

Activation	**Yes**
Network	**pub**

Prefix	Leave blank
Ranges	0-9
Substitute	Leave blank
TrGpList	Enter the trunk group list index
Called(ISVPN/H450)	**het**

Configuring ARS Optional Parameters

If the VoIP trunks are configured as public (see § Configuring VoIP Trunks as Public), the **Calling** and **Called/PP** parameters of a public **Automatic Routing: Prefixes** can be left at their default values.

On an installation combining both public and private SIP trunk groups, if the VoIP trunks are configured as public, the **Calling** and **Called/PP** parameters of the private **Automatic Routing: Prefix** must be set to **Priv**:

1. In OMC (Expert View), select **System** > **Numbering** > **Automatic Routing Selection** > **Automatic Routing: Prefixes**
2. Right-click the line and select **Opt. Parameters**
3. Review/modify the following parameters:

Calling	Select **Priv**
Called/PP	Select **Priv**

Creating an ARS Prefix

1. In OMC (Expert View), select **System** > **Numbering** > **Dialling Plans** > **Internal Dialling Plan** tab
2. Create or modify the **Main Trunk Group** prefix

Feature	**Main Trunk Group**
Start	0
End	0
Base	**ARS**
NMT	**Drop**
Priv	**No**

3. Confirm your entries

6.4.2.4.5 Configuring The Gateway and IP Parameters

Configuring ARS IP Parameters with DNS SRV Disabled

The figure : ARS Configuration with DNS SRV disabled describes the main parameters to configure, and their relationship, when DNS SRV is disabled.

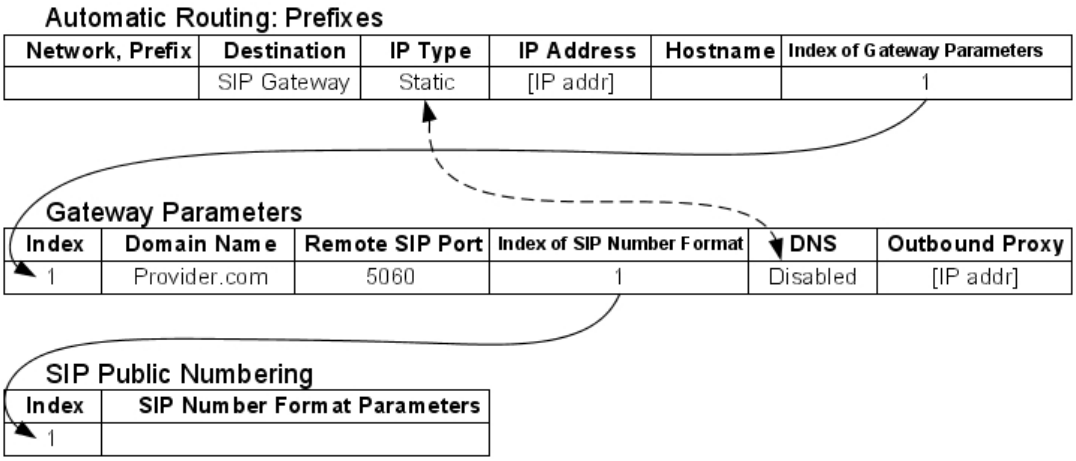


Figure 6.16 : ARS Configuration with DNS SRV disabled

Configuring the Route IP Parameters

1. In OMC (Expert View), select **System** > **Numbering** > **Automatic Routing Selection** > **Automatic Routing: Prefixes**
2. Right-click the line and select **IP Parameters**

Destination	**SIP Gateway**
IP Type	**Static**
IP Address	Enter the IP address of the outbound proxy. *Note 1:* *This IP address is used to identify the origin of in-coming calls.* *Note 2:* *This field can be left empty if the **Hostname** is filled.*
Hostname	This field is optional and can be entered as an alternative to the IP address of the remote SIP gateway. *Note 3:* *The hostname must be locally DNS solved (in OMC and PC's DNS parameters).*
Gateway Alive Protocol	Select **ICMP** or **SIP Option**.
Gateway Alive Timeout/s	Enter the timeout between 20 and 3600 s.
Gateway Bandwidth	Select the bandwidth available towards the remote gateway. The number of simultaneous communications towards the gateway depends on this value.

Codec/Framing	• **Default**: the codec/framing chosen depends on the remote party. • Other values: Alcatel-Lucent OmniPCX Office Communication Server uses only this codec/framing.
Index of Gateway Parameters	Enter the gateway index.

Configuring the **Gateway Parameters**

1. In OMC (Expert View), select **System** > **Numbering** > **Automatic Routing Selection** > **Gateway Parameters**
2. Review/modify the following parameters:

Index	Enter an index between 1 and 200.
Domain Name	Enter the domain name of the provider. *Note:* *This parameter is used to fill the domain part of the To header of an INVITE message.*
Remote SIP Port	Enter the number of the UDP port used to send SIP messages.
Index of SIP Numbers Format	1
DNS	**Disabled**
Primary DNS Server	Leave blank.
Secondary DNS Server	Leave blank.
Outbound Proxy	Enter the IP address of the outbound proxy.

Configuring ARS IP Parameters with DNS SRV Enabled

The figure : ARS Configuration with DNS SRV enabled describes the main parameters to configure, and their relationship, when DNS SRV is enabled.

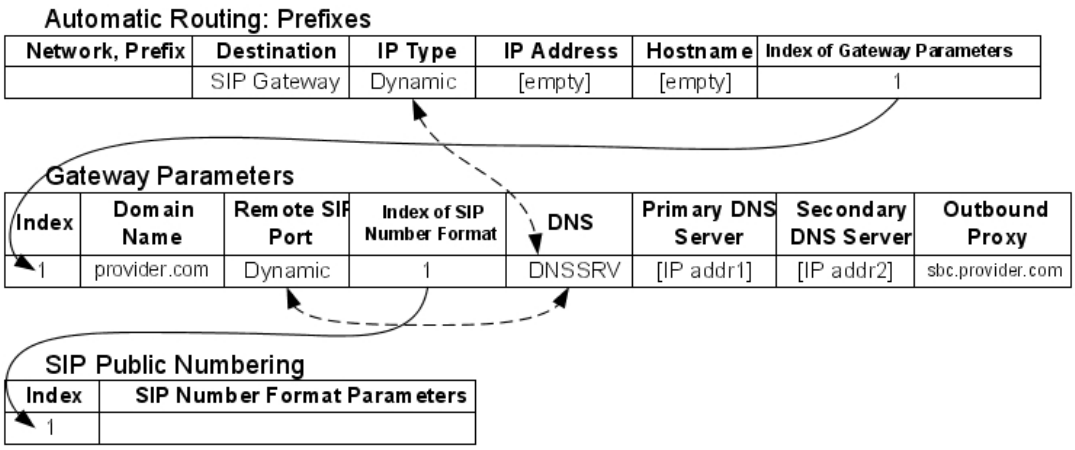


Figure 6.17 : ARS Configuration with DNS SRV enabled

Configuring the Route IP Parameters

1. In OMC (Expert View), select **System** > **Numbering** > **Automatic Routing Selection** > **Automatic Routing: Prefixes**
2. Right-click the line and select **IP Parameters**

Destination	**SIP Gateway**
IP Type	**Dynamic**
IP Address	Leave blank.
Hostname	Leave blank.
Gateway Alive Protocol	Leave blank (keep-alive is disabled when DNS SRV is used).
Gateway Alive Timeout/s	Leave blank.
Index of Gateway Parameters	Enter the gateway index.

Configuring the **Gateway Parameters**

1. In OMC (Expert View), select **System** > **Numbering** > **Automatic Routing Selection** > **Gateway Parameters**
2. Review/modify the following parameters:

Index	Enter an index between 1 and 200.
Domain Name	Enter the domain name of the provider. *Note 1:* *This parameter is used to fill in the domain part of the **To** header of an INVITE message.*
Remote SIP Port	**Dynamic**

Index of SIP Numbers Format	1
DNS	Select **DNSSRV**.
Primary DNS Server	Enter the IP address of the primary DNS server.
Secondary DNS Server	Enter the IP address of the secondary DNS server. *Note 2:* *This IP address is used when the primary server does not answer.*
Outbound Proxy	Enter the name or the IP address of the outbound proxy.

Note 3:
The Alcatel-Lucent OmniPCX Office Communication Server can belong to one domain only. If several gateways are defined, they use the same DNS servers. The modification of DNS server addresses for one gateway is automatically applied to the other gateways for which DNS SRV is enabled. However, it is possible to mix gateways with DNS SRV enabled and gateways with DNS SRV disabled.

Configuring SIP Public Numbering

SIP public numbering configuration is described in module Public SIP Trunking - Feature Description § Numbering Formats .

6.4.2.4.6 Configuring the Local Domain Name

1. In OMC (Expert View), select **System** > **Voice Over IP** > **VoIP: Parameters** > **SIP** tab
2. Review/modify the following parameter:

Local Domain Name	This name is used in the domain part of the FROM header. It can be, for example, the domain name of the provider.

6.4.2.4.7 Configuring Timers

1. In OMC (Expert View), select **System** > **Voice Over IP** > **VoIP: Parameters** > **SIP** tab
2. Review/modify the following parameters:

Timer T1	Retransmission timer: waiting duration before re-sending a request. Default value: 1000 ms
Timer T2	Response timer *Note:* *T1 and T2 timers are defined in the RFC3261.*
Number of Retries	Maximum number of retries.

6.4.2.4.8 Configuring Registration Parameters

If the Alcatel-Lucent OmniPCX Office Communication Server must register, registration parameters must be configured.

1. In OMC (Expert View), select **System** > **Voice Over IP** > **VoIP: Parameters** > **SIP** tab
2. In the **Registration** pane, check the **Requested** box
3. Review/modify the following parameters:

Registered User Name	Enter the name provided by the provider. This can be for example the installation number. In this field is left empty, the name of the main VoIP board is used.
Expiration Time	Enter the validity time of the registration. Default value: 3600 s

4. If DNS SRV is not used, review/modify the following attributes:

Registrar IP Address	Enter the Registrar IP address.
Port	Enter the port number to be used for registration.
Outbound Proxy IP	Enter the Outbound Proxy IP address.

5. If DNS SRV is used, check the **DNS SRV** box and review/modify the following attributes:

Registrar Name	Enter the Registrar name.
Outbound Proxy	Enter the Outbound Proxy name.

6. Alcatel-Lucent OmniPCX Office Communication Server supports the Digest authentication scheme (MD5). If Alcatel-Lucent OmniPCX Office Communication Server must authenticate to the provider, enter the authentication parameters:

User Name	Enter the user name (login) for authentication.
Shared Secret	Enter the password associated with the user name for authentication.
Registered Realm	Enter the realm name.

6.4.2.4.9 Appendix: Noteworthy Addresses for Codec/Framing Negotiation

Codec/Framing Negotiation

Three noteworthy addresses have an impact on codec/framing negotiation: **MultAnsReinv**, **PrefCodec** and **PrefFraming**.

Notes:

*Noteworthy addresses have no impact when the **Codec/Framing** in the **Automatic Routing: Prefixes** parameters is not set to **Default***

Noteworthy addresses apply:

- *To outgoing calls when the called party answer contains a list of codec/framing*
- *To incoming calls when the caller INVITE message contains a list of codec/framing*

Outgoing Call

MultAnsReinv = **00** **PrefCodec** = **0** **PrefFraming** = **0**	1. The Alcatel-Lucent OmniPCX Office Communication Server sends the list of all supported codec/framing in the SDP part of the INVITE message. 2. The called party answers with a list of codec/framing. 3. The Alcatel-Lucent OmniPCX Office Communication Server sends the list of all supported codec/framing in the SDP part of the INVITE message.
MultAnsReinv = **01** **PrefCodec** = **0** **PrefFraming** = **0**	1. The Alcatel-Lucent OmniPCX Office Communication Server sends the list of all supported codec/framing in the SDP part of the INVITE message. 2. The called party answers with a list of codec/framing. 3. The Alcatel-Lucent OmniPCX Office Communication Server sends G711/30ms in the SDP part of a Re-INVITE message. 4. The called party either accepts or rejects the call.
MultAnsReinv = **01** **PrefCodec** = **x** **PrefFraming** = **y**	1. The Alcatel-Lucent OmniPCX Office Communication Server sends the list of all supported codec/framing in the SDP part of the INVITE message. 2. The called party answers with a list of codec/framing. 3. There are two cases: • If present in the list received from the called party, the Alcatel-Lucent OmniPCX Office Communication Server sends the preferred codec/framing in a Re-INVITE message. • If the preferred codec/framing is not in the list received from the called party, the Alcatel-Lucent OmniPCX Office Communication Server sends G711/30ms in the SDP part of a Re-INVITE message. 4. The called party either accepts or rejects the call.

Incoming Calls

PrefCodec = **0** **PrefFraming** = **0**	1. The caller sends a list of codec/framing in the INVITE message. 2. The Alcatel-Lucent OmniPCX Office Communication Server sends the list of all supported codec/framing in the answer. 3. The caller acknowledges with one of the codec/framing received in the answer.
PrefCodec = **x** **PrefFraming** = **y**	1. The caller sends a list of codec/framing in the INVITE message. 2. There are two cases: • If the preferred codec/framing is in the list received, the Alcatel-Lucent OmniPCX Office Communication Server answer with the preferred codec/framing. • If the preferred codec/framing is not in the list received, the Alcatel-Lucent OmniPCX Office Communication Server answer with the list of all supported codec/framing.

Noteworthy Addresses Configuration

MultAnsReinv

1. In OMC (Expert View), select **System** > **System Miscellaneous** > **Memory Read/Write** > **Debug Labels**
2. Select **MultAnsReinv**

MultAnsReinv	• **01** (default value): Re-invite sent on multiple-codec answer • **00**: No Re-invite sent on multiple-codec answer

PrefCodec and **PrefFraming**

1. In OMC (Expert View), select **System** > **System Miscellaneous** > **Memory Read/Write** > **Other Labels**
2. Modify the following addresses to enable preferred codec/framing:

   Note:
   To enable preferred codec/framing, both addresses must be different from 0.

PrefCodec	Enter one of the following values: • **0 (00 00)** (default value): disabled • **2 (02 00)**: G723 • **3 (03 00)**: G729 • **4 (04 00)**: G711 A law • **5 (05 00)**: G711 µ law
PrefFraming	Enter one of the following values: • **0 (00)** (default value): disabled • **10 (0A)**: 10 ms • **20 (14)**: 20 ms • ... • **110 (6E)**: 110 ms • **120 (78)**: 120 ms

6.4.2.4.10 Appendix: VoIP Noteworthy Addresses

Overview

The values of noteworthy addresses (`VOIPnwaddr`) can be modified as typical Alcatel-Lucent OmniPCX Office Communication Server noteworthy addresses can be.

Any modification must be followed by a warm reset of the Co-CPU.

Restart the Alcatel-Lucent OmniPCX Office Communication Server when a VoIP daugther board is present on the main CPU.

Presentation

- **Name**: internal name of the value
  This value can be read with the `webdiag` tool:
  a. In the VoIP Information Menu, select **VoIP Check**
  b. In the file Content, select `*.cfg`
  c. Select **noteworthy_val.cfg**
- **Position**: position of the value in the **Noteworthy address** buffer of OMC
  The first position is at 0, the last position is at 0x63
- **Length**: length of the value in bytes
- **Default**: default value after a cold reset of the Alcatel-Lucent OmniPCX Office Communication Server

- **Range**: range of accepted values

List of Values

Privacy Level

Presentation

Name	Position (byte)	Length (byte)	Default	Range	Example
`Sipgw_priv_lvl`	2	2	1	00	**00** or **01**

Description

Set the Alcatel-Lucent OmniPCX Office Communication Server privacy policy when CLIR is active.

If the identity presentation of user 1234 is restricted, the `From` field of an outgoing `INVITE` message from the Alcatel-Lucent OmniPCX Office Communication Server is:

- If Privacy Level = 0
  `From: sip:anonymous@anonymous.invalid`
- If Privacy Level = 1
  `From: sip:1234@LocalDomain`

Session Timer

Presentation

Name	Position (byte)	Length (byte)	Default	Range	Example
`Session Timer`	4	2	0000	0000-FFFF	**0060** for one hour

Description

The session timer is the delay parameter specified in RFC4028.

For each call, a keep alive (session refresh) operation, which consists in a re-invite message, is performed at 50% of the period specified by this variable.

If no session refresh operation is performed or is successful by the end of this timer, the call is released.

The timer unit is the minute:

- The **0000** default value refers to the default timer, of a 720 minutes (12 hours) duration.
- The **FFFF** value results in disabling the session timer: no keep alive operation is performed. This selection avoids several interoperability problems.
- Any other value defines the session timer duration in minutes.

Don't Use DNS SRV Unreachable Proxy List

Presentation

Name	Position (byte)	Length (byte)	Default	Range	Example
Don't use DNS SRV unreachable proxy list	6	1	00	00-01	**01** results in not using the unreachable proxy list

Description

DNS SRV makes use of a quarantine list to memorize unreachable proxies. This optimizes overflow by not trying to connect to known unreachable proxies.

The default value **00** results in using the unreachable proxy list.

The **01** value results in not using the unreachable proxy list.

NAT Keep Alive for DNS SRV

Presentation

Name	Position (byte)	Length (byte)	Default	Range	Example
NAT Keep Alive	8	2	0000	0000-FFFF	**0258** results in NAT connection in router during 600 seconds

Description

When the Alcatel-Lucent OmniPCX Office Communication Server is reached via a router (NAT/Firewall), the NAT connection must be permanently open.

This noteworthy address is the duration of the NAT connection in the router.

When DNS SRV is enabled, the Alcatel-Lucent OmniPCX Office Communication Server sends the OPTION messages at 75% of the delay in order to maintain the NAT connection.

The **0** value results in no NAT Keep Alive.

A value above **0** results in enabled NAT Keep Alive for DNS SRV rules, and specifies the NAT connection duration.

Signalling Source Port

Presentation

Name	Position (byte)	Length (byte)	Default	Range	Example
Signalling Source Port	10	2	0000	0000-FFFF	**13C4** results in using **5060** as source port for request sending

Description

This parameter allows to force the Alcatel-Lucent OmniPCX Office Communication Server source port for SIP signalling. This parameter is associated to both UDP and TCP transport.

The **0** Default value results in the use of a dynamically allocated source port. The source port is dynamically chosen in a pool of free ports.

Any value above **0** results in this port used as source for SIP signalling.

Note:
Ensure a free port is selected.

6.4.3 Private SIP Trunking

6.4.3.1 SIP Gateway Services

6.4.3.1.1 Services

In Alcatel-Lucent OmniPCX Office Communication Server R5.0, SIP (Session Initiation Protocol) comes as a second VoIP protocol. It has been designed to replace H.323 standard protocols.

Alcatel-Lucent OmniPCX Office Communication Server R5.0 embeds an integrated SIP gateway with the following features:

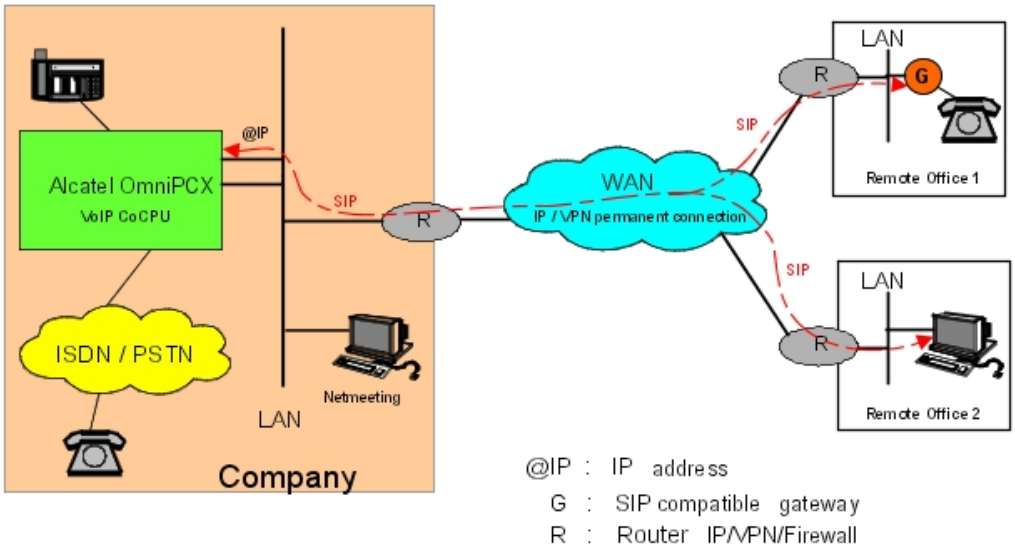
- Up to 96 simultaneous VoIP calls
- G711, G729a, and G723.1 support
- RTP/RTCP: manages audio signals, including real-time packetisation of media streams and control reports
- T38: real-time Fax over IP
- Echo cancellation
- Tone detection/generation
- Voice Activity Detection (VAD)/Silence suppression
- ICMP Keep Alive (to remote gateway)

Alcatel-Lucent OmniPCX Office Communication Server R6.0 in comes with the following additional SIP features:

- SIP option Keep Alive (to remote gateway)
- Direct RTP
- SIP registration and authentication
- SIP public numbering

Overview

Alcatel-Lucent OmniPCX Office Communication Server users can communicate with remote SIP components such as gateways, proxies or terminals, through SIP for signalling and RTP/RTCP for voice.



Transfer

Transfer in private networks complies with standards RFC 3515, 3891 and 3892.

Transfer in conversation and in ringing with optimized audio path is fully supported in private networks.

Fax over IP (FoIP)

The FoIP service is available when a Fax is detected in an SIP call. When this happens, the Audio channels are closed and T38 sessions are initialized to transmit or receive Internet Fax packets (IFP).

Alcatel-Lucent OmniPCX Office Communication Server only allows T38 sessions over UDP. In order to ensure the reliability of the UDP transmission, the packets are sent several times to ensure that the information reaches its destination. This operation is called "UDP Redundancy".

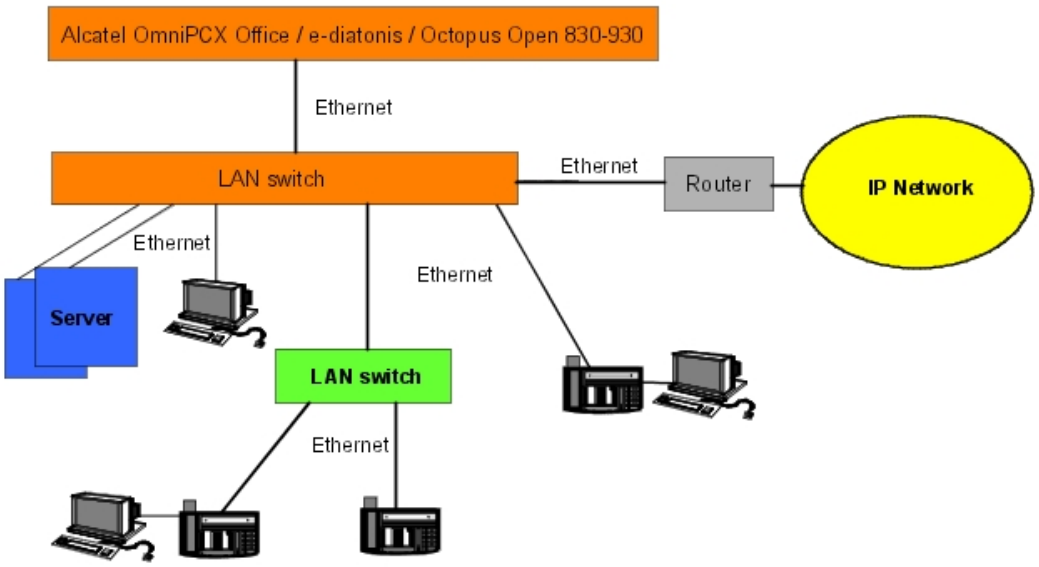
In order to reduce bandwidth use, an operation (framing) allows the concatenation of packets of the same type.

The FoIP service does not require any particular configuration of the ARS table. A Fax call is considered as a transparent SIP call.

6.4.3.2 Topologies

6.4.3.2.1 Architecture

The following topology is recommended for connecting an Alcatel-Lucent OmniPCX Office Communication Server R5.0 using SIP.



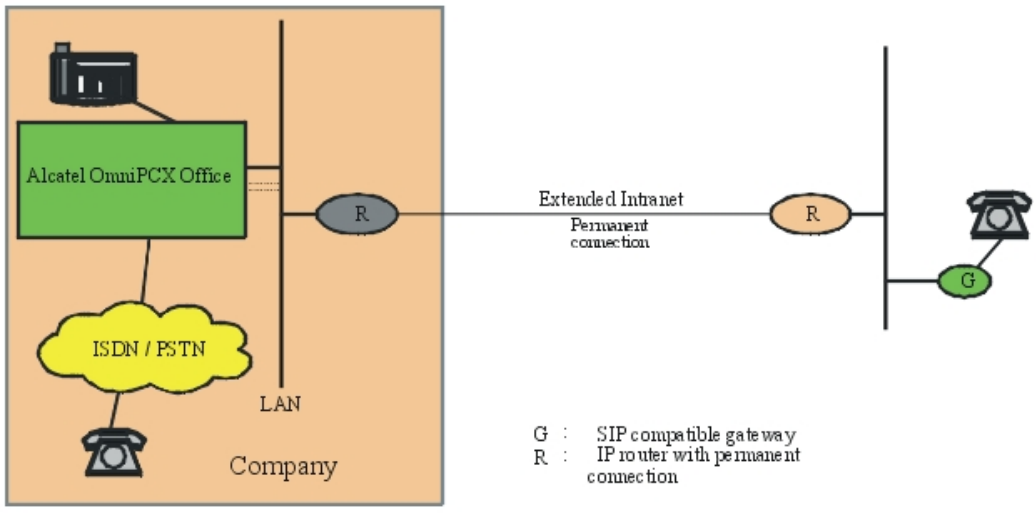
The bandwidth of an Ethernet LAN can be 10 or 100 Mbps. If the network operates at 100 Mbps, adding terminals operating at 10 Mbps risks downgrading the bandwidth used by VoIP and hence audio quality. You might need to isolate these devices on external LAN switches hooked up to the system.

CoCPU boards are connected to the local client network using a LAN switch. This solution helps reduce Ethernet traffic on the CoCPU board.

Multi-site configurations

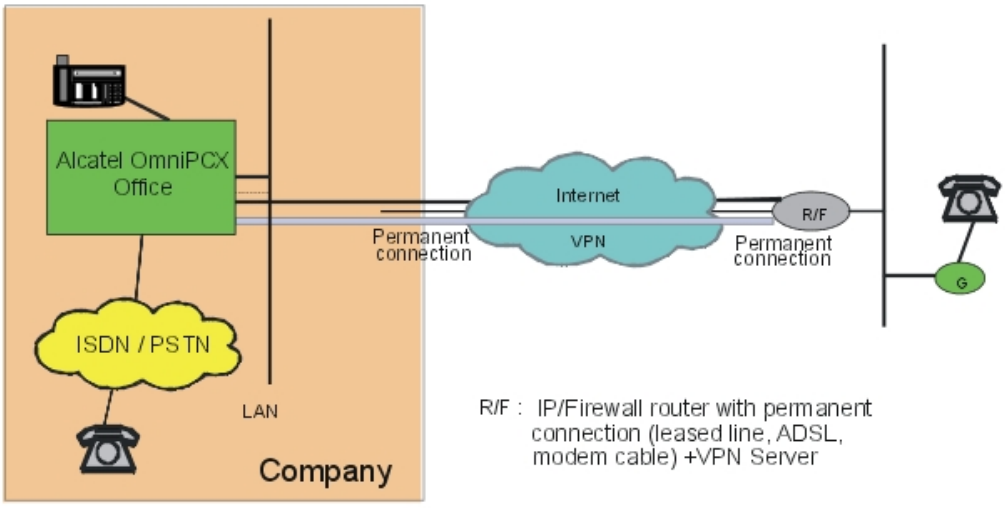
A multi-site configuration is possible via an extended Intranet or an Internet VPN.

SIP gateway integrated into an extended Intranet



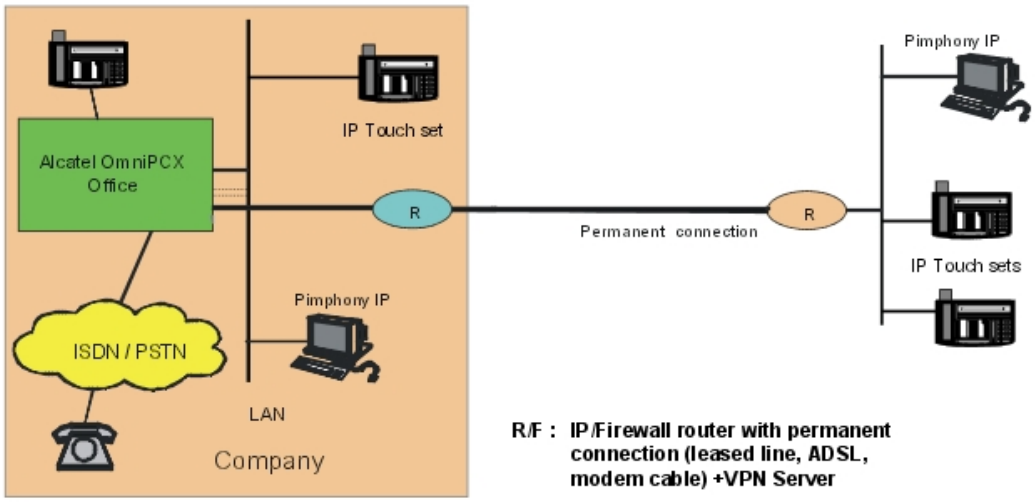
The IP router (R) connected to the Intranet can be a simple IP router. The reservation of bandwidth is "guaranteed" if this router supports Ipv4 ToS (DiffServ).

SIP gateway integrated into a VPN



The IP router (R/F) at the front end of the VPN must offer Proxy/Firewall and VPN server functionality (IPSec with 3DES encryption for interoperability with the system's built-in router).

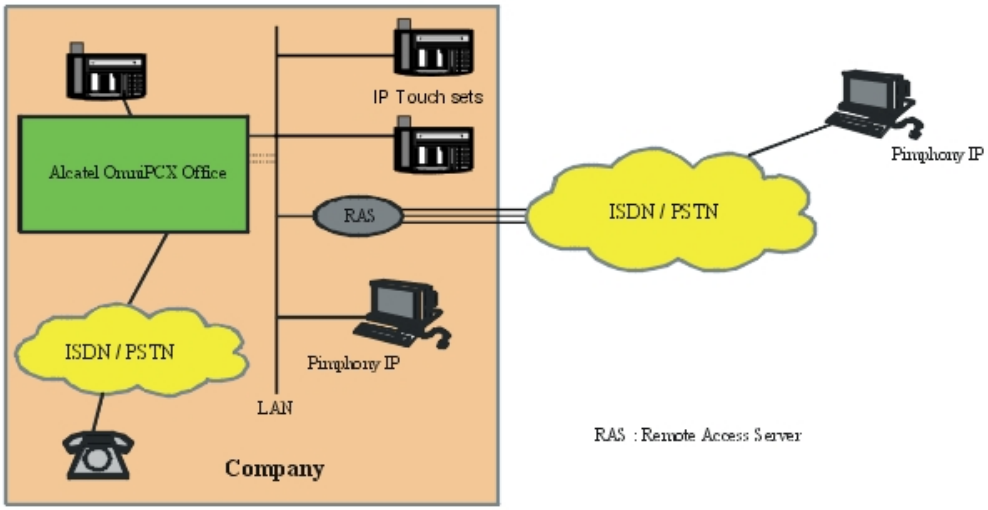
IP telephony in an extended Intranet



Note:

See also the Home Worker and Remote Worker topologies described earlier.

PIMphony IP through RAS (Remote Access Server)



The RAS is equipped with a pool of modems or a T0/T2. The RAS client PC is authenticated by a PAP/CHAP authentication procedure, then is called back by the RAS (callback).

PC with Microsoft NetMeeting®

A NetMeeting PC can connect to the company via the VPN (PPTP connection on Internet) or directly by a RAS connection via the telephone network (PSTN/ISDN).

6.4.3.3 Authentication/Registration

6.4.3.3.1 Authentication and Registration

Authentication and ARS

The Alcatel-Lucent OmniPCX Office Communication Server authentication mechanism conforms to the RFC 3261 recommendation and to data registered in the ARS table. Two fields are provided in the ARS table for SIP components: login and password (username and shared secret).

Incoming calls

There is no authentication for incoming calls. Only calls from IP addresses registered in the ARS table are accepted.

Outgoing calls

The type of authentication depends upon the destination listed in the ARS table. For calls to proxy servers, Alcatel-Lucent OmniPCX Office Communication Server sends an authentication

request when a 407 response is received. Authorisation is accomplished by a combination of a username and a password (shared secret) in accordance with recommendations RFC 2617 and RFC 1321.

Parameters

From Alcatel-Lucent OmniPCX Office Communication Server R6.0 and higher: In a consistent SIP protocol configuration in the ARS table, a new field, Gateway Parameters, enables you to activate an authentication index.

By OMC (Expert View): **Numbering -> Automatic Routing Selection-> Automatic Routing: Prefixes**

When the index has been activated, the following fields are displayed in the **Gateway Parameters** window:

- **Index**
- **Login**
- **Password**
- **Domain Name**
- **Realm**
- **RFC3325** (not used for authentication)
- **Remote SIP port** (not used for authentication)
- **SIP public numbering** (not used for authentication)

For more information on these fields, you can also refer to the OMC On-line documentation.

Registration parameters

The following fields are used to control registration and authentication:

- **Registration requested (yes/no)**: indicates if registration is required
- **Reg. expire time**: timeout used to refresh registration periodically (by default, 3600 seconds)
- **Username**: username (login) for authentication
- **Shared secret**: password associated with the username for authentication
- **IP Address**: Registrar's IP Address

from R6.0 and higher,

- **Registered Username**: Username used for registration
- **Port**: UDP number for REGISTER request
- **Registered Realm**

6.4.3.4 Configuring SIP Gateway

6.4.3.4.1 Hardware configuration

SIP Gateway is an application layer which works as an interface between IP telephony (SIP stack) and switched telephony (Alcatel-Lucent OmniPCX Office Communication Server PBX call manager).

Modifying the default protocol

H.323 is set as the default protocol in Alcatel-Lucent OmniPCX Office Communication Server. You must set SIP as default protocol.

By OMC (Expert View): **System -> Voice on IP -> VoIP: Parameters -> General** tab

Once the protocol has been modified, OMC asks you to reboot the VoIP CoCPU boards. When VoIP is defined on the main CPU, you will need to reboot the whole Alcatel-Lucent OmniPCX Office Communication Server.

Configuring the system as the SIP gateway

By default, after initialisation, all the DSP channels are assigned to the pool of VoIP subscriber channels (IP telephony).

In a pure SIP gateway configuration, all the DSP channels of the system VoIP daughter boards are used for "IP network" accesses.

By OMC (Expert View): **System -> Voice on IP -> VoIP: Parameters -> General** tab

Number of VoIP access channels (IP trunks): Number of channels for VoIP IP access, i.e. 1 DSP channel for 1 "network access".

Direct RTP: The direct RTP service provides direct RTP and RTPC flow exchange between IP endpoints (IP sets, DSP channel on VoIP or CoCPU boards, distant gateways).

To activate the direct RTP option, check the check box. This should be carried out when there is no traffic on the system.

Note:
Each DSP channel placed in the "VoIP access" pool is considered as a "network access" by the PBX, i.e. 1 VoIP DSP = 1 B-channel. As there can be a maximum of 6 VoIP daughter boards, each with 16 DSP channels, there can be no more than 96 VoIP access DSP channels, i.e. 96 "IP" B-channels.

Network accesses (T0, T2, analogue TL, DLT0, DLT2) + VoIP accesses = 120 accesses Max.

Once the protocol has been modified, OMC asks you to reboot the VoIP CoCPU boards.

Quality of IP service: Selection of QoS type for the remote SIP gateway VoIP calls.

If all the network elements support the IP ToS, you can choose an IP priority from 1 to 7.

If all the network elements are "DiffServ" compatible, you can choose:

- DiffServ PHB Best Effort Forwarding (BE) (priority bits: 00000000), or
- DiffServ PHB Expedited Forwarding (EF) (priority bits: 10111000).

Configuring the Gateway timeouts (optional)

By OMC (Expert View): **System -> Voice on IP -> VoIP: Parameters -> Gateway** tab

NB: The parameters have standardized values, do not change them without prior analysis.

- **RAS Request Timeout:** Maximum authorised response time for a RAS request ("Registration, Admission, Status") made to the gatekeeper; between 10 and 180; default value = 20

- **Gateway Presence Timeout :** Determines the presence of a remote Gateway; value between 10 and 600; default value = 50
- **Connect Timeout:** Maximum authorised time interval between initialisation and connection; value between 10 and 1200; default value = 500
- **H.245 Request Timeout:** Maximum authorised response time for an H.245 request; value between 10 and 60; default value = 40
- **SIP: End of dialling timeout**: Default value = 5

Configuration of T38 parameters for Fax over IP (optional)

By OMC (Expert View): **System -> Voice on IP -> VoIP: Parameters -> Fax** tab

- **UDP Redundancy:** Number of Fax data packets forwardings; value between 0 and 2; default value = 1
- **Framing:** Number of data packets in the same frame; value between 0 and 5; default value = 0. In fact, the number of packets is equal to the number set in this field + 1

Note:

***a**) Only T38 traffic is supported: modem, V90, V24, etc. are not available via H323/SIP connection. **b**) if the UDP redundancy is set to 0, any framing value (0 to 5) can be used. If the UDP redundancy is set to 1, the framing must not be configured to a value higher than 1*

6.4.3.5 Configuring a Remote SIP Gateway

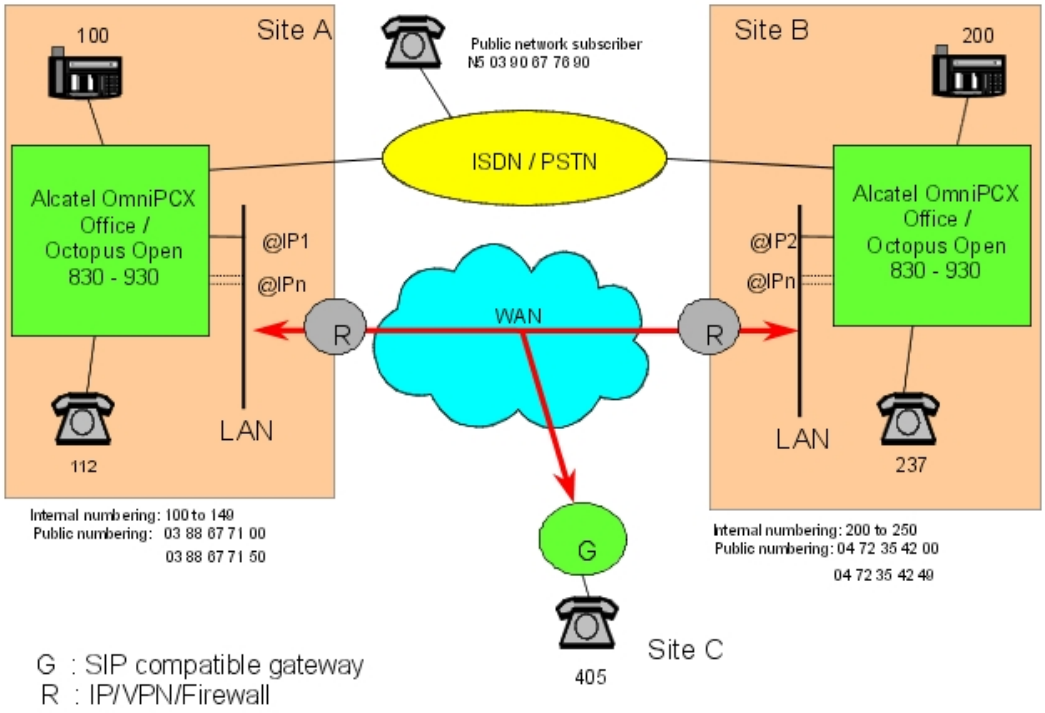
6.4.3.5.1 Configuration examples

Configuring outgoing communication (ARS table)

The choice of routing a telephone communication between a public network access or a VoIP access and the busy trunk overflow feature is defined in the ARS table.

Like conventional outgoing telephone calls, a VoIP call is subject to the ARS mechanisms: link categories, ARS time slot management, overflow on busy, etc.

In the diagram below, sites A and B are Alcatel-Lucent OmniPCX Office Communication Servers. Site C is a remote system integrating a SIP gateway.



- @IP1: IP address of the master VoIP CoCPU/CoCPU-1/CoCPU-2 board at site A -
- @IP2 : IP address of the master VoIP CoCPU/CoCPU-1/CoCPU-2 board at site B. For example: 192.189.50.120
- @IPn: IP address of slave board(s)

Basic call

The site A stations call the site B stations by dialling their internal numbers:

Internal numbering plan (site A):

Function	Start	End	Base	NMT	Priv
Secondary trunk group	2	2	ARS	Keep	Yes

ARS Table:

Network	Access	Range	Substitute	List. Trunk group list	Called Party (ISVPN/H450)	Comment
Priv.	2	00-49	2	4	het	SIP to site B

- By default, the "Called(ISVPN/H450)" field is set to "het" (heterogeneous). When set to "hom" (homogeneous), a remote IP is expected to support optimised forwarding and transfer; local and remote numbering plans are supposed to be consistent.
- The "User Comment" field enables a comment to be associated with the ARS input (20 characters maximum).

Note:

The IP parameters in the ARS table are accessed by right-clicking and selecting "IP parameters".

Destination	IP Type	IP address	Hostname	Gateway Alive Protocol	Gateway Alive Timeout	Gateway Bandwidth	Gateway Alive Status
SIP Gateway	Static	192.189.50.120	option	either ICMP (default) or SIP option	300	128 Kbits (5 calls)	Enabled

- The "Destination" field of an ARS input to VoIP accesses must be set to "SIP Gateway".
- For a "SIP Gateway" destination, the "IP Type" must be a static IP address (non-modifiable field).
- The "IP Address" field must be that of the remote SIP gateway. In the example, this value corresponds to the IP address of the master VoIP CoCPU/CoCPU-1/CoCPU-2 board at site B.
- The "Host name" can be used instead of the IP address of the remote gateway. Requires a DNS server.
- "Gateway Alive Protocol":
  - The gateway alive protocol can be either:
    - ICMP
    - SIP option (From Alcatel-Lucent OmniPCX Office Communication Server R6.0)
- "Gateway Alive Timeout":
  The gateway alive timeout can be selected between 20 and 3600 seconds (300 by default). When set to 0, the gateway alive protocol mechanism is inhibited. This option is to be used specifically when it is impossible to use ICMP to test the presence of the remote gateway. In this case, it is impossible to know whether the gateway is alive or out of service.
- Gateway Bandwidth / QoS: for each ARS input to a remote SIP gateway, a bandwidth must be reserved for the VoIP to the remote SIP gateway. The number of simultaneous communications that can be held depends on this value:

Bandwidth	Number of possible simultaneous communications
None	No communication possible (Default value)
55.6 Kbps	1
64 Kbps	2
128 Kbps	5
256 Kbps	10
512 Kbps	20
# 1024 Kbps	> 20

Example: if the total bandwidth corresponding to the data rate to a remote gateway is 256

Kbps, and the mean traffic level is 50%, it would be wise to define a bandwidth of 128 Kbps for VoIP.

Remark concerning the quality of service (QoS)

If we take our example, site A can make SIP calls to sites B and C. One assumes that the bandwidths reserved for VoIP at the LAN/WAN gateways of each site are the following:

- Bandwidth reserved for VoIP on site A: 1024 Kbps (20 calls or more)
- Bandwidth reserved for VoIP on site B: 128 Kbps (5 simultaneous calls)
- Bandwidth reserved for VoIP on site C: 64 Kbps (2 simultaneous calls)

In this configuration, you can see that it is possible to make 7 simultaneous calls from site A to the remote SIP gateways: 5 to site B and 2 to site C.

7 DSPs can therefore be assigned in the "VoIP access" pool for site A (7 being the number of DSPs needed to call sites B and C simultaneously).

However, let us assume that there is no ongoing communication between sites A and C, and that 5 calls are established between A and B. The total number of VoIP network access DSPs consumed in PBX A is 5: therefore 2 DSPs remain available to establish two other calls to site B.

Yet in this example we exceed the bandwidth reserved for VoIP at the LAN/WAN gateway of site B: the quality of service is no longer guaranteed.

To avoid downgrading the VoIP service, the system uses the "Gateway Bandwidth" field of the ARS table associated with the input to the remote SIP gateway of site B, which will be configured at 128 Kbps (5 calls), as quality indicator (QoS). Although there are still 2 DSPs available, the PBX will refuse a 6th call to site B.

Note:

To optimise management of this ARS table parameter, it is vital to have precise information on the available bandwidth (reserved) for VoIP calls.

- "Gateway Alive Status": this regularly updated read-only field indicates the status of the remote gateway:
  - Alive: remote gateway present
  - Down: remote gateway absent / out of service

However, it may turn out to be judicious to deactivate the mechanism if one is sure of network reliability, in order to reduce the traffic.

Incoming call

An incoming "VoIP access" call is analysed in the private numbering plan. In our example:

Private numbering plan of site B:

Function	Start	End	Base	NMT	Priv
Local call	200	249	200		No

Forcing a public call to the SIP gateway

LCR: Least Cost Routing

When a site A subscriber dials the public number of the site B station, the call can be forced to the VoIP network accesses.

Internal numbering plan of site A:

Function	Start	End	Base	NMT	Priv
Main trunk group	0	0	ARS	Drop	No

ARS Table:

Network	Access	Range	Substitute	List. Trunk group list	Called Party (ISVPN/H450)	Comment
Pub.	04723542	00-49	2	4	het	SIP to site B

Overflow

When a site A subscriber calls a site B station by its internal number, ARS routing enables the calls to be re-routed to the public network when it is no longer possible to call via the VoIP accesses. The following criteria render a "VoIP access" trunk group inaccessible:

- The VoIP CoCPU/CoCPU-1/CoCPU-2 board of site A is out of service
- No more DSPs associated with the VoIP accesses are available
- The remote SIP gateway is out of service (VoIP CoCPU/CoCPU-1/CoCPU-2 board of site B is out of service)
- The quality of service (QoS) to the remote gateway is poor (exceeding of the simultaneous communications threshold for the reserved VoIP bandwidth of this remote SIP gateway)

ARS table of site A: Network

Calling the site B station by its internal number:

Network	Access	Range	Substitute	List. Trunk group list	Called Party (ISVPN/H450)	Comment	Destination
Priv.	2	00-49	2	4	het	SIP to site B	SIP Gateway
			04723542	1	het	ISDN Access	Not IP

Calling the site B station using its public number:

Network	Access	Range	Substitute	List. Trunk group list	Called Party (ISVPN/H450)	Comment	Destination	
Pub.	04723542	00-49	2	4	het	SIP to site B	SIP Gateway	
			04723542	1	het	ISDN Access	Not IP	
Pub.	04723542	50-99	04723542	1	het	ISDN Access	Not IP	*

* : As the public numbers 04723542 50 to 99 do not belong to site B, they must be routed to the public network.

Break In

The break-in service enables the PBX to re-route a public number from site A to site B. In our example, the public network subscriber dials the number 03 88 67 71 50 which is routed to station 250 on site B:

Public numbering plan (site A):

Function	Start	End	Base	NMT	Priv
Secondary trunk group	7150	7150	ARS	Keep	No

ARS Table:

Network	Access	Range	Substitute	List. Trunk group list	Called Party (ISVPN/H450)	Comment
Pub.	0388677150		250	4	het	SIP to site B

Reminder: it is vital for the PBX "Installation number" field to be configured; e.g. for site A: 388677100.

Break Out

The break-out service enables proximity calls to be made. In our example, a site A station dials a public number starting with 04, the call is routed to site B via the SIP gateway, then routed to the public network from site B. Configuration:

Internal numbering plan of site A:

Function	Start	End	Base	NMT	Priv
Main trunk group	0	0	ARS	Drop	No

ARS table of site A: Network

Network	Access	Range	Substitute	List. Trunk group list	Called Party (ISVPN/H450)	Comment	Destination	
Pub.	04		004	4	het	SIP to site B	SIP Gateway	*
			04	1	het	ISDN Access	Not IP	**

* : as the prefix 0 is dropped in the internal numbering plan, 004 must be substituted for 04,

** : this sub-line allows overflow to the public network lines of site A when the VoIP access calls are inaccessible.

As an incoming VoIP access call is analysed in the private numbering plan, the private numbering plan of site B must be programmed as follows:

Function	Start	End	Base	NMT	Priv
Main trunk group	0	0	0	Drop	No

6.5 Installation

6.5.1 Overview

A few precautions must be taken when adding a machine into a local network to ensure the lasting compatibility and quality of the network.

The starting point for the integration and configuring of Alcatel-Lucent OmniPCX Office Communication Server on a LAN is the knowledge of the network structure, its characteristics and its elements. After that, it is necessary to collect the significant parameters and

characteristics of the LAN.

Below is a list of the parameters to be collected:

CPU Board

- Hostname: DNS name or alias of the board
- IP Address: IP address of the board
- IP Subnet Mask : subnet mask of the LAN

General

- Number of IP trunk DSP channels: number of channels associated with remote H.323 gateway access
- Number of IP subscriber DSP channels: number of channels associated with the IP Telephony service
- Quality of service: type of quality of service to be implemented according to the LAN equipment

H.323 Gateway

- IP addresses of remote H.323 gateways
- Gatekeeper integrated into the PBX: use of an integrated gatekeeper or not
- Identification of gatekeeper: IP address of external gatekeeper

SIP Gateway

- IP address of remote SIP registrar
- IP addresses of remote SIP gateways

IP Telephony

- Activate the integrated DHCP server: use of the integrated DHCP server or not
- Dynamic Range: dynamic IP address range for IP telephony (IP sets) or for PCs

Remark:

In the case of a configuration involving Alcatel-Lucent OmniPCX Office Communication Server with Internet Access services, the DHCP server is configured in WBM (Web Based Management).

6.6 Installing VoIP Boards

6.6.1 Overview

You can install up to 6 CoCPU-1/CoCPU-2 boards (2 max. in the main module, 3 in the add-on modules) connected to a given Ethernet LAN, via RJ45 connectors. Each board has its own IP address.

If several boards are installed, one of them is the "master" board; its IP address and software characteristics serve as a reference. The other CPU boards are known as "slaves".

Note the following:

- If the main CPU board of the system is equipped with a VoIP daughter module, a maximum of 5 CoCPU boards can be installed in the system (one CoCPU board less).
- A main CPU board equipped with a VoIP daughter board is always considered as the

master VoIP board (additional CoCPU boards are considered as slaves).

- Two systems equipped with CPU boards must not be connected to the same LAN. They must be separated by a router or VLAN-compatible LAN switch. When the system starts, the CPU board performs a Bootp query and will connect to the main CPU board which answers this query first.

Caution:

The CPU boards can only be inserted when the system is powered down.

Default IP addresses

When the main CPU board is equipped with a VoIP-1 daughter board, the default IP addresses are the following:

- **CPU board used**
  - Master CPU: 192.168.92.246
  - CoCPU (5): from 192.168.92.248 to 192.168.92.252
- **Only CoCPU boards used**
  - Master CPU: 192.168.92.248
  - CoCPU: from 192.168.92.249 to 192.168.92.253

The IP addresses of all CPU/CoCPU boards must belong to the same subnet.

Remark:

Whatever the configuration, there is at least one master board and up to 5 slave boards.

6.6.1.1 General software configuration

The general configuration defines the minimum parameters to be set regardless of the VoIP service to be implemented:

- H.323 gateway only
- IP telephony only
- H.323 gateway and IP telephony

6.6.1.2 *CoCPU board with VoIP-1*

If VoIP-1 on main CPU:

General network parameter settings

- CPU hostname: DNS name or alias of the board (optional parameter)
- CPU IP address: IP address of the board
- IP Subnet Mask : subnet mask of the board
- Always master

6.6.1.3 General network parameters

By OMC (Expert View): **Hardware and Limits -> IP Addresses -> Boards** tab

Significant parameters:

- **Default router address:** IP address of the CPUe-1 or CPUe-2 (Internet Access) board or of the external router

- **IP of subnet mask:** subnet mask containing the PBX

These fields are necessary to access the WAN.

6.6.1.4 *Configuring the DSPs (optional)*

By OMC (Expert View): **System -> Voice on IP -> VoIP: Parameters -> DSP** tab

It is recommended not to change these parameters.

Meaning of parameters:

- **Law Mode:** Law A or Law µ compression (read only)
- **Echo Cancellation:** cancellation of the echo ("no" by default)
- **Voice Active Detection:** cancellation of silence ("yes" by default)

6.7 VLAN

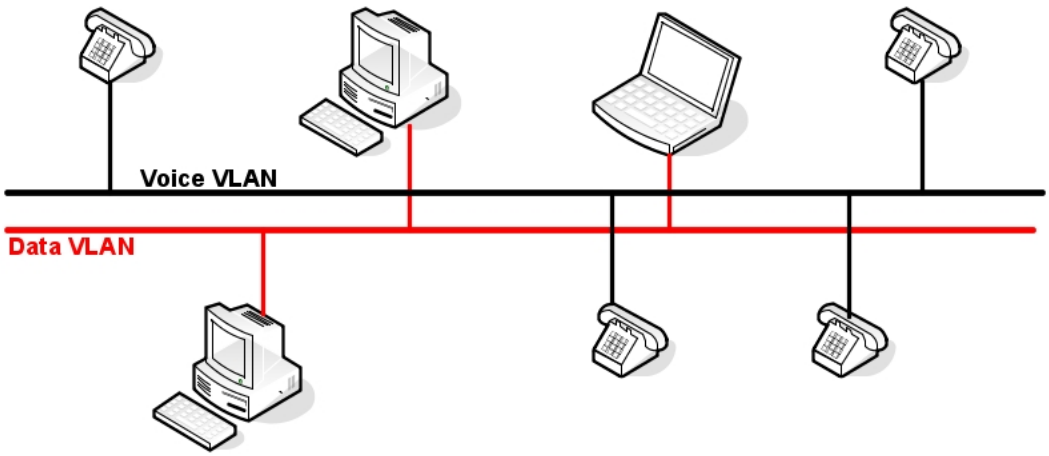
6.7.1 Overview

6.7.1.1 *Basic description*

A Virtual Local Area Network (VLAN) is a group of network elements from one or more LANs that are configured in such a way that they can communicate as if they were attached to the same wire.

VLANs are very flexible because they are based on logical connections instead of physical connections. The purpose is to segment ethernet traffic logically.

The figure below represents the abstraction of a physical LAN divided into two VLANs: a Voice VLAN (VoIP frames) for IP phone sets, and a Data VLAN for computers. In VLAN uses, the number of VLAN can be different depending the LAN management rules and the choice of the network administrator.



A VLAN architecture offers the following advantages:

- Increased performance through traffic segmentation (voice and data frames)
- Network tuning and simplified software configurations: LAN administrators can optimise their networks by grouping users logically
- Physical topology independance
- Increased security options: LAN administrators can segment privileged users (access to sensitive information) and standard users into separate VLANs, regardless of their physical location

6.7.2 Topologies

6.7.2.1 Detailed description

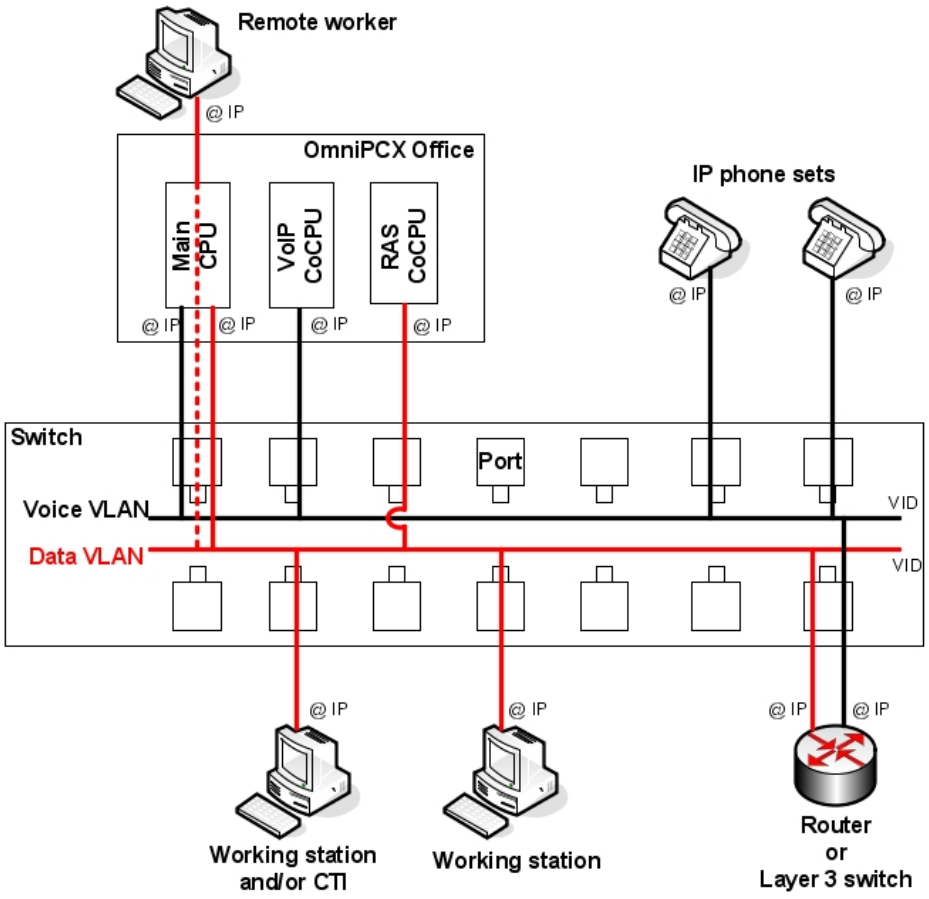
The purpose of this section is to show how Alcatel-Lucent OmniPCX Office Communication Server could be connected to VLANs. The OmniPCX Office is able to operate on 2 VLANS (1 for Voice and 1 for Data):

- The CPU and the CoCPU RAS are members of the Data VLAN group.
- The CPU and the CoCPU VoIP are members of the Voice VLAN group.

Because the CPU board works with both VLANs it must have a unique IP address for each VLAN.

Note:

SLANX and LANX boards must not be used in a VLAN topology because they do not recognise or support VLAN-tagged frames (802.1Q).



In the figure above, VoIP CoCPU boards are connected to a voice VLAN. Alcatel-Lucent OmniPCX Office Communication Server is configured to manage two VLANs, one for voice and the other for data. Additional voice and data VLANs will be managed by the external ethernet switch configuration and external routers (communication between VLANs).

Alcatel-Lucent OmniPCX Office Communication Server is connected to a switch with the following characteristics:

- VLAN-aware: a switch that can recognise and support VLAN-tagged frames.
- Each port to which the CPU boards and IP phone sets are connected must be of hybrid type with the same VLAN identifier (VID). A hybrid port is a switch port configured to send and receive 802.3 (data VLAN protocol) or 802.1Q (voice VLAN protocol) frames

6.7.3 Configuring VLAN

6.7.3.1 Configuration procedure

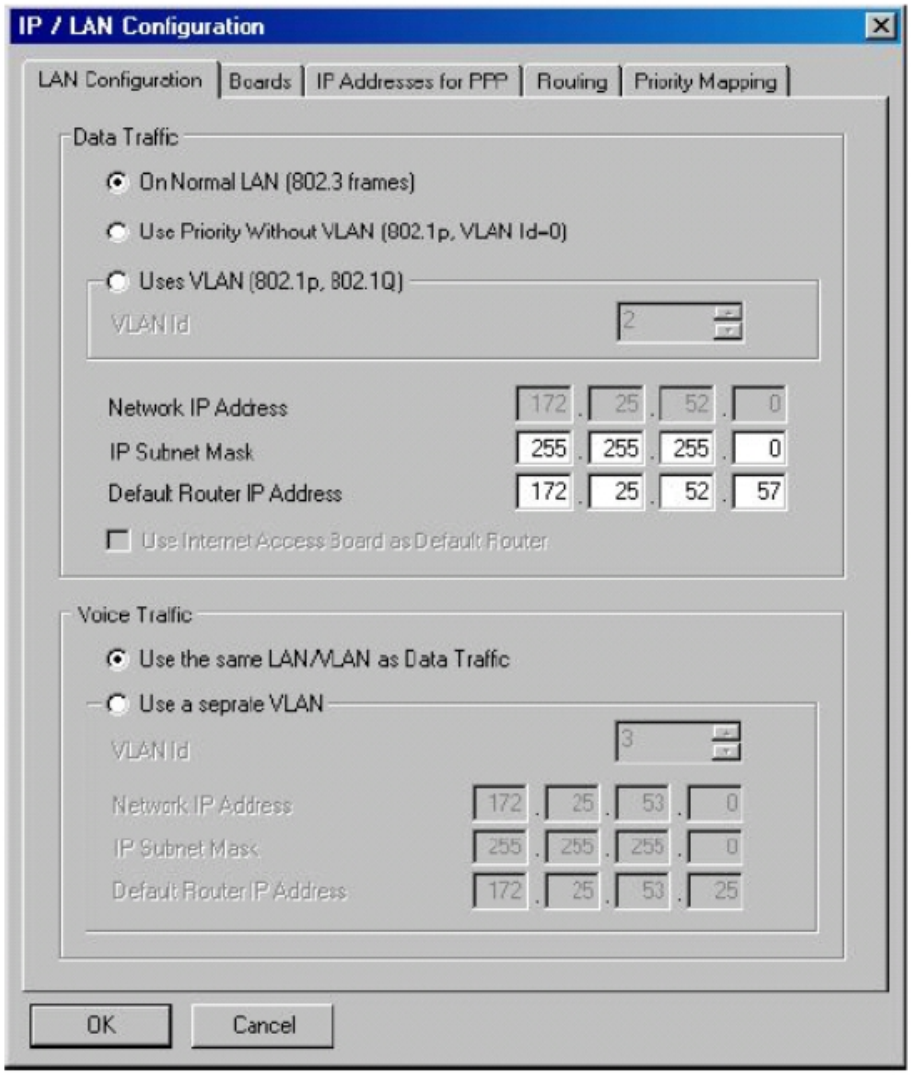
VLAN is configured for Alcatel-Lucent OmniPCX Office Communication Server through OMC. As VLAN configuration is closely related to IP Address configuration, both configurations are defined on the same node:

The IP/LAN Configuration property sheet contains the following pages:

- LAN Configuration
- Boards
- IP Addresses for PPP
- Routing
- Priority Mapping

6.7.3.1.1 LAN Configuration

This property page defines the overall LAN logical structure. It is divided into two areas: **Data Traffic** and **Voice Traffic**.



The example above shows the default LAN configuration properties where the:

- **Data Traffic** property is set to **On normal LAN** - all LAN data traffic circulates in 802.3 frames.
- **Voice Traffic** property is set to **Use the same LAN/VLAN as Data Traffic** - voice and data packets are not tagged. There is no VLAN for voice traffic so traffic is not segmented.

If the **Voice Traffic** property is set to **Use Separate VLAN** data packets are not tagged but voice packets are sent with the **VLAN=3** tag (as shown in the example above).

When you change the **IP Subnet Mask** or the **Default Router IP Address** fields, the **Network IP Address** field is recalculated and a warning icon is displayed to indicate that all boards IP addresses have been recalculated to match the new network. (This only applies to data traffic)

VLAN IDs

Select the Data Traffic property **Use VLAN (802.1p, 802.1Q)** to define a VLAN ID for data traffic.

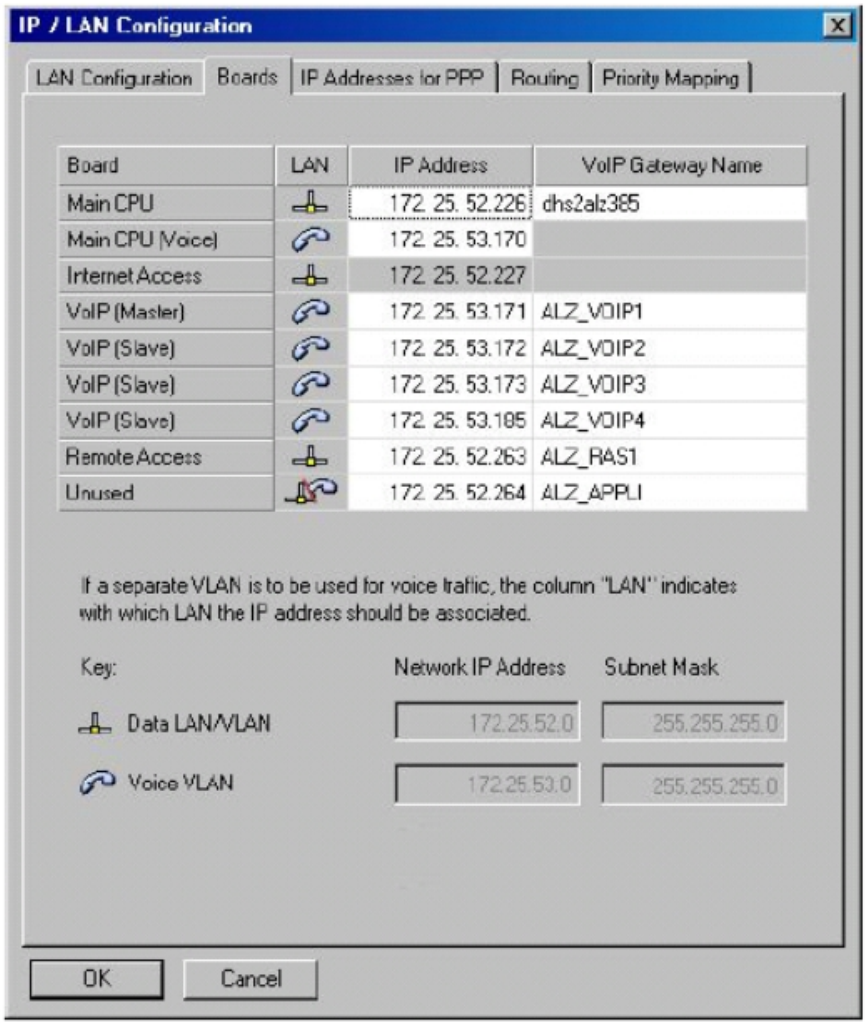
Select the**Voice Traffic** property **Use a separate VLAN** to define a VLAN ID for voice traffic. Note that the **Voice Traffic default router IP address** is calculated from the router IP address provided in the **Data Traffic** section.

Note:

*The default **VLAN ID** for Data Traffic is 2. The default **VLAN ID** for Voice Traffic is 3.*

6.7.3.1.2 Boards

When voice traffic has been assigned to a separate VLAN (see LAN Configuration section), the Boards page appears as follows:



In the LAN column, an icon indicates to which VLAN (data or voice) a board is associated.

The IP addresses defined for each board should be consistent with the network settings in the LAN Configuration page. To help you choose consistent addresses, the network and subnet mask IP addresses are explained beside each VLAN icon at the bottom of the page.

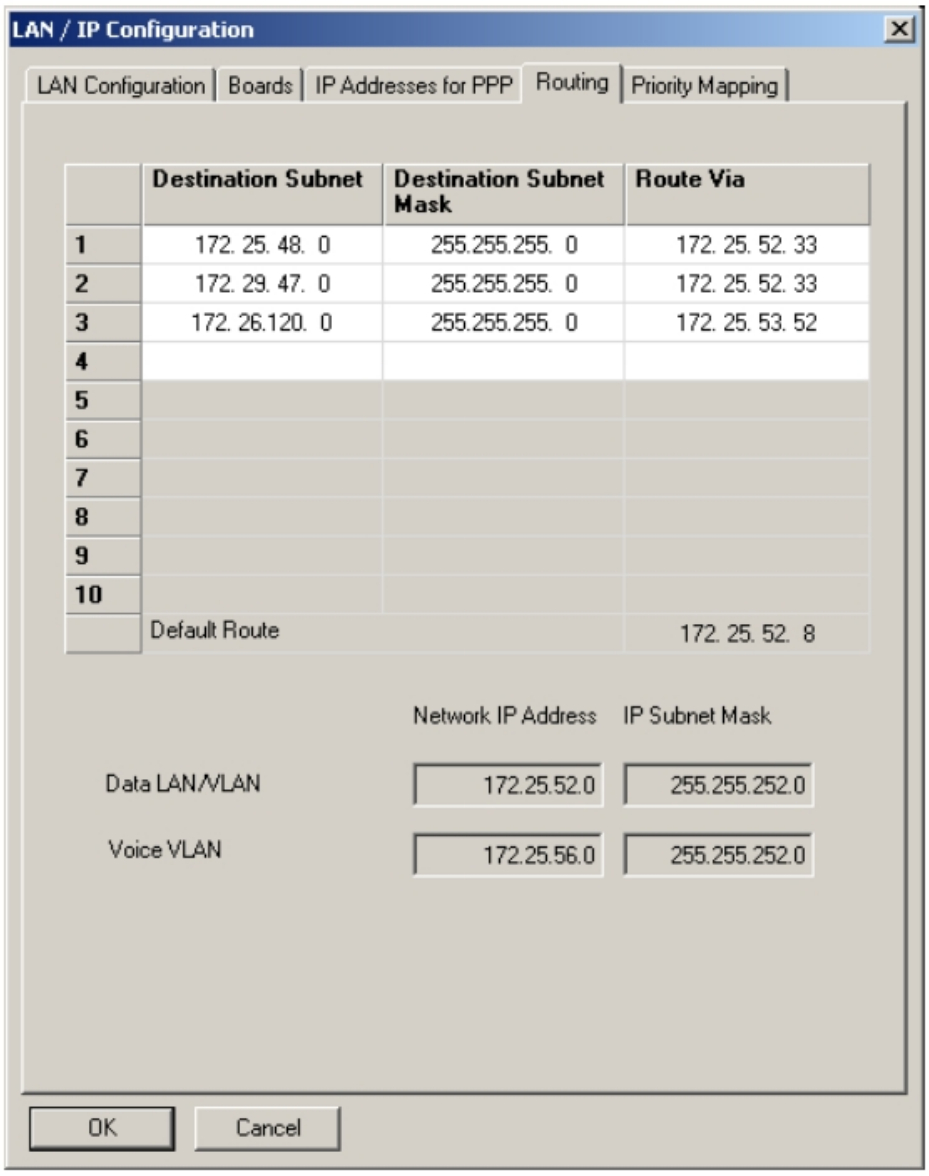
The "Main CPU" and "Main CPU (Voice)" fields have a particular behaviour. They can be used to modify the networks. Changes are reported to the LAN Configuration page for system consistency. In that case, all corresponding IP addresses associated to the same VLAN (data or voice) are automatically recalculated to match the new networks.

6.7.3.1.3 Routing

With the introduction of traffic segmentation, the main CPU can be connected to more than one LAN/VLAN. To send packets to a destination whose IP address is related to one of these LANs/VLANs, the main CPU only needs a network IP address and a subnet mask IP address. When the target destination lies beyond the main CPU's visible LANs/VLANs, a routing

decision must be taken.

In OMC R5.0, you can specify up to 10 routes. Each route is defined by a destination subnet (network IP address and subnet mask) and the IP address of the router via which the packets must be routed. This router must be visible from one of the LANs/VLANs to which the main CPU is connected. (See network IP addresses and subnet masks of voice and data VLANs at the bottom of the page.)



When Web Based Management (WBM) is active, it is used to define routing tables. In that case, the Routing page is disabled and displays no data.

6.7.3.1.4 Priority Mapping

This page allows mapping Diffserv code points (DSCP) to 802.1p Ethernet priority values.

802.1p priority

Standard Ethernet frame headers are made of the source and destination MAC address followed by a 2-byte length/type field. Tagged Ethernet frames include an extra 2 bytes in the header in order to support VLAN (802.1Q) and priority (802.1p) protocols. Three bits are available for priority, giving 8 possible priority values. Mapping is simple: 0 is the lowest priority and 7 is the highest.

IP ToS, precedence, and DSCP

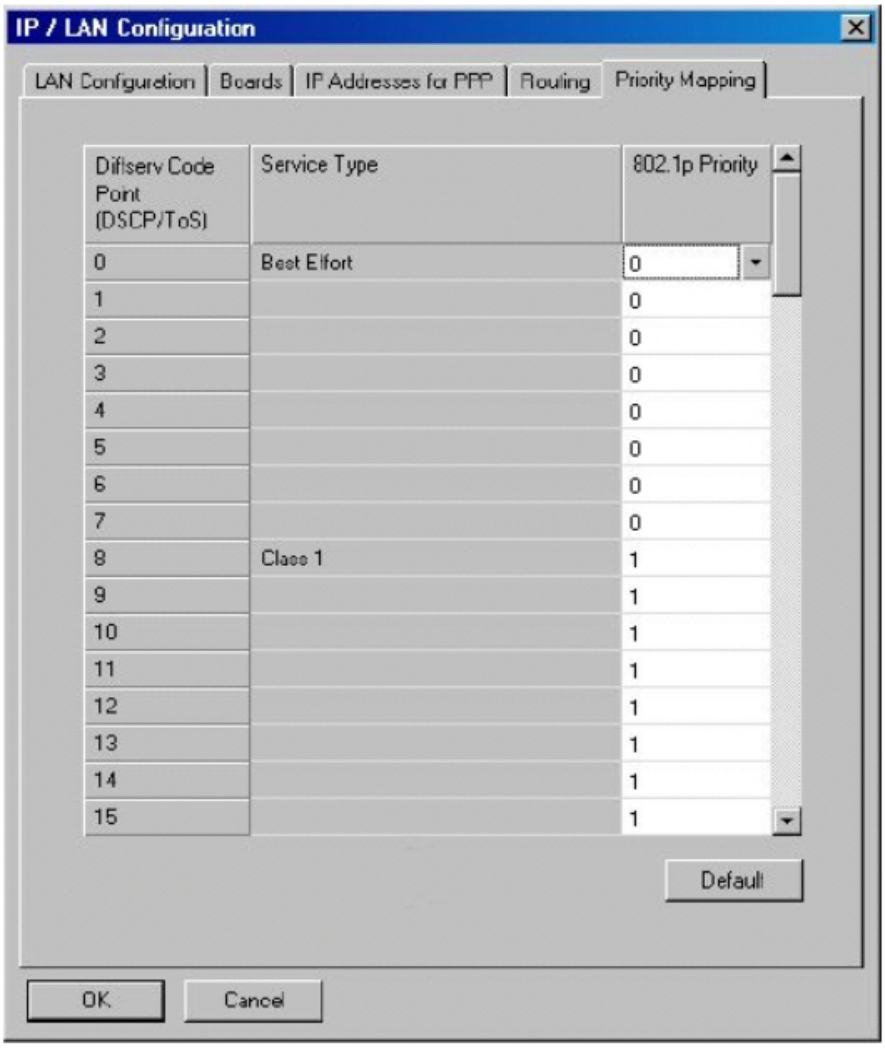
An IP packet header contains a byte called Type of Service. This byte contains several fields whose interpretation has evolved over the years. Initially interpreted as a 3-bit precedence value plus several ToS flags, the current interpretation uses the top 6 bits as a single value called the "Differential Services Code Point".

Remember the following points:

- DSCP can be interpreted as a 6-bit number
- The top 3 bits occupy the same position in the IP header as in the original definition of the "IP Precedence" field
- To keep a minimum compatibility with the older interpretation, DSCP values are organised into several classes of increasing priority. For example, the lowest priority class covers DSCPs 0 to 7
- The values within a class are not necessarily organised in order of increasing priority
- Some values have a specific meaning. For example: 0 means "Best Effort" (BE), 46 means "Expedited Forwarding" (EF), a high precedence DSCP often used for VoIP traffic
- The interpretation of DSCPs is not fully imposed. There is a notion of Diffserv domain and the DSCP code of a packet may change as it passes across a domain boundary

Priority mapping in OMC

As far as OMC is concerned, all that is required is to provide a way to determine the frame priority that should be used when an IP packet is transmitted through an Ethernet frame. In other words, you need to associate an 802.1p priority value (between 0 and 7) to each of the possible 64 DSCPs.



The "Service Type" column displays a description for the following DSCPs:

DSCP	**Description**
0	Best Effort (BE)
8	Class 1
16	Class 2
24	Class 3
32	Class 4
40	Express Forwarding
46	Expedited Forwarding (EF)
48	Control

56	Control

The default priority assignments are the following:

DSCP values	802.1p priority
0 - 7	0
8 - 15	1
16 - 23	2
24 - 31	3
32 - 39	4
40 - 47	5
48 - 55	6
56 - 63	7

6.8 Dimensioning

6.8.1 Detailed description

6.8.1.1 SYSTEM SIZING

Information in this chapter is valid for releases of Alcatel-Lucent OmniPCX Office Communication Server:

- prior to R6.0, which do not include the direct RTP feature
- R6.0, without direct RTP
- The same system sizing principles applies to both and are presented as *Case of DSP channels required without direct RTP*.
- R6.0, with direct RTP activated
- System sizing principles are presented as *Case of DSP channels required with direct RTP*.

6.8.1.1.1 DSP channels required for IP Trunk services

Number of DSPs = Number of VoIP network accesses = 96 max.

6.8.1.1.2 DSP channels required by VoIP services

The number of DSP channels (VoIP ports) required depends on the system configuration and the VoIP services to be implemented.

The most common situations are the following:

- H.323/SIP gateway only: the number of DSP channels is equal to the number of IP network accesses.

  Note:
  The desired number of DSP channels can be limited by the bandwidth reserved for VoIP accesses. Example: if the reserved bandwidth is 64 KBps, only 2 calls can be made simultaneously; the number of VoIP accesses can thus be limited to 2 channels.

- IP Telephony only
- Conventional telephony (Reflexes / DECT / Z, etc.) and IP Telephony
- H.323/SIP gateway and IP Telephony

6.8.1.1.3 Case of DSP channels required with direct RTP

Note 1:

Information in this section concerns Alcatel-Lucent OmniPCX Office Communication Server R6.0 and higher.

The direct RTP feature enables direct audio paths between IP sets and distant gateways or IP sets. Certain VoIP services no longer necessitate an allocation of a DSP channel.

A selection of typical configurations examples in the table below shows how to calculate DSP needs.

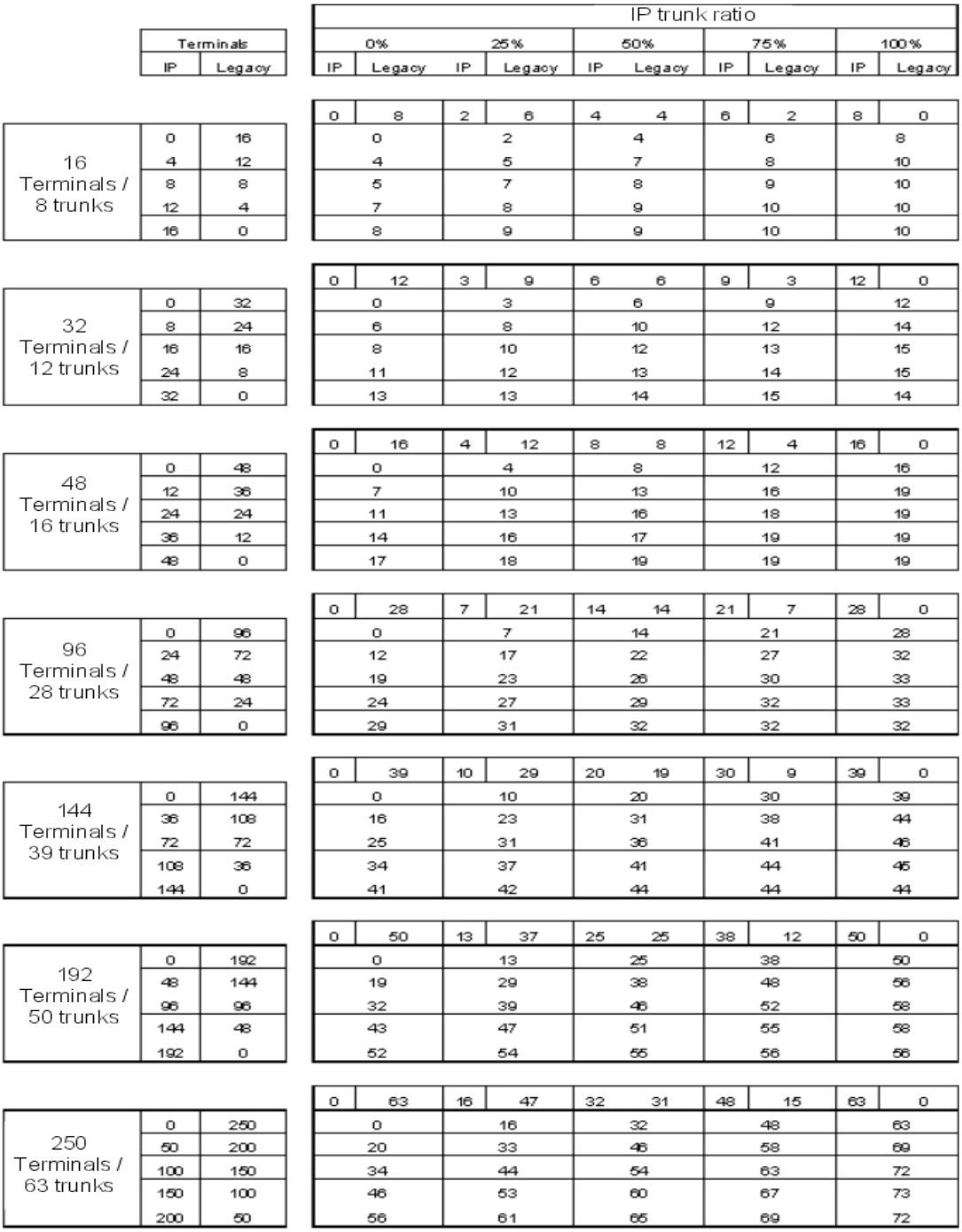
figure : DSP channel needs with direct RTP illustrates how direct RTP decreases the need for DSP channels.

From left to right, columns show:

- the number of terminals and the number of trunks **necessary**
- the mix of IP terminals and legacy sets in numbers
- for a given ratio of IP/Legacy trunks in the configuration, the number of necessary DSP channels

Note 2:

Configuration possibilities are not limited to the examples given in the table.



	Terminals		IP trunk ratio									
			0%		25%		50%		75%		100%	
	IP	Legacy	IP	Legacy	IP	Legacy	IP	Legacy	IP	Legacy	IP	Legacy
16 Terminals / 8 trunks	0	16	0	8	2	6	4	4	6	2	8	0
	4	12	0	2		4		6		8		
	8	8	4	5		7		8		10		
	12	4	5	7		8		9		10		
	16	0	7	8		9		9		10		
			8	9								
32 Terminals / 12 trunks	0	32	0	12	3	9	6	6	9	3	12	0
	8	24	0	3		6		9		12		
	16	16	6	8		10		12		14		
	24	8	8	10		12		13		15		
	32	0	11	12		13		14		15		
			13	13		14		15		14		
48 Terminals / 16 trunks	0	48	0	16	4	12	8	8	12	4	16	0
	12	36	0	4		8		12		16		
	24	24	7	10		13		16		19		
	36	12	11	13		16		18		19		
	48	0	14	16		17		19		19		
			17	18		19		19		19		
96 Terminals / 28 trunks	0	96	0	28	7	21	14	14	21	7	28	0
	24	72	0	7		14		21		28		
	48	48	12	17		22		27		32		
	72	24	19	23		26		30		33		
	96	0	24	27		29		32		33		
			29	31		32		32		32		
144 Terminals / 39 trunks	0	144	0	39	10	29	20	19	30	9	39	0
	36	108	0	10		20		30		39		
	72	72	16	23		31		38		44		
	108	36	25	31		36		41		46		
	144	0	34	37		41		44		45		
			41	42		44		44		44		
192 Terminals / 50 trunks	0	192	0	50	13	37	25	25	38	12	50	0
	48	144	0	13		25		38		50		
	96	96	19	29		38		48		56		
	144	48	32	39		46		52		58		
	192	0	43	47		51		55		58		
			52	54		55		56		56		
250 Terminals / 63 trunks	0	250	0	63	16	47	32	31	48	15	63	0
	50	200	0	16		32		48		63		
	100	150	20	33		46		58		69		
	150	100	34	44		54		63		72		
	200	50	46	53		60		67		73		
			56	61		65		69		72		

Figure 6.33 : DSP channel needs with direct RTP

Note 3:

The total number of DSP channels to be implemented for IP Telephony and/or IP network access will be

incremented to the next highest value out of the possible combinations of DSPs present in the system (reminder: a VoIP daughter board supports 4, 8 or 16 DSPs; the system contains from 4 to 96 DSPs, by steps of 4).

6.8.1.1.4 Case of DSP channels required without direct RTP

figure : DSP channel needs with no direct RTP below illustrates DSP channels required by VoIP services and shows how to calculate DSP needs.

From left to right, columns show:

- the number of terminals and the number of trunks **necessary**
- the mix of IP terminals and legacy sets in numbers
- for a given ratio of IP/Legacy trunks in the configuration, the number of necessary DSP channels

Note 1:

Configuration possibilities are not limited to the examples given in the table.

	Terminals		IP trunk ratio									
			0%		25%		50%		75%		100%	
	IP	Legacy	IP	Legacy	IP	Legacy	IP	Legacy	IP	Legacy	IP	Legacy
16 Terminals / 8 trunks	0	16	0	8	2	6	4	4	6	2	8	0
	4	12	0	2			4	6			8	10
	8	8	4	6			8	10			12	14
	12	4	5	7			9	11			13	15
	16	0	7	9			11	13			15	17
			8	10			12	14			16	18
32 Terminals / 12 trunks	0	32	0	12	3	9	6	6	9	3	12	0
	8	24	0	3			6	9			12	15
	16	16	6	9			12	15			18	21
	24	8	8	11			14	17			20	23
	32	0	11	14			17	20			23	26
			13	16			19	22			25	28
48 Terminals / 16 trunks	0	48	0	16	4	12	8	8	12	4	16	0
	12	36	0	4			8	12			16	20
	24	24	7	11			15	19			23	27
	36	12	11	15			19	23			27	31
	48	0	14	18			22	26			30	34
			17	21			25	29			33	37
96 Terminals / 28 trunks	0	96	0	28	7	21	14	14	21	7	28	0
	24	72	0	7			14	21			28	35
	48	48	12	19			26	33			40	47
	72	24	19	26			33	40			47	54
	96	0	24	31			38	45			52	59
			29	36			43	50			57	64
144 Terminals / 39 trunks	0	144	0	39	10	29	20	19	30	9	39	0
	36	108	0	10			20	30			39	49
	72	72	16	26			36	46			55	65
	108	36	25	35			45	55			64	74
	144	0	34	44			54	64			73	83
			41	51			61	71			80	90
192 Terminals / 50 trunks	0	192	0	50	13	37	25	25	38	12	50	0
	48	144	0	13			25	38			50	63
	96	96	19	32			44	57			69	82
	144	48	32	45			57	70			82	95
	192	0	43	56			68	81			93	106
			52	65			77	90			102	115
250 Terminals / 63 trunks	0	250	0	63	16	47	32	31	48	15	63	0
	50	200	0	16			32	48			63	79
	100	150	20	36			52	68			83	99
	150	100	34	50			66	82			97	113
	200	50	46	62			78	94			109	125
			56	72			88	104			119	135

Figure 6.34 : DSP channel needs with no direct RTP

Note 2:

The total number of DSP channels to be implemented for IP Telephony and/or IP network access will be incremented to the next highest value out of the possible combinations of DSPs present in the system (reminder: a VoIP daughter board supports 4, 8 or 16 DSPs; the system contains from 4 to 96 DSPs, by steps of 4).

6.8.2 Configuration examples

6.8.2.1 H.323/SIP gateway only

Note:
*Configuration possibilities are **not** limited to the example given in this section.*

- 1 Attendant station (non-IP)
- 40 Reflexes stations (non-IP)
- 5 T0 accesses
- 6 VoIP network accesses (example: 2 to site A with a bandwidth = 64 KBps and 2 accesses to site B with a bandwidth = 64 KBps plus 2 other channels for NetMeeting PCs)

As all the DSP channels are associated with the H.323/SIP gateway (no IP telephony), the number of DSP channels needed for this configuration corresponds to the number of VoIP accesses, i.e. 6 (increased to 8).

6.8.2.2 Small IP Telephony configuration

Note:
*Configuration possibilities are **not** limited to the example given in this section.*

- 1 Attendant station (non-IP)
- 16 IP sets
- 3 T0 (=6 channels)

The average number of DSPs needed for this configuration is 8.

6.8.2.3 Large IP telephony configuration

Note:
*Configuration possibilities are **not** limited to the example given in this section.*

- 1 Attendant station (non-IP)
- 70 IP sets
- 1 T2 access with 30 channels

The average number of DSPs needed for this configuration is 23, (increased to 24).

6.8.2.4 Average configuration in mixed telephony: IP and conventional telephony (DECT/PWT)

Note:
*Configuration possibilities are **not** limited to the example given in this section.*

- 1 Attendant station (non-IP)

- 25 IP sets
- 25 DECT/PWT stations
- 6 T0 accesses

The average number of DSPs needed for this configuration is 12.

6.8.2.5 Average configuration in mixed telephony: IP and conventional telephony (Reflexes)

Note:
*Configuration possibilities are **not** limited to the example given in this section.*

- 1 Attendant station (non-IP)
- 5 IP sets
- 40 conventional Reflexes stations
- 6 T0 accesses

The number of DSPs needed for this configuration is 4.

6.8.2.6 Medium configuration for mixed telephony + H.323/SIP gateway

Note:
*Configuration possibilities are **not** limited to the example given in this section.*

- 1 Attendant station (non-IP)
- 5 IP sets
- 40 conventional Reflexes stations
- 4 T0 accesses
- 5 VoIP network accesses
- The number of DSP channels needed for IP telephony is Min(5,9) = 5
- The H.323/SIP gateway requires 5 additional DSP channels

The average number of DSPs needed for this configuration is 9 (increased to 12).

6.8.2.7 Bandwidth

In an H.323/SIP gateway configuration, a bandwidth can be associated with each ARS table entry to a remote H.323/SIP gateway.

Number of DSPs depending on call type:

- PIMphony IP or IP Phone
  - IP Phone - IP Phone: 0 DSP
  - IP Phone in conference: 1 DSP
  - IP Phone or PIMphony IP - Reflexes station or analogue/ISDN network: 1 DSP
  - IP Phone or PIMphony IP - PC H323 or H323 gateway (IP trunk): 2 DSPs
- PC - PC: 0 DSP
- PC with internal H323 gateway - PC with internal H323 gateway: 1 DSP

The following table indicates the potential number of simultaneous calls depending on the

bandwidth reserved for VoIP calls:

Data rate (bandwidth)	Number of possible simultaneous communications	CODEC used
55.6 Kbps (or less)	1	G.723.1/G729a
64 Kbps	2	G.723.1/G729a
128 Kbps	5	G.723.1/G729a
256 Kbps	10	G.723.1/G729a
512 Kbps	20	G.723.1/G729a
= 1024 Kbps	Depends on the number of IP trunks	G.723.1/G729a

6.8.3 Limits

6.8.3.1 VoIP services

Voice over IP services require a software key.

6.8.3.2 VoIPx-1 on main CPU

- Main CPU always master VoIP board
- Maximum 5 VoIP CoCPU boards in addition
- VoIP4-1,VoIP8-1 or VoIP16-1 on main CPU

Caution:

The module's slot #8 can only be used for a LANX board because the VoIP-1 daughter board on the main CPU board consumes switching resources used for slot 8.

6.8.3.3 VoIP CoCPU/CoCPU-1/CoCPU-2 board

There can be a maximum of 6 boards in a system: one "master" board and five "slave" boards.

The "master" VoIP CoCPU/CoCPU-1/CoCPU-2 board will be the first board seen by the system. If a VoIP CoCPU/CoCPU-1/CoCPU-2 board is added to the system, it will be considered as a "slave" board.

A VoIP CoCPU/CoCPU-1/CoCPU-2 board is equipped with a daughter board of 4, 8 or 16 DSPs maximum.

An Alcatel-Lucent OmniPCX Office Communication Server can contain a maximum of 96 DSPs.

If there is more than one VoIP CoCPU/CoCPU-1/CoCPU-2 board in a system, each of the Ethernet ports of each board must be connected to the LAN and they must be connected to the same subnet.

It is possible to combine VoIP CoCPU/CoCPU-1/CoCPU-2 boards with a different number of DSPs: if the system combines the IP Telephony and H.323/SIP Gateway services, it is strongly recommended for the board with the largest number of DSPs to be the "master" board and that its IP address should be used as the reference for the remote H.323/SIP gateways.

The VoIP CoCPU/CoCPU-1/CoCPU-2 boards are to be connected via a LAN Switch: this solution reduces Ethernet access traffic.

6.8.3.4 DSP channels

After a cold reset, all the DSPs of the VoIP CoCPU/CoCPU-1/CoCPU-2 board are assigned to the VoIP subscriber channel pool by default. The DSP assignment can be modified using OMC.

Any DSP assigned to the VoIP access pool is removed from the VoIP subscriber pool: it will therefore no longer be available for IP telephony. Conversely, a DSP from the VoIP user pool will not be able to be used for H.323/SIP gateway calls.

6.8.3.5 IP sets

The theoretical limit on the number of IP sets + PIMphony IP stations that can be connected is 200, however:

- It is compulsory for the operator station to be a Reflexes station connected to a UA link, which means that at least one UAI board must be installed in the system
- The IP sets are "deducted" from the limit on Reflexes stations

The Ethernet access of an IP set is at 10 or 10/100 MBps.

6.8.3.6 "VoIP Access" channels: H.323/SIP gateway

A DSP channel of a VoIP CoCPU/CoCPU-1/CoCPU-2 board assigned to the pool of VoIP access channels is considered by the system to be a public network access, that is to say "1 B channel".

Alcatel-Lucent OmniPCX Office Communication Server can have a maximum of 120 public network accesses: the maximum number of DSPs assigned to the VoIP access pool is 96.

Network accesses (T0, T2, DLT2, DLT0, TL) + VoIP accesses = 120 max. accesses

6.8.3.7 ARS entry

The number of entries in the ARS table with a remote H.323/SIP gateway as destination is limited to 200.

The number of entries in the ARS table that make reference to a PC (individual entry or with a range) is limited to 150.

6.9 Maintenance

6.9.1 VoIP Boards

6.9.1.1 Maintenance

6.9.1.1.1 VoIP SERVICES - CoCPU BOARD

System with a single CoCPU board equipped with a VoIP daughter board

If the CoCPU board equipped with a daughter board is out of service, none of the VoIP services (H.323/SIP gateway and IP Telephony) is available.

Resetting the H.323/SIP gateway (CoCPU board equipped with a VoIP daughter board reset) releases all ongoing communications on the H.323 gateway; reinitialising the IP telephony service resets all the IP sets and the communications in progress on the Multimedia PCs.

Modifying the IP address associated with the CoCPU board equipped with a VoIP daughter board resets the board and all the ongoing VoIP services.

System with several CoCPU boards equipped with a VoIP daughter board

If the "master" CoCPU board equipped with a VoIP daughter board is out of service, all the VoIP services (H.323/SIP gateway and IP Telephony) are temporarily unavailable. The PBX "switches" the VoIP services over to a "slave" CoCPU board equipped with a VoIP daughter board: the system assigns it the IP address of the faulty board (reference address for the VoIP services: H.323/SIP gateway, TFTP server, etc.), thereby enabling the VoIP services to be maintained (the number of possible VoIP communications will however be limited to the number of DSPs remaining).

After replacing the faulty CoCPU board equipped with a VoIP daughter board, it will automatically be assigned the old IP address, which is now free, of the new "master" CoCPU board equipped with a VoIP daughter board: the new board will be "slave"; the system does not return to the pre-failure configuration.

Note:
It is recommended that the "master" CoCPU board equipped with a VoIP daughter board of a PBX should be the one that has the largest number of DSPs. For systems with 2 boards, such as a CoCPU board equipped with a VoIP daughter board with 16 DSPs and a CoCPU board equipped with a VoIP daughter board with 4 DSPs, if the 4-DSP CoCPU board equipped with a VoIP daughter board has become the system "master" board following a fault affecting the 16-DSP CoCPU board equipped with a VoIP daughter board, then you should return to the original configuration after replacing the 16-DSP CoCPU board equipped with a VoIP daughter board by unplugging the 4-DSP CoCPU board equipped with a VoIP daughter board for a few minutes.

The CoCPU boards equipped with a VoIP daughter board cannot be plugged or unplugged on a powered-up system.

If a "slave" CoCPU board equipped with a VoIP daughter board is out of service, all the VoIP services will be redirected to the "master" CoCPU board equipped with a VoIP daughter board. However, the number of possible VoIP calls will be limited to the number of DSPs remaining.

6.9.2 IP Telephony

6.9.2.1 Maintenance

6.9.2.1.1 Loss of IP connectivity

It takes several seconds to detect a loss of connection: the IP set attempts to restore the connection for several seconds. During this period the user may observe a slowing in the station displays resulting from repeated restoring and loss of connections.

6.9.2.1.2 Multimedia PC

If the "keep alive" mechanism detects a problem between a NetMeeting PC and the system (PBX reset, CoCPU board equipped with VoIP daughter board reset, IP connectivity problems), NetMeeting sends the user an error message: the user can either quit the application or wait to be reconnected.

6.9.2.1.3 Alcatel-Lucent 8 series stations: error messages

See module IP Touch 4008/4018 Phone - Maintenance and module IP Touch 4028/4038/4068 Phone - Maintenance .

6.9.3 Service Alarm Messages

6.9.3.1 Maintenance

The NMC (Network Management Center) application Alcatel-Lucent 4740/4760 enables the following alarm messages specific to Voice over IP to be retrieved:

- Reset of xxxxx CoCPU board equipped with a VoIP daughter board (message identical to those of the other boards in the system).
- xxxxx CoCPU board equipped with a VoIP daughter board out of service.
  - Diagnosis: reset and/or replace the board.
- DSP of xxxxx CoCPU board equipped with a VoIP daughter board out of service.
  - Diagnosis: reset and replace the CoCPU board equipped with a VoIP daughter board if the fault persists or recurs.
- Ethernet interface of xxxxx CoCPU board equipped with a VoIP daughter board out of service.
  - Diagnosis: check the connection to the LAN and possibly the LAN components (Hub, switch, etc.).
- Ethernet interface of xxxxx CoCPU board equipped with a VoIP daughter board in service.
- Remote gateway xxxxx Out of Service.
  - Diagnosis: check the IP connectivity with the remote gateway (LAN, intermediate IP router) and the status of the remote gateway.
- Remote gateway xxxxx In Service.
- Automatic overflow: too much traffic to/from remote gateway xxxxx.
  - Diagnosis: if this alarm occurs frequently, the bandwidth associated with this remote gateway in the ARS table and the number of DSPs assigned to VoIP accesses must be increased if possible.
- Automatic overflow: VoIP call to/from gateway xxxxx refused because "not enough VoIP access channels available".
  - Diagnosis: if this alarm occurs frequently, the sizing of the DSPs must be reviewed: either the bandwidth in the ARS table must be increased, or the number of DSPs assigned to VoIP accesses must be increased, or another CoCPU board equipped with a VoIP daughter board must be added.
- IP Telephony failures: no more DSP channels available.
  - Diagnosis: if this alarm occurs frequently, the number of DSPs assigned to the IP subscriber pool must be increased (either by reducing the number of VoIP access DSPs or by adding a CoCPU board equipped with a VoIP daughter board).
    This alarm is generated every 10th (value by default) allocation failure.
- The IP set cannot be initialised because of a DHCP server fault (no IP addresses available).
  - Diagnosis: increase the number of IP addresses in the DHCP server range (this range of IP addresses must be greater than or equal to the number of IP sets to be installed).

6.9.4 Service Traffic Counters

6.9.4.1 Maintenance

The VoIP services feature the following specific traffic counters accessible via OMC in the menu: **System Miscellaneous -> VoIP -> Traffic counters**

6.9.4.1.1 "General" tab:

- Number of incoming VoIP calls
- Number of outgoing VoIP calls
- Number of transiting VoIP calls (Break In, Break Out)
- Number of outgoing VoIP calls to remote gateway xxxxx refused because "all VoIP access channels busy"
- Number of incoming VoIP calls to gateway xxxxx refused because "all VoIP access channels busy"
- Number of failed IP Telephony (audio) calls: all the DSP channels reserved for IP Telephony are busy

6.9.4.1.2 "Gateways" tab:

These counters indicate the number of VoIP calls to each of the remote VoIP gateways refused for the following reasons:

- Overflow on outgoing VoIP calls: CoCPU board(s) equipped with VoIP daughter board out of service
- Overflow on outgoing VoIP calls: no more bandwidth available
- Incoming VoIP calls refused: no more bandwidth available

Chapter 7

Private Networks

7.1 General Presentation

7.1.1 Overview

7.1.1.1 THE NETWORK OFFERING

7.1.1.1.1 Global offering

Depending on the medium (or protocol) used, placing Alcatel-Lucent OmniPCX Office Communication Server systems on private networks offers the following main services:

- Calls on ISDN, QSIG and VPN lines: CLIP/COLP services, conversion into private dialling for outgoing and incoming calls.
- Public or Private ISVPN: in addition to the previous services, optimisation of transfers and forwarding, additional information (transmission of the name, busy status, forwarding).
- ISVPN+: with regard to ISVPN services, addition of tracking call record information.
- IP Networking: setting up an IP network using the existing data network to carry voice data at lower cost; for more details see the "Voice over IP" section.

The table below shows the principles of use for the various protocols, depending on the amount of traffic and the requested level of service.

<table>
<tr><td></td><td colspan="3">Integration of services →</td></tr>
<tr><td rowspan="3">Voice traffic ↓</td><td>ISDN</td><td>Heterogeneous ISVPN</td><td>Public ISVPN</td></tr>
<tr><td></td><td>VPN</td><td>Public VPN + ISVPN</td></tr>
<tr><td>QSIG</td><td></td><td>Private ISVPN
ISVPN+</td></tr>
<tr><td>Voice + data traffic</td><td colspan="2">IP Networking</td><td></td></tr>
</table>

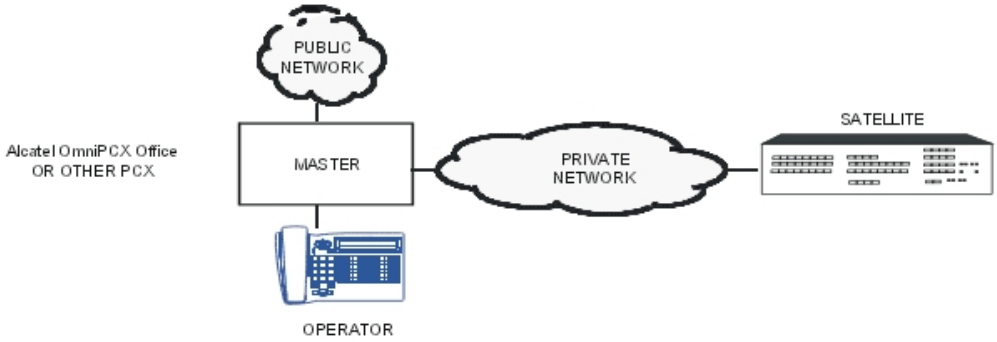
A private network can be homogenous or heterogeneous:

- Homogenous: all PCXs in the network belong to the same family (Alcatel-Lucent OmniPCX Office Communication Server or Alcatel-Lucent OmniPCX Enterprise Communication Server).
- Heterogeneous: the PCXs in the network belong to different families (Alcatel-Lucent and others).

7.1.1.1.2 DEFINITIONS

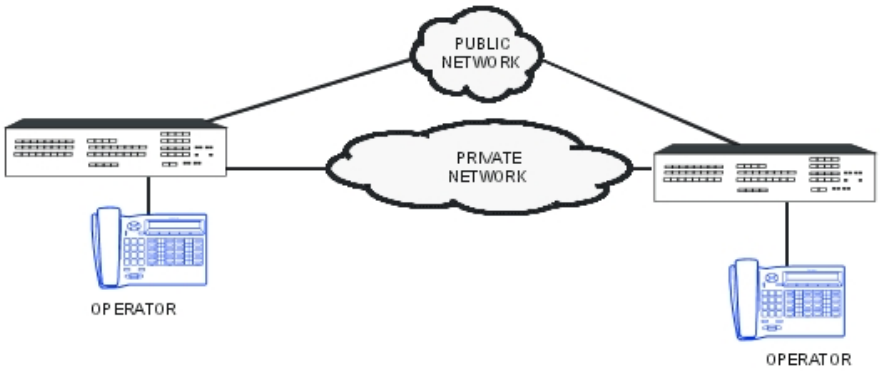
MASTER/SATELLITE CONFIGURATION

Only the master system has an Attendant station and external access connected to the public network. The satellite system uses the master system's external resources. Several satellite systems can be connected to the same master system.



PEER TO PEER CONFIGURATION

In this topology, the 2 Alcatel-Lucent OmniPCX Office Communication Server systems each have their own Attendant Station and their own external accesses.



DIGITAL PROTOCOLS

The following protocols can be used:

- QSIG_BC (QSIG Basic Call): protocol managing exchanges between private networks at basic communication level.
- ISVPN: Alcatel-Lucent proprietary protocol = standard ISDN protocol + additional information by means of UUS (User to User Signalling).
  - on public lines: public ISVPN
  - on leased lines: private ISVPN
- ISVPN+: Alcatel-Lucent proprietary protocol = ISVPN + additional information contained in the UUS. This protocol can only be used with Alcatel-Lucent OmniPCX Office Communication Server systems. The additional information can only be used by an Alcatel-Lucent 4740 or Alcatel-Lucent 4760 Management Center.

7.1.1.1.3 ENVIRONMENTS

Note:

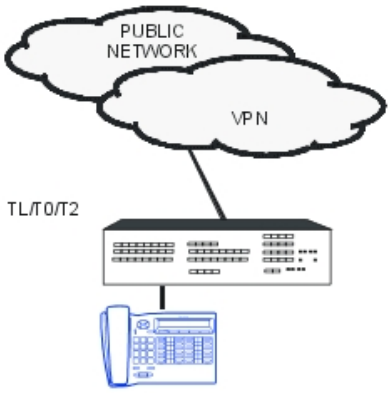
The DLT0/2 - analogue trunk interconnection must be implemented with precaution in order to avoid any analogue trunk blocking (e.g. a break-in by transfer between an analogue trunk

without polarity inversion and a DLT0/2 joining on a remote user forwarded to an external number by another analogue trunk; in this case, there is no release of calls on these analogue trunks).

VPNs ON PUBLIC LINKS

These virtual networks are specific to the country and the network attendant. In these networks, which use the public carrier protocols (analogue or ISDN), private and public calls are routed on the same lines. Among these networks are:

- Fiat in Italy: analogue or ISDN protocol
- Transgroupe (Collisée Performance) in France: ISDN protocol only



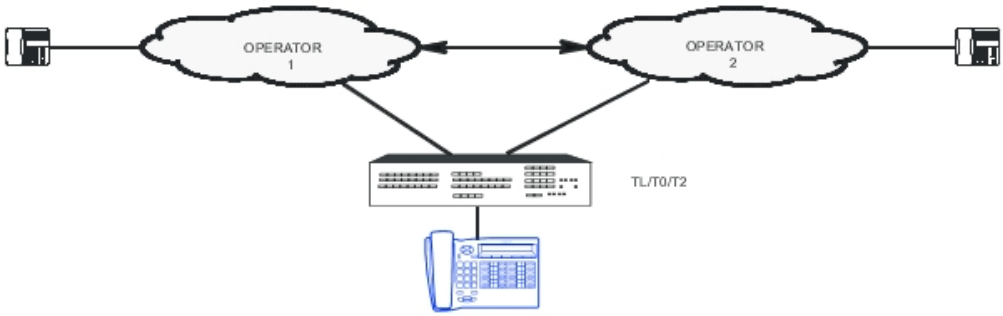
Characteristics of Transgroupe dialling (France only)

- public numbers are preceded by 0.
- private numbers are defined in a private numbering plan: closed dialling from 5 to 10 digits) with short numbers as an option (10 to 15, 160 to 169, 36XX).

MULTI-CARRIER OPERATION

The system has 2 direct accesses with different exchange carriers. With the ARS mechanisms, this environment enables:

- use of the cheapest exchange carrier to call a party.
- overflowing through the other exchange carrier when the cheapest one is unavailable.

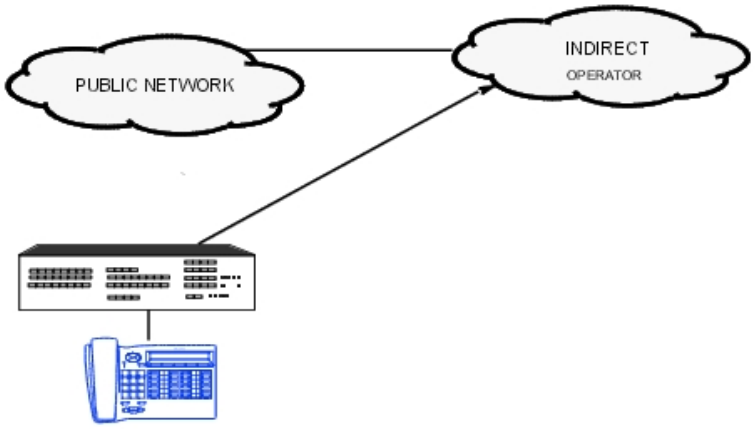


INDIRECT attendant

This environment makes it possible to redirect calls to exchange carriers offering attractive rates, for international calls or calls to GSM for example.

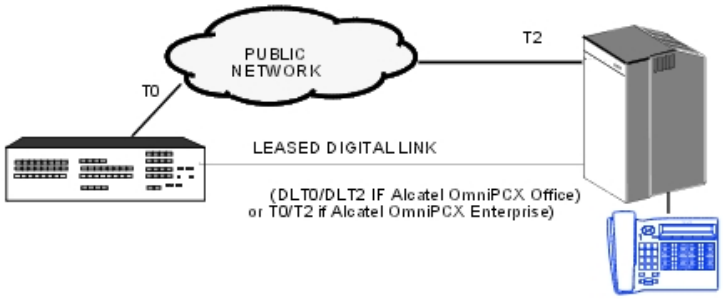
Depending on the analysis of the requested number, the ARS automatically redirects the call, transparently for the user, to another indirect substitution network and then retransmits the destination number as follows:

- seizure of a line in the network of the primary carrier
- dialling the access code or the number of the indirect carrier
- waiting for an intermediary tone (or pause)
- switching into transparent MF dialling
- optional transmission of the account code (waiting for a 2nd tone or pause)
- optional waiting for a second intermediary tone (or pause)
- dialling the destination call number



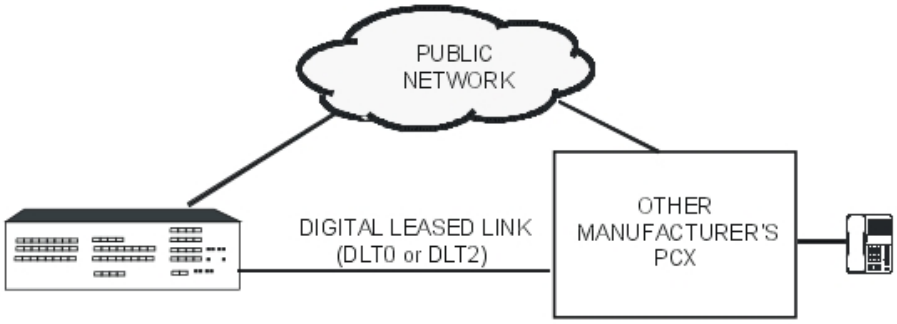
ISVPN ON LEASED/PUBLIC LINKS

Using the proprietary ISVPN protocol on leased digital links makes it possible to connect an Alcatel-Lucent OmniPCX Office Communication Server system with an Alcatel-Lucent OmniPCX Enterprise Communication Server system or another Alcatel-Lucent OmniPCX Office Communication Server system.



QSIG-BC

The QSIG protocol on digital leased links can be used for interconnecting an Alcatel-Lucent OmniPCX Office Communication Server with a system from another manufacturer if compatible with QSIG_BC (Basic Call).



7.1.2 Services provided

OPTIMIZED FORWARDING AND TRANSFER (digital networks only)

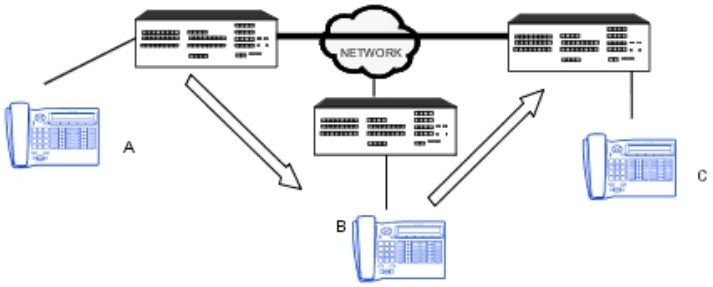
The path used by a call can be optimized in the following cases:

- immediate forwarding
- external dynamic forwarding
- external forwarding of operator calls
- transfer

Optimized immediate forwarding

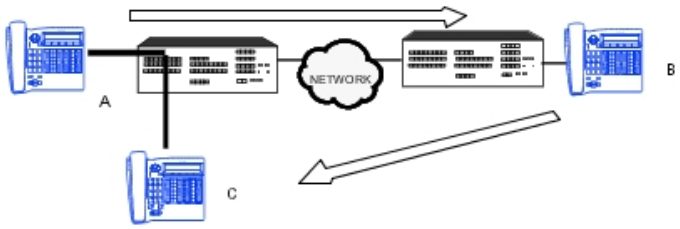
Optimization of the path is carried out by rerouting the call.

- Optimisation of the path between 3 nodes



A (1st node) calls B (2nd node) forwarded on C (3rd node). The result of the optimization corresponds to a direct call from A to C.

- Optimisation of the path between 2 nodes



A (1st node) calls B (2nd node) forwarded on C (1st node). The result of the optimization corresponds to a local call from A to C.

Note 2:

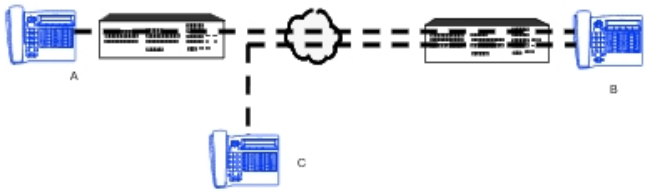
If the forwarding destination calls the forwarding initiator, then the forwarding is overridden.

A parameter (OMC -> System Miscellaneous -> Feature Design -> Part 5) allows to define the maximum number of successive forwardings (transmissions threshold: 5 by default).

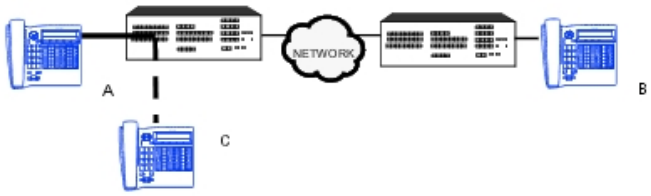
Optimized transfer

The optimization mechanism is applied when the 2 external correspondents are on the same ISVPN node; the transfer can be monitored (connected) or not (on ringer).

Situation: B (master) is in communication with 2 correspondents (A and C) on the same system.



Optimisation: the 2 communications are released and resynchronized on the remote system: a local call is made from A to C.



NETWORK FORCING (forced dialing)

For reasons of cost, a call from a public network user can be made to use private links as a priority, followed by public lines if the private network is completely busy (ARS configuration).

OVERFLOW

When a destination can be joined in several ways and one of the paths fails (no more resources available for example), the ARS automatically tries to take another path (private network -> public network or vice versa, from one public operator to another).

Overflow is controlled by the barring and traffic sharing mechanisms.

Overflow can also be applied to data communications.

BREAK-IN / BREAK-OUT (INCOMING TRANSIT / OUTGOING TRANSIT)

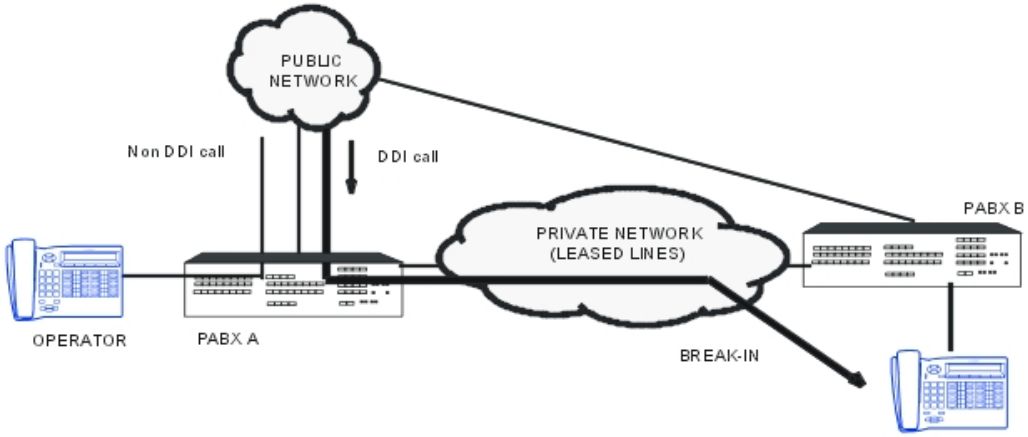
Break-in and break-out services make it possible to carry out inter-establishment communications from a private network; this is realized with the use of lines leased between 2 or more PCXs belonging to this private network.

Break-in (Incoming Transit)

This service corresponds to the transit of incoming calls from the public network to a private network via leased lines; thus, an external correspondent can join a private network user who is not connected to the same system as the line on which the call is routed.

Break-in can be implemented in 2 ways:

- automatically by DDI numbers
- manually by the operator (joining by transfer)



For the caller, it is also possible to set up a simple directory (a single group of numbers to call all users from one or several sites).

Manual break-in

This is a joining by transfer between an incoming T0/T2 access or a TL and a leased line.

In this case, the external correspondent accesses the line leased between PCXs A and B only through an operator (or a station); the operator of PCX A puts the caller on hold, establishes an enquiry call communication (seizure of the leased line + number of the remote subscriber) then carries out a transfer.

Settings:

- According to the environment (analog/digital), authorize the various joinings between external lines:

• by OMC (Expert View), select: **System Miscellaneous**-> **Traffic Sharing and Barring** -> **Joining** ->check the boxes to authorize the necessary joinings.

- At system level, authorize external/external transfers: select

• by OMC (Expert View) select: **System Miscellaneous** -> **Feature Design** -> check Transfer Ext/Ext

- For each station, authorize external/external manual transfers: select

• by OMC (Expert View) select: **Subscribers/Base stations List**-> **Subscribers/Base stations List** -> **Details**-> **Features** -> check "Join Incoming and Outgoing" and "Join Outgoing and Outgoing".

Automatic break-in

The public network correspondent joins a remote system subscriber using his DDI number. This service is only offered for calls routed on T0 or T2 and on customized TL (analog network line under call distribution).

Configuring with OMC:

The numbering plan for public incoming calls and ARS mechanisms enable correspondence between the DDI number coming from the public network and the subscriber (or hunting

group) directory number in the private network.

Note 3:

- if the break-in call fails, the call is handled depending on the configuration of the analog protocol or the table corresponding to incoming calls for digital leased lines (forwarded to operator or released).
- manual call pick-up (with RSP key) from a member of the operator hunting group is impossible in call phase (before remote connection or re-routing to operator).
- distribution of a welcome message on a break-in call is impossible.

Break-out/Proximity break-out

- Break-out (Outgoing Transit)

A break-out makes it possible for the user of PCX A to call, via leased lines, a public network user by using lines external to PCX B.

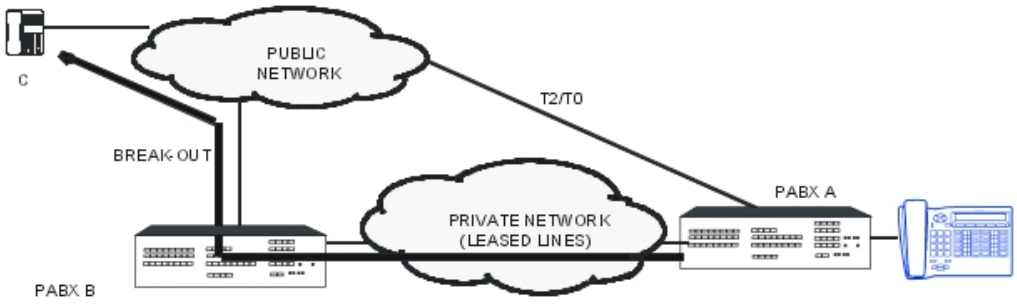
- Proximity break-out

A proximity break-out is a special use of the break-out: a call to the public network can be guided in order to exit via the public accesses which are closest to the destination.

Example: a PCX A user (STRASBOURG) calls C (PARIS); the call is redirected on the private network between PCXs A and B (PARIS) in such a way that it exits via B's public accesses.

This feature makes it possible to offer communications which are advantageous from a cost point of view; there are 2 ways of calling a public user from A:

- direct call by the public network; in this case, the communication is charged as a national communication.
- exit via B; thanks to the line leased between the 2 PCXs, only the part of the call from PCX B is charged as a local communication.



The following break-outs are possible:

- incoming call on leased line -> ISDN
- incoming call on leased line -> analogue public network

The break-out can be implemented in 2 ways:

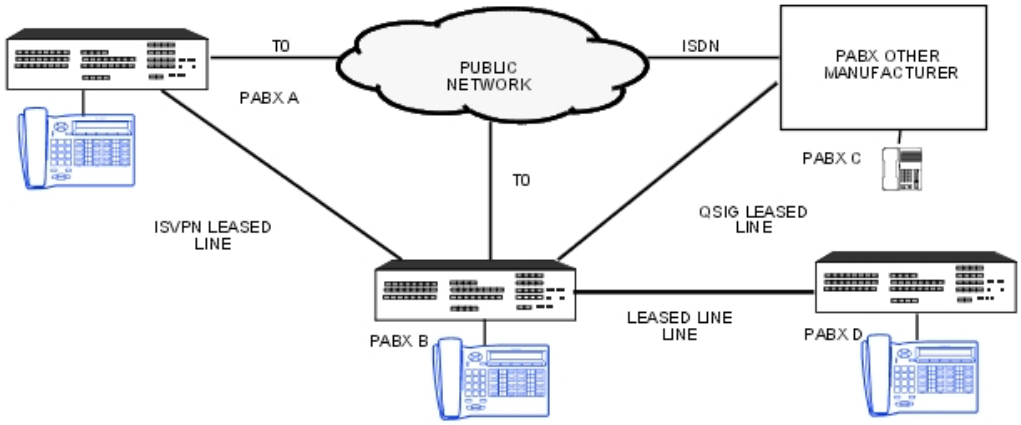
- automatically
- manually (transfer by operator for example)

The ARS tables can be programmed so that the automatic break-out mechanism is used (overflow or forcing on the private network).

There is no operator recall in the following cases of failure (the call is released):

- the trunk group is busy
- ISDN releases the call, the time-out for awaiting the 1st digit or interdigit having elapsed

TRANSIT



PCX B enables the transit of the following communications:

- from a user A to users of PCXs C and D
- from the public network to users of PCXs C and D

These communications are established by:

- public or private break-in -> private
- private break-out -> private or public

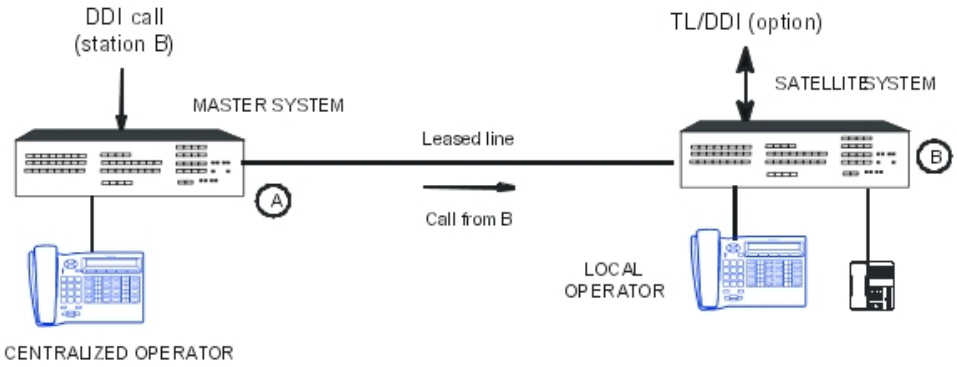
The transit system acts as an access between the different protocols used; the level of service offered depends on the protocols implied in the communication:

- QSIG <-> ISVPN: services offered by QSIG
- ISVPN on public line <-> ISVPN on leased line: ISVPN services
- ISDN <-> ISVPN or QSIG: ISDN services

CENTRALIZED OPERATOR

An incoming call, in transit on a PCX or transferred whilst ringing (unsupervised transfer) on a leased line, which is not answered after a certain amount of time, is automatically re-directed to the operator of the system which received the call.

The CENTRALIZED OPERATOR, the name given to this feature, is organized around the PCXs connected to the network over leased lines. One of the PCXs, configured as the "Master", will have the CENTRALIZED OPERATOR STATION. The other "Satellite" PCXs may also have local operators.

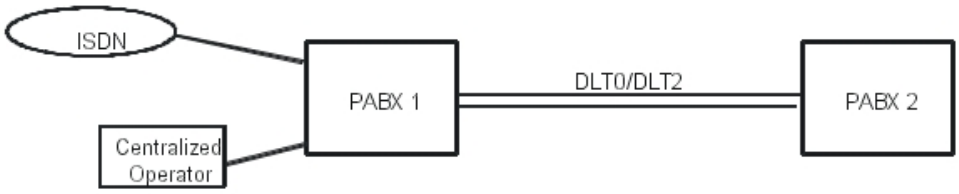


Environment

When installing this feature on a PCX network, the following must be taken into account:

- A specific programming procedure, performed for each PCX in the network, makes it possible to configure a Master PCX and Satellite PCXs. The operator of the PCX configured as the Master becomes the Centralized Operator.
- Only incoming calls issued from the T0 or T2 network interfaces of the Master PCX go through the centralized operator mechanism. Nevertheless, Satellite PCXs can be equipped with network junctors and a local operator thus enabling autonomous management of their traffic.
- An incoming call routed to the centralized operator benefits from the welcome message mechanism, if it is active.
- The display on the centralized operator is usually provided for incoming calls which are routed to it.
- An incoming call which is considered as "non telephone" by the system, is not subject to the centralized operator mechanism. For example, an incoming T0 ISDN call a G4 Fax service.

Configuring a network with external lines on only one PCX



To redirect the call to the centralized operator, there are two possible solutions: the "ReroutOpe" function of the transit system (PCX1), or dynamic routing/attendant forwarding of PCX2.

Using ReroutOpe:

- Configure a timeout value before re-routing through PCX1:

System Miscellaneous -> **Memory Read/Write** -> **Misc. Labels** -> **ReroutOpe**.

Default value: 00 00: rerouting of in transit calls towards the centralized operator is inactive.

Configuration example: ReroutOpe = C8 00 (no 100 ms, 20 seconds).

An call in transit towards the satellite, in the event of no reply, will be rerouted to the centralized operator on PCX1 after 20 seconds (PCX1 releases the line to PCX2).

Note 4:

Only DDI calls routed directly to PCX2 (break-in) fall under ReroutOpe timeout (this mechanism does not apply to a network line under call distribution).

If PCX2 users are using dynamic routing (for example towards the Voice Mail unit), the ReroutOpe timeout value must be superior to the dynamic routings used by PCX2 users.

Dynamic routing/Attendant group routing:

It is also possible to re-route calls from PCX1 to PCX1 using dynamic routing on PCX2 stations and the Attendant group routing function within the time ranges of PCX2.

- Configuring a collective speed dial number in PCX2 (n# 8000 for example) with PCX1's operator as destination.

The trunk group assigned to this number must be an homogenous logical direction for optimization to be effective.

Time ranges -> **Destination for time ranges = 8000; Attendant Diversion = Yes within forwarding time ranges**

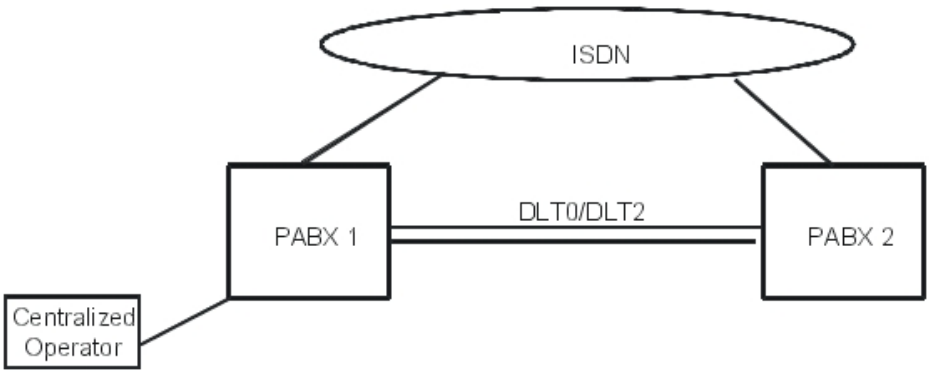
- Configuring PCX2 stations supporting dynamic routing on attendant group:

Subscribers/Basestations List -> **Station (choose station)** ->**Details** -> **Dyn routing** -> **Timeout T2 = XX ; External calls column - Level 2 : check "Use Timer 2", "Forwarding to general level" and "Diversion apply".**

This configuration offers the same operation as ReroutOpe timeout but is more flexible for choosing which calls are rerouted or not to the centralized operator:

- by choosing dynamic routing of PCX2 users, it is possible to choose which calls, internal or external, are rerouted to the centralized operator.
- this configuration can be customized for each station (for example by suppressing dynamic routing at general level for an analog device equipped with a fax.
- It is possible to choose different re-routing timeouts (T1, T2) for each user.

Configuring a network with external lines on each PCX



If there is no local operator in PCX 2, use the programming shown in the previous example (dynamic routing/attendant group routing).

When there is a local operator in PCX 2, in addition to the attendant diversion to PCX1 using the attendant group diversion by time range function described earlier, it is possible to perform a forced diversion using the "Attendant Diversion" function.

- to program an "Attendant Diversion" key.

Subscribers/Base stations List -> **Subscriber (select OS)** -> **Details** -> **Keys** -> **Type = Function Key** -> **Function = Attendant Diversion, Number = 8000 (speed dial n# corresponding to a call to the centralized operator).**

Set up from the Operator:

- press the "Attendant Diversion" key
- operator code (help1954 by default); the LED associated with the key flashes.
- to cancel: same operation

Call handling

The table below describes the reactions of a centralized operator network with or without a satellite local operator.

SITUATION	SAT. WITHOUT LOCAL OPER.	SAT. WITH LOCAL OPER.
The call no. in the satellite does not exist or is incomplete	The centralized operator is rung	The time-out (ReroutOpe) starts up The local operator is rung
No connection rights	The called party is released	
The called party is released	The time-out (ReroutOpe) starts up The set is rung	
The called party is grade 1 busy	The time-out (ReroutOpe) starts up If the satellite has the right to camp on, then the call is camped on; if not, the centralized operator is rung	The time-out (ReroutOpe) starts up If the satellite has the right to camp on, then the call is camped on; if not, the local operator is rung if the destination's dynamic routing is inferior to the "ReroutOpe" timeout.
The called party is grade 2 busy	The centralized operator is rung	The time-out (ReroutOpe) starts up The local operator is rung
The call no. is out of service		
The called party is in DND		
The time-out (ReroutOpe) expires	The call is directed to the centralized operator	
The incoming call is transferred to the satellite	The time-out (TransfeTim) starts up The set is rung	
The time-out (TransfeTim) expires	Depending on configuration of "Master recall" to the centralized operator the call is: - either routed to the centralized operator - or routed to the initiator of the transfer. When the time-out (Duration of Hold Recall Ringing) has lapsed, the call is directed to the centralized operator	

Note 5:

By default, the "ReroutOpe" timeout is equal to 00 00; for a re-routing to the central operator after 20 seconds for example, the configuration must be "ReroutOpe" = C8 00.

For normal operation, the "ReroutOpe" timeout must be inferior to the dynamic routing timeouts of the slave system.

EXTERNAL FORWARDING OF OPERATOR CALLS

This service makes it possible to forward all operator calls (local calls, public and private incoming calls, operator recalls, dynamic forwardings) to a public or private external destination.

For a more detailed description, see the relevant section in "Telephone Features".

AUTOMATIC CALL-BACK ON BUSY TRUNK GROUP

If a call goes through ARS mechanisms and if all the configured trunk groups are busy, it is possible to activate an automatic call-back request on a busy trunk group. The user is called back as soon as a line in the first trunk group (traffic sharing) proposed by the ARS mechanisms is released.

DISTRIBUTION IN A PRIVATE DIGITAL NETWORK

- The handling of external calls (on public lines) and internal calls (on leased lines) can be configured differently.

- by OMC (Expert View), select: **External lines**-> **Incoming Call Handling**. For each type of line, you can define the actions (call released or forwarded to the operator) in the following situations:
  - depending on whether the caller is public or private
  - called party busy 2nd degree
  - other called party status (in Do Not Disturb forwarding, out of service, recall situation following a transfer failure)
  - misdial

In the case of unanswered calls on leased lines, the dynamic forwarding mechanisms of an internal (local) call relative to the called set are applied.

PRESENTATION OF CALLS

- Presentation to the called party
  You can select the presentation mode for private calls:
  - presentation as local call:
  - internal ringer
  - number of the caller not memorized in the directory of last callers (except if the call has a UUS)
  - no welcome message option
  - presentation as external call:
  - external ringer
  - number of the caller memorized in the directory of last callers
  - welcome message option

- by OMC (Expert View), select: **System Miscellaneous** -> **Feature Design** -> **Private Call Presentation**

- Presentation to the caller

On the caller's set, the display always shows the number dialed by the user (not the one after modifications by the ARS).

The number can be replaced by the name (name received if ISVPN, or name in the personal or collective speed dial numbers).

- Handover

In case of a transfer within an ISVPN network, the ISVPN subscribers" displays are handled as if they were in the same system. Especially after a transfer of an incoming call from user A to user B in a different node, the display of B indicates the external caller rather than the user A.

- Diversion/Dynamic routing

If an incoming call to subscriber A is diverted to subscriber B in a different node, the call is presented to B with the name of A on the display (or, failing that, the number of A).

CALLED PARTY STATUS

During an outgoing call, the ISVPN protocol makes it possible to signal to the caller whether the called party is busy; the called party's busy status is only indicated by a message on the caller's display; there is no audio indication (the caller always hears the call-back tone transmitted by the network).

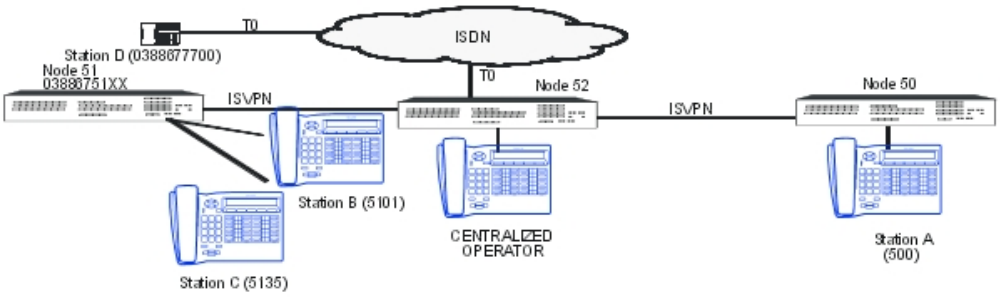
INTRUSION

When the remote correspondent is grade 1 busy, the ISVPN protocol makes it possible to intrude on this set (unless it is protected against intrusion).

INFORMATION DISPLAYED

ISVPN on leased lines

Example:



Call	Number dialed	Number transmitted	Caller's display	Called party's display
A -> C	5135 (private network call)	5135 on leased line	Name of C	Name of A
B -> C	5135 (local call)	5135	Name of C	Name of B
B -> OPER.	9 (private network call)	9 on leased line	Name of operator	Name of B
B ->D	00388677700 (public network call)	0388677700 by break-out	0388677700 or name of D (if managed locally)	0388675101

Forwarding

For a call on digital lines (ISDN or QSIG) and if the called party is forwarded, it is possible to define, using OMC (Expert View), the identity which is transmitted to the rung set:

- either that of the caller (set B in the example)
- or that of the called set (forwarded set A)

- by OMC (Expert View), select: **System Miscellaneous** -> **Feature Design** ->check one of the 2 boxes # CLI for external diversion or # CLI is Diverted Party.

SUMMARY TABLE

Features	**VPN**	**ISVPN "Public"**	**ISVPN "Private"**	**QSIG**	**ISVPN+**
Differentiation between public and private calls	YES	YES	YES	YES	YES
Internal or external incoming call handling	YES	YES	YES	YES	YES
Break-in/break-out	--	--	YES	YES	YES
CLIP/CLIR	YES	YES	YES	YES	YES
COLP/COLR	--	--	--	YES	YES
Non answered calls repertory	YES	YES	YES	YES	YES
Sub-addresses	YES	YES	YES	YES	YES
Display of caller	--	YES	YES	--	YES
Optimization of the transfer	--	YES	YES	--	YES
Optimization of forwarding	--	YES	YES	--	YES
Indication of forwarding on the centralized operator	--	YES	YES	--	YES
Transporting of the name in UUS	--	YES	YES	--	YES
Intrusion	--	YES	YES	--	YES
Information on metering sent to the master in Master/Satellite configurations	--	--	--	--	YES

7.2 Principles of ARS Mechanisms

7.2.1 Mechanisms

7.2.1.1 Overview

7.2.1.1.1 OUTLINE

ARS is a mechanism which, during the routing of a call:

- forces the use of the most appropriate path according to the number dialed.
- chooses another path if the most appropriate one is overloaded.

This mechanism is applied independently of the type of:

- trunk group: public or private

- support: analog or digital
- call: voice or data

ARS is completely transparent for the user; the number dialed is, if necessary, modified automatically according to the chosen itinerary.

Note:

If the ARS mechanism modifies the number dialed by the user:

- the station's display shows the number dialed by the user.
- It is the **emitted** number (modified by the ARS) which is analyzed in the discrimination.
- the charge ticket shows the **emitted** number (modified by the ARS).

The ARS mechanism can be applied for the following calls:

- outgoing call with manual dialing:
  - without specific line seizure
  - with specific public line seizure
  - using resource keys assigned to a trunk group
- outgoing call with automatic dialing:
  - call keys
  - personal and collective speed dial numbers, call by name
  - last number redial, temporary memory number
  - last callers directory
- all types of forwarding and routing to an external destination
- VPN configurations (Transgroupe/heterogeneous network) for converting a public number into a private number (incoming call) or vice versa (outgoing call).

7.2.1.2 Interactions

LINE ALLOCATION

This feature is incompatible with ARS mechanisms.

BARRING AND TRAFFIC SHARING

The traffic sharing mechanism within a trunk group list or between trunk group lists can be used to authorize overflow between trunk groups for specific users.

When barring prohibits dialing on the selected trunk group, no overflow is possible and the call is released.

EMERGENCY NUMBERS

This paragraph only concerns the emergency numbers defined when the system is initialized (numbers installed in ROM).

ARS table base fields:

Network	Prefix	Ranges	Substitute	TrGp list	Called Party (ISVPN/H450)	User com.
Urg	-	-	-	XX		

The only possible configurations for emergency numbers ("Network" field = Urg.) are:

- prefix = empty; replace = empty: transparent dialing in the ARS table
- prefix = empty; replace = XXX: addition of digits XXX (useful for break-out)

The traffic sharing and barring mechanisms are not applied to emergency numbers (as with collective speed dial numbers).

If the emergency number is dialed after line seizure, the call goes through the ARS mechanisms if the line figures among the trunk groups in the ARS tables; if not, the number is transmitted on this line directly.

If the ARS table has no entry for emergency numbers, the trunk group associated with the default public prefix is used, if there is one; if not, the main trunk group is used.

7.2.2 Parameters

7.2.2.1 Configuration procedure

ARS is implemented when the "Base" field is empty for the "Main trunk group seizure" and "Secondary trunk group seizure" features in the main numbering plan and the numbering plans for private and public incoming calls.

Main dialling plan

Start	End	Base	Feature	NMT	Private
XXXX	XXXX		Main trunk group	Keep or Drop	Yes/No
XXXX	XXXX		Secondary trunk groups	Keep or Drop	Yes/No

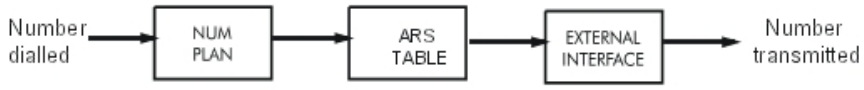
Base: if this field is empty, the call is of type ARS; if not, it is a trunk group call.

NMT: this field defines whether the digits defined in the "Start" and "End" fields are absorbed or conserved.

Priv: this field is a reference for the "Network" parameter in the ARS table:

- Yes: the outgoing number in the dialling plan is compared to the entries in the ARS table with "Network" = Private.
- No: the outgoing number in the dialling plan is compared to the entries in the ARS table with "Network Identifier" = Public, Urg. or Code auth.

After analysis and possible modification by the NMT, the outgoing digits in the dialling plan are entered in the ARS table.



ARS TABLES

The installer determines the numbers or parts of numbers in front of the ARS handling. For each destination defined by a prefix, it creates a "trunk group list". For each index in the list, it is possible to assign one or several trunk groups and commands for modifying the dialling.

The ARS prefix replaces the external seizure prefix. On recognition of the prefix, the system determines the associated "trunk group list". The ARS mechanism therefore uses the route by activating the call on the corresponding trunk group. If the trunk group is busy, the next

programmed route is used.

Note 2:

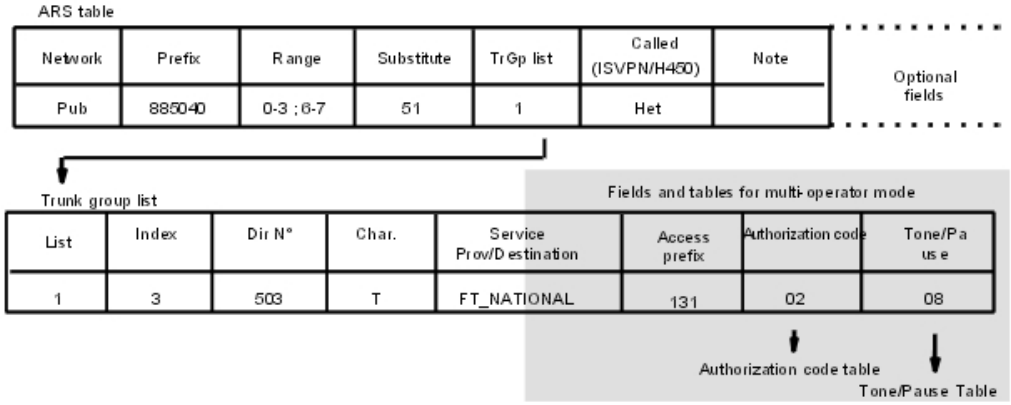
In some instances, the equivalent French acrostic "ADL" may be found instead of "ARS".

USE OF THE VARIOUS TABLES

- The various parameters required for ARS operations are configured using OMC (Expert View) only

- by OMC (Expert View), select: **Dialling plan** -> **Automatic Routing Selection**. -> then configure the following tables:
  - ARS table
  - Trunk groups list
  - Hours table
  - Day table
  - Providers / Destinations
  - Authorisation codes
  - Tone/Pause
  - ARS miscellaneous

- Structure of the main tables:



- Dimensions:

Max. number of prefixes (= number of lines in each of the 2 tables): 500

Max. number of entries in the trunk group lists (= number of lines in each of the 2 tables): 500

Max. number of ranges: 500

Max. number of entries in the ARS table: 500 (entries in the prefix table + trunk groups + time ranges: 500 max; one entry in the prefix table with 2 ranges or with a sub-line counts for 2 entries.

ARS TABLE

Base fields:

These fields are necessary and sufficient for the majority of network topologies.

Network	Prefix	Ranges	Substitute	TrGp list	Called Party (ISVPN/H450)	User com.
Pub	885040	0-3 ; 6-7	51 885040	2 1	Het.	

As many trunk group lists as are authorised can be assigned to each prefix; by default, no prefix is defined.

Network: this network identifier defines the prefixes as public prefixes (Pub), private prefixes (Priv), public emergency numbers (Urg) or public access codes (Code auth.).

Prefix: an empty field (default value) corresponds to the numbers which do not correspond to any prefix for the network identifier concerned.

Range: this is used both for outgoing and incoming calls; there is no range for public emergency numbers or public access codes. It is possible to enter several ranges (separate them using the ";" character) within the authorised limits (see previous page).

Replace: the ARS prefix can be modified by the contents in this field.

- prefix = empty; replace = empty: transparent dialling in the ARS table
- prefix = empty; replace = XXX: addition of digits XXX
- prefix = XXX; replace = empty: absorption of digits XXX
- prefix = XXX; replace = XXX: no modification (no addition nor absorption)
- prefix = XXX; replace = YYYY: replace XXX by YYYY

TrGp List: this field defines the index for one or several selected trunk group lists. Priority is given to the trunk groups in the first list, in the order of programming, then to the second list, and so on.

Called party (ISVPN/H450): the called party belongs to a homogenous network (Alcatel-Lucent OmniPCX Office Communication Server or Alcatel-Lucent OmniPCX Enterprise Communication Server) or a heterogeneous network (systems made by different manufacturers).

Note: the information entered in this field is stored in the system.

Optional fields:

Metering	Caller	Called/PP
	Priv.	Pub
Overflow	Pub	Pub

Metering: only significant for a centralised account charging application (NMC), this field is only used for entering additional information in the counters data:

- field empty
- overflow
- network (private network forcing)
- VPN
- VPN + network
- VPN + overflow

Description of the "Caller" and "Called" parameters

The following fields are to be filled in for specific network topologies (in the majority of cases, the default values are sufficient). These fields concern the coding and contents of the data sent in a call.

Caller: the caller's number corresponds to the private dialling plan (the caller's private number, made up from the private installation number, must be transmitted) or to the public dialling plan (the public number is made up from the public installation number).

Called/PP: the sent called party's number is public or private (field reserved mainly for VPNs; "Type of dialling plan" in the setup: Public Network).

Important:

Use of default values in the "Caller" and "Called" fields.

For appropriate use of default values in these fields, the installer must consider the following:

- The type of line must be configured correctly.

• by OMC, select: **External Lines** -> **External Lines** ->select line -> **Details** ->select or deselect ? Public Trunk): • a DLT2/DLT2/VOIP access must be configured as a private line (default value) • a T0 or T2 access must be configured as a public line (or a private line if linked with an Alcatel-Lucent OmniPCX Enterprise Communication Server

- On a private link, the caller's private number is transmitted by preference; nevertheless, if the private number is not available, the public number (break-out only) or the private installation number (call in the private network) is transmitted.
  On a public link, the caller's public number is transmitted; if it is not available, no caller identification is supplied.
- The default values are to be used for all outgoing calls to the public network (the 2 fields are public) and for all calls in the private network (the 2 fields are private).
  On the other hand, it is recommended to use specific values for VPN calls (the 2 fields are private while the external line is public) or when the Alcatel-Lucent OmniPCX Office Communication Server is connected by a line leased to a particular system.

Possible combinations

This paragraph describes the significant combinations for the "Caller" and "Called" fields according to the network environment of an Alcatel-Lucent OmniPCX Office Communication Server system.

- for an outgoing call on a leased link (QSIG): only the following fields are significant:
  - caller = private or public
  - called = private (heterogeneous and homogenous values are also used).
- for an outgoing call on public link:
  - caller = private or public
  - called = values according to the table below:

Called/PP	Called Party (ISVPN/H450)	Use
Public	Homogenous	Internal call from a user in a private network (homogenous ISVPN)

Public	Heterogen.	Outgoing call to the public network or internal call from a user in the private network (heterogeneous ISVPN)
Private	Heterogen.	Internal call from a user in the private network (heterogeneous VPN) or outgoing call to the public network by VPN private dialling (ISDN user also declared in VPN)
Private	Homogenous	Internal call from a user in a private network (homogenous VPN)

TRUNK GROUP LISTS

Each trunk group list can have as many trunk groups as are authorised within the global limits.

The "Access digits", "Authorisation code" and "Tone/pause" fields are specific to MULTI-CARRIER MODE.

Example:

TrGp list	Index	TrGp.	Char.	Provider/Destination	Access digits	Authorisation code	Tone/Pause
1	1	0		FT LOCAL			
	3	503	T	FT LOCAL	131	02	02

List: identifier for each trunk group list (see table of prefixes).

Index: this field makes it possible to select one or several trunk groups identified by an index (1 to 120); for a list with several trunk groups, priority is given to the first index. INTERNAL is used when no trunk is used to call the destination and allows to configure this entry as an internal call.

N°: this field automatically displays the directory number of each trunk group in the list.

Char: this field defines a character used in account charging or on set displays (for example: T for Transgroupe).

Provider/destination: the operator name used depends on the time range (see below).

If a label is defined for a trunk, the control system checks the validity of the label for the considered time range. If it is valid, the trunk group is selected if it follows the traffic sharing conditions. If not, there will be an overflow to the next trunk group. The presence of a label in this field implies the configuration of time slots, groups of days, etc.

Access digits: this field defines the code for accessing an indirect network.

Auth. Code ID: index (1 to 24) in the "customer code" table.

Tone/Pause: index (1 to 8) in the "Tone/Pause" table

Note 3:

Using the "Provider" field requires a complete programming of the ARS time ranges.

NETWORK SERVICE PROVIDERS

This table defines the names of the various network service providers associated with a trunk group list for each time range. The table can also receive internal destinations.

TIME RANGES

The use of time ranges in the ARS makes it possible to select the route offering the best cost conditions at any given time. Access to the carrier can be direct (e.g. Cégétel) or indirect (e.g. Espadon).

Start	End	Day group	Provider/Destination 1	Provider/Destination 2	Provider/Destination 3	Provider/Destination 4
08:00		1	FT LOCAL	ESPADON	CEGETEL	
		2	CEGETEL			
		3				
12:00		1	FT LOCAL			
		2				
		3				

The table defines different time ranges and to associate providers with each day group in each range; it is also possible to enter internal destinations (the same as are indicated in the "Provider / Destinations" table).

4 providers can be associated with each combination of time range/day groups. If 2 labels out of the 4 relate to the same destination, the associated trunk groups must be different so as to enable overflow if one of the providers is busy.

If no provider is defined for a given combination, a route will be selected from among the trunk groups without associated provider labels, independently of the time ranges. The same operation applies for the days in the week or bank holidays not associated with a day group.

It is recommended to put one trunk group without provider in each trunk group list to be able to flow the call in all possible cases of figures.

Total number of time ranges: max. 500 (including the entries of the prefix and of the trunk group tables)..

DAY GROUPS

This table defines an operating mode (a day group) for each day of the year.

- Days of the week:

In order to simplify management, the 7 days of the week are split into 7 groups (for example: the 5 working days = group 1, Saturday and Sunday = group 2)

Day of the week	Day	Month	Year	Day group
Monday				1
Tuesday				1
Wednesday				1
Thursday				1
Friday				1
Saturday				2
Sunday				2
	14	7	*	2
	1	5	*	2
	30	3	1997	2

- Bank holidays:

There is no need to define the year for fixed bank holidays (* character = each year); for

variable bank holidays, indicate the year (using 4 figures).

Note 4:

The data contained in this table can also be entered using MMC-Station.

AUTHORISATION CODES (MULTI-CARRIER ONLY)

This table (24 entries of up to 10 characters) defines the secret access codes between the networks of different carriers.

"TONE/PAUSE" (MULTI-CARRIER ONLY)

This table (8 entries max.) is indicated by the "Tone/Pause" parameter of trunk group lists. It defines the reactions when a call is redirected to an indirect network: pause duration or tone detection, automatic switch over to MF dialling (DTMF).

Example:

Index	Time/Tone before Auth.(ms)	Time/Tone after Auth (ms)	Force MF
1	Tone	8	No
2	Tone		Yes

Time/Tone: the following values are possible:

- Tone: if value = Tone, the PCX waits for the dial tone before transmitting the dialling on the line. Waiting for the tone is only possible on analogue lines.
- XXX: the PCX waits XXX milliseconds (from 8 to 20000, in multiples of 8 ms) before transmitting the dialling on the line.

Force MF: after the access code, the network which is called indirectly can receive the digits in a signalling mode different from the one on the line in use. If the value in this field is YES, then all dialling transmitted after the access code is MF.

ARS MISCELLANEOUS (MULTI-CARRIER ONLY)

2 flags are proposed:

- Manual direct access: this flag is only analysed if the "Prefix" field in the ARS table relates to a public access code (code auth). If the dialled number has a public access code and if the flag is not authorised, the call is rejected.
- Automatic indirect access: this flag is analysed when the "Access digits" field in a trunk group list is filled in. When the flag is not authorised, the next line in the trunk group list is analysed.

7.2.3 Principles

7.2.3.1 Basic description

For a particular prefix, it is possible to define several ranges

Network	Prefix	Ranges	Substitute
Priv	36	0-1 ; 22-23 ; 444-555 ; 6666-7777	03887766
Priv	36	24-25 ; 87-97	03884433
Priv	36	-	03881100

36123 dialled -> selection of the first entry (123 belonging to the range 0-1).

368899 dialled -> selection of the second entry (8899 belonging to the range 87-97).

3699 dialled -> selection of the third entry (99 not belonging to any range defined for the prefix 36).

If a range covers other prefixes for outgoing calls, the first range corresponding to the digits dialed is selected

Network	Prefix	Ranges	Substitute
Priv	36	5-6 ; 888-999	03887766
Priv	36	88-99	03884433
Priv	36	55-56	03881100

3655 dialled -> selection of the first entry (55-66 included in 5-6).

36889 dialled -> selection of the first entry (888-999 included in 88-99).

Different ranges cannot be defined between the fields "Prefix" and "Substitute"

36 [01-03] cannot be replaced by 03886777[51-53] -> 3 entries have to be created in the ARS table.

Network	Prefix	Ranges	Substitute
Priv	3601		0388677751
Priv	3602		0388677752
Priv	3603		0388677753

As soon as a prefix is recognized and if the digits dialed do not belong to the range, there is no overflow from one prefix to another

Network	Prefix	Ranges	Substitute
Priv	7	1000-7299	7
Priv	77	300-320	1

77299 dialled -> recognition of prefix 77: 299 not belonging to the range defined for this prefix, the dialled number is not taken into account by the ARS mechanisms (even though this number corresponds to entry 7[1000-7299]. To remedy this situation, configure the following ARS table:

Network	Prefix	Ranges	Substitute
Priv	7	1000-6999	7
Priv	77	000-299	77
Priv	77	300-320	77

Pay attention to overlaps in the "Substitute" field

Network	Prefix	Ranges	Substitute
Priv	36	00-99	03887766
Priv	3588	-	0388776688

There is an overlap between 03887766[00-99] and 0388776688. For incoming calls, there are 2 possible conversions of the public number 0388776688 into private numbers: 3688 and 3588. For example, to convert the public number into the private number 3688, configure the ARS as follows:

Network	Prefix	Ranges	Substitute
Priv	36	00-87	03887766
Priv	3588	88-88	03887766
Priv	3689	89-99	03887766

For incoming calls, the public number received, 03887766XX is converted into the private number 35[88-99] if XX does not belong to the range 00-87.

Network	Prefix	Ranges	Substitute
Priv	36	00-87	03887766
Priv	35		03887766

7.2.4 Internal Destinations

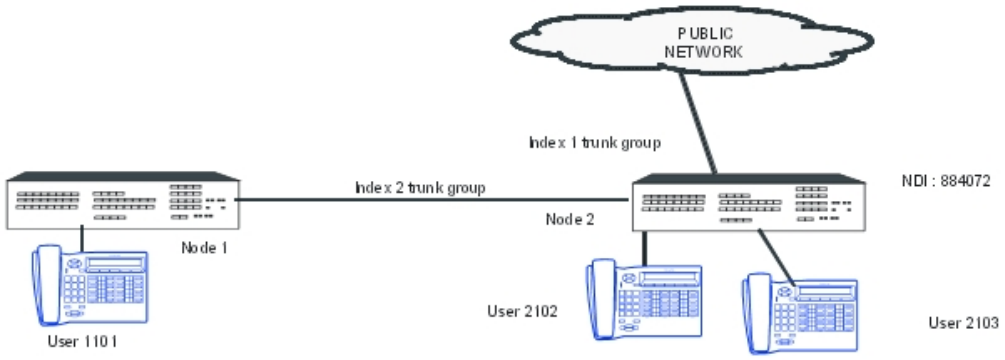
7.2.4.1 Detailed description

ARS mechanisms can handle internal destinations.

7.2.4.1.1 INTERNAL CALL FORCING

When a user tries to call a correspondent (connected to the same Alcatel-Lucent OmniPCX Office Communication Server system or belonging to the same private network) by dialing the correspondent's public number, the ARS mechanism converts the public number into an internal number, and an internal call is made.

Configuration example



"ARS Table" configuration:

Network	Prefix	Ranges	Substitute	TrGp list	Called Party (ISVPN/H450)	User com.
Pub	8840722	100 - 200	2	4		

Pub	8840721	100 - 200	1	1		

"Trunk group list" configuration:

TrGp list	Index	TrGp.	Char.	Provider / Destination	Access digits	Authorization code	Tone/Pause
1	2	500					
4	LOCAL	---					

In this example:

- the public call from user 2102 to user 2103 (by dialing 08840722103) is converted into a local call by replacing 8840722 by 2; the system therefore sends the number 2103.
- the public call from user 2102 to user 1101 (by dialing 08840721101) is converted into a local call by replacing 8840721 by 1; the system therefore sends the number 1101 over trunk group 2 (as the 2 sets do not belong to the same PCX).

7.2.5 Selecting a Destination

7.2.5.1 Configuration procedure

7.2.5.1.1 SELECTING THE DESTINATION ACCORDING TO THE TIME

It is also possible to route a call to different internal destinations depending on the date and time. This is achieved using overflow mechanisms between trunk group lists with the same index.

Configuration example

"ARS Table" configuration:

Network	Prefix	Ranges	Substitute	TrGp list	Called Party (ISVPN/H450)	User com.
Priv	5000		102 103	100 200		

"Trunk group list" configuration:

TrGp list	Index	TrGp.	Char.	Provider / Destination	Access digits	Authorization code	Tone/Pause
100	LOCAL			User 102			
200	LOCAL			User 103			

"Time Ranges" configuration:

Start	End	Day group	Provider / Destination 1	Provider / Destination 2	Provider / Destination 3	Provider / Destination 4
00:00	12:00	1	User 102			
12:00	00:00	1	User 103			

"Day Groups" configuration:

- All the days of the week are assigned to day group 1.

"Providers / Destinations" configuration:

Providers / Destinations
User 102
User 103

In this example, if an internal user dials 5000: a call made between 0 and 12.00 hours will be put through to set 102 and a call made between 12.00 and 0 hours will be put through to set 103.

- between 0 and 12.00 hours: trunk group list 100 is selected; 5000 is replaced by 102 and user 102 is called.
- between 12 and 0 hours: first of all trunk group list 100 is selected; 5000 is replaced by 102. Overflow occurs in the ARS table and the second entry (trunk group list 200) is selected. 5000 is replaced by 103 and user 103 is called.

7.2.6 Rerouting on Operator Busy

7.2.6.1 Overview

7.2.6.1.1 Definition

When a call cannot get through because the operator is busy, this mechanism automatically reroutes it via another operator.

The rerouting mechanism is totally transparent to the user (no specific tone or display).

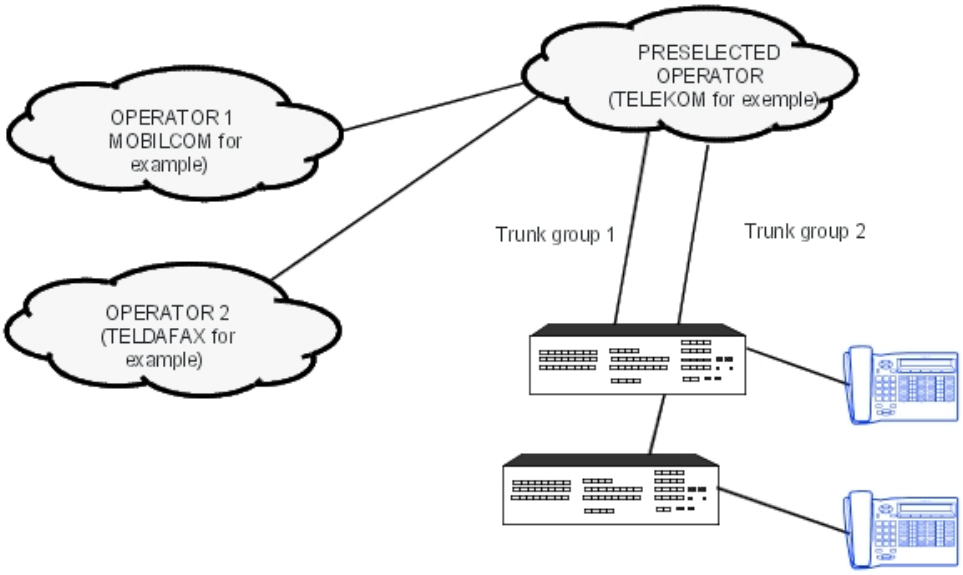
The mechanism is only offered for calls routed by ARS over ARS trunk groups (ISDN trunk groups only).

Automatic rerouting when the operator is busy is activated by the triggers defined by the "BsyPrvCaus" flag and refers to the ARS table settings.

7.2.6.1.2 Configuration example

In this example, at any moment of the week calls starting by 089 are processed by the operator Mobilcom, and by Teldafax if Mobilcom is busy. If Teldafax is also busy, these calls will be processed by the preselected operator Telekom.

All other external calls (calls not starting with 089) are processed by Telekom.



"Dialing plan" configuration:

- "Secondary trunk groups seizure" function: Start, End = 0; Base = ARS; NMT = Absorbed. All calls starting with 0 are ARS calls and the subsequent figures are analyzed by the ARS tables.

"ARS Table" configuration:

Network	Prefix	Ranges	Substitute	TrGp list	Called Party (ISVPN/H450)	User com.
Pub	089		089	1	Het	Operator
Pub				2		Telekom

"Trunk group list" configuration:

TrGp list	Index	TrGp.	Char.	Provider / Destination	Access digits	Authorization code	Tone/Pause
1	1 1 1	0 0 0		Mobilcom Teldafax None	01019 01030	None None None	None None None
2	1	0		None		None	None

"Time Ranges" configuration:

Start	End	Day group	Provider / Destination 1	Provider / Destination 2	Provider / Destination 3	Provider / Destination 4
00:00	00:00	1 2 3	Teldafax None None	Mobilcom None None	None None None	None None None

"Day Groups" configuration:

- All the days of the week are assigned to day group 1.

"Providers / Destinations" configuration:

Providers / Destinations
Mobilcom
Teldafax

7.2.6.1.3 Configuration

- Define the activation causes for the mechanism (5 causes maximum, FF indicating the end of the list of causes)

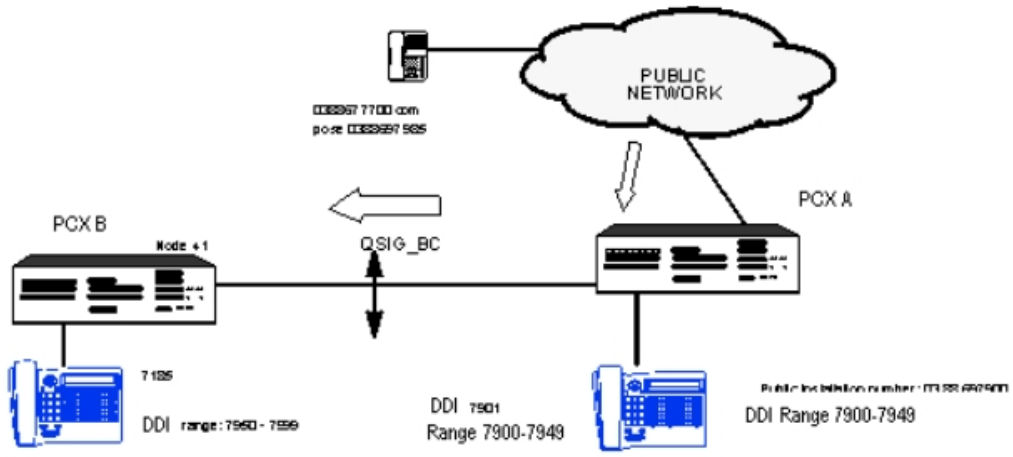
- by OMC (Expert View): **System Miscellaneous -> Memory Read/Write -> Labels -> Misc. Labels -> "BsyPrvCaus"**
- by MMC-Station: **Global -> Rd/Wr -> Address -> " BsyPrvCaus" -> Return -> Memory**

7.2.7 Configuration examples

7.2.7.1 SIMPLE CONFIGURATIONS

BREAK-IN

A public user calls a user of a PCX B by break-in in PCX A.



Public numbering plan of PCX A

Start	End	Base	Feature	NMT	Private
7900	7949	100	Set	-	no
7950	7999	-	Secondary trunk group	Keep	No

ARS table of PCX A

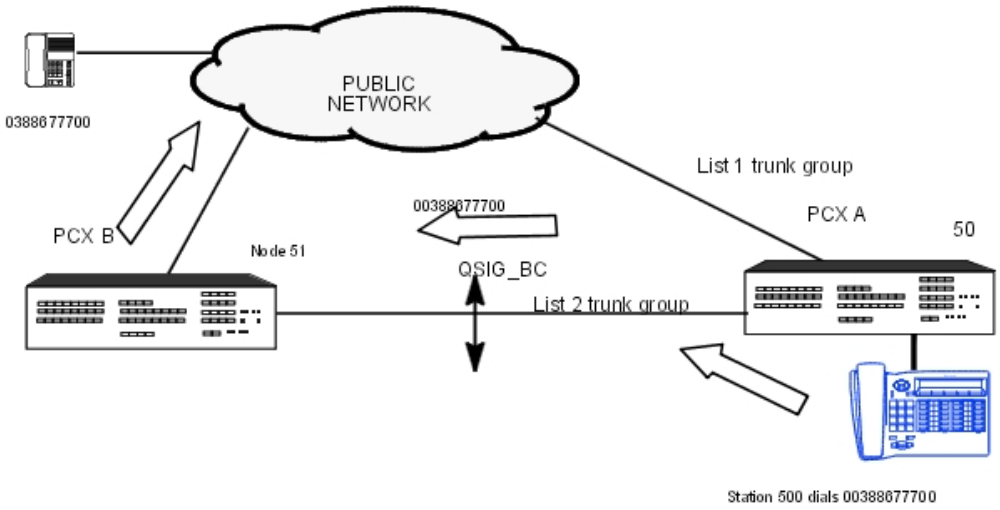
Network	Prefix	Ranges	Substitute	TrGp list	Called Party (ISVPN/H450)	User com.
Pub	03886979	-	41	1	Homogenous	

Private numbering plan of PCX A

Start	End	Base	Feature	NMT	Private
4150	4199	100	Set	-	Yes

BREAK-OUT

Set 500 in PCX A (node 50) calls user 0388677700 on the public network. The ARS operations force the call to use the private network. If the private network is busy, the start call will be made on the network access of PCX A.



Main numbering plan of PCX A

Start	End	Base	Feature	NMT	Private
0	0	ARS	Main trunk group	Absorb	No
51	51	ARS	Secondary trunk group	Keep	Yes

ARS table of PCX A

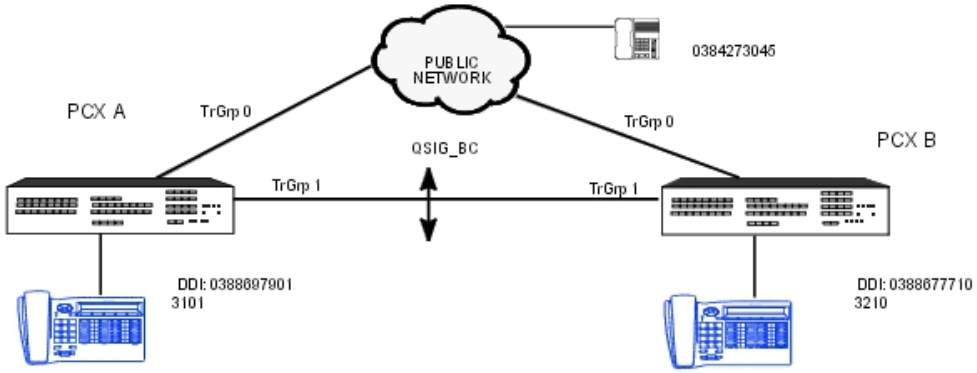
Network	Prefix	Ranges	Substitute	TrGp list	Called Party (ISVPN/H450)	User com.
Pub	-	-	-	1	Heterogen.	
Priv.	51	-	51	2	Homogenous	
Pub	038867	- -	0038867 038867	2	Homogenous Heterogen.	Overflow

CONVERSION BETWEEN PUBLIC AND PRIVATE DIALLING PLANS

Case 1: Peer to peer - ISVPN and overflow

This configuration corresponds to a call in an ISVPN heterogeneous network or an overflow on

a public link when the private QSIG-BC link is busy.



ARS table of a PCX A for overflow mechanism

Network	Prefix	Ranges	Substitute	TrGp list	Called Party (ISVPN/H450)	User com.
Pub	32	- 00 - 99	32 03886777	1 0	Heterogen. Heterogen.	

Case 2: Peer to peer - private network forcing

ARS table of a PCX B

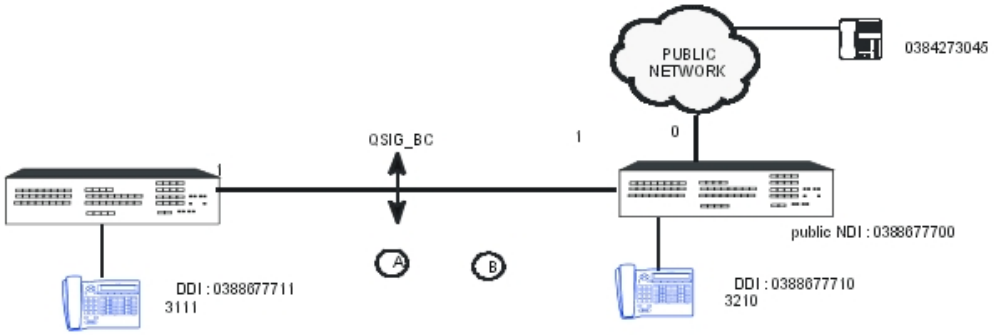
Network	Prefix	Ranges	Substitute	TrGp list	Called Party (ISVPN/H450)	User com.
Pub	03886979	- 00 - 99	31 03886979	1 0	Heterogen. Heterogen.	

In this configuration, if user 3210 calls a user of a PCX A with his public number (0388697901), the call is forced to use the private link with the private number 3101.

Case 3 : master/satellite

In this configuration, the DDI numbers in PCX A are managed remotely by PCX B ; a public numbering plan in PCX A is therefore not necessary if:

- PCX B can convert a private number into a public number (for outgoing call by break-out).
- PCX B can convert the private number of the connected set into a public number (incoming call by break-in).
- PCX B can convert the public DDI number of a user of PCX A into a private number (incoming DDI call by break-in destined for a user).



Main numbering plan of PCX B

Start	End	Base	Feature	NMT	Private
0	0	-	Main trunk group	Absorb	No

Public numbering plan of PCX B

Start	End	Base	Feature	NMT	Private
7700	7710	100	Set	-	-
7711	7720	-	Secondary trunk group	Keep	No

ARS table of PCX B

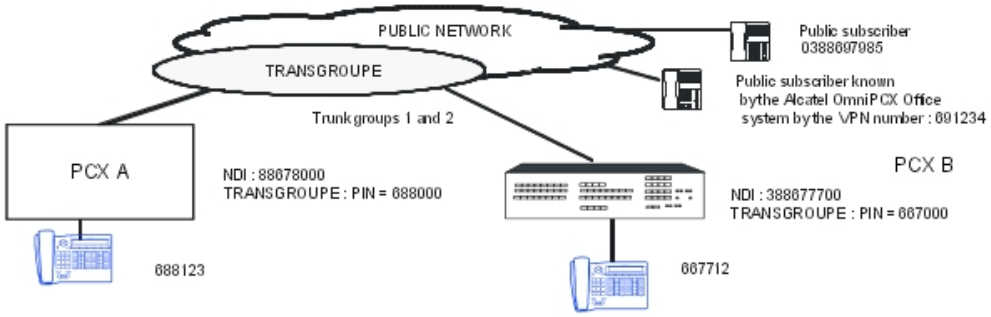
Network	Prefix	Ranges	Substitute	TrGp list	Called Party (ISVPN/H450)	User com.
Pub	03886777	11 - 20	31	1	Heterogen.	

Note:
Private -> public conversion requires the full public number (ABPQMCDU or NPANXXMCDU) to be entered in the ARS (and not only the MCDU).

In PCX B, these settings make the following services available:

- break-in: a public network subscriber dials 0388677711. PCX B receives the call and analyses 7711 in the DDI numbering plan. The full number is handled by the ARS table and converted into the private number 3111. PCX B can now make a private call on the QSIG link and join with the incoming public call.
- private network forcing: for example, user 3210 dials the number 00388677711; the ARS converts this public number into the private number 3111.
- break-out: user 3111 calls 0384273045; he dials 00384273045. The caller's number sent on the QSIG link is the private number 3111. In PCX B, 3111 is converted by the ARS into the public number 0388677711.

7.2.7.2 TRANSGROUPE VPN



The Alcatel-Lucent OmniPCX Office Communication Server PCX B, as a member of Transgroupe (PIN = 667000) must be configured to:

- make direct private calls without prefix (internal destination).
- make public calls after dialling an outgoing prefix (0) with automatic insertion of the outgoing prefix on Transgroupe (0).

Main numbering plan of PCX B

Start	End	Base	Feature	NMT	Private
0	0	-	Main trunk group	Absorb	No
68	68	-	Secondary trunk group	Keep	Yes
69	69	-	Secondary trunk group	Keep	Yes

ARS table of PCX B

Network	Prefix	Ranges	Substitute	TrGp list	Called Party (ISVPN/H450)	User com.
Pub		-	0	1	Heterogen.	
Priv.	68	-	68	2	Heterogen.	
Priv.	69	-	69	2	Heterogen.	

- Trunk group list 1

TrGp list	Index	TrGp.	Char.	Access digits	Authorisation code	Tone/Pause
1	1	-	-	-	-	-

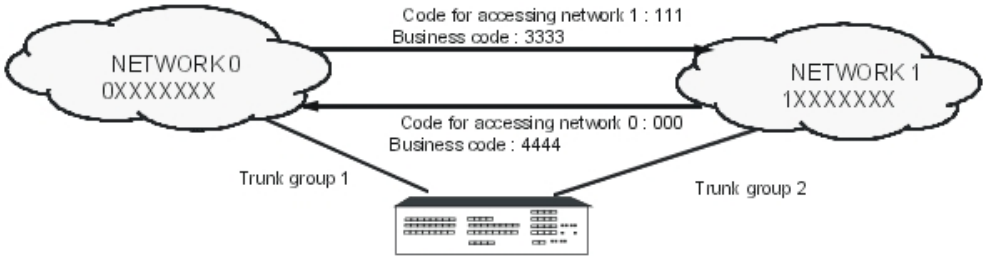
- Trunk group list 2

TrGp list	Index	TrGp.	Char.	Access digits	Authorisation code	Tone/Pause
2	1	-	T	-	-	-

The table below summarises the different types of possible outgoing calls with the values entered in the "called party number" and "caller number" fields (PCX B).

Outgoing calls	Called party number	Caller number
Call to public network	Number dialled: **0388697985** Num. plan: public	Public NDI + MCDU DID: **388677**700 + **7712** Num. plan: public
Internal call in Transgroupe	Number dialled: 688123 Num. plan: private	Internal prefix + MCDU DID: **66**7000 + **7712** Num. plan: private
Call to public network by Transgroupe	Number dialled: **691234** Num. plan: private	Internal prefix + MCDU DID: **66**7000 + **7712** Num. plan: private

7.2.7.3 MULTI-CARRIER CONFIGURATION



When a number beginning with 1XXXXXXX (belonging to network 1) is dialled from network 0, the access prefix 111 and the client code 3333 are sent from network 0 to network 1.

Main dialling plan

Start	End	Base	Feature	NMT	Private
0	0	-	Main trunk group (ARS)	Absorb	No

ARS table

Network	Prefix	Ranges	Substitute	TrGp list	Called Party (ISVPN/H450)	User com.
Pub		-		1	Heterogen.	
Pub	0	-	0	2	Heterogen.	
Pub	1	-	1	3	Heterogen.	

- Trunk group list 1

TrGp list	Index	TrGp.	Char.	Access digits	Authorisation code	Tone/Pause
1	1	-	-	-	-	-

- Trunk group list 2

TrGp list	Index	TrGp.	Char.	Access digits	Authorisation code	Tone/Pause
2	1	-	-	-	-	-
	2	-	-	000	01	-

- Trunk group list 3

TrGp list	Index	TrGp.	Char.	Access digits	Authorisation code	Tone/Pause
3	2	-	-	-	-	-
	1	-	-	111	02	-

Authorisation code table

Index	Authorisation code
01	4444
02	3333

When the user dials 0 0XXXXXXX, the ARS table forces the use of network 0 and sends the number 0XXXXXXX; the overflow operation allows the use of network 1 and sends the number 000 4444 0XXXXXXXX.

When the user dials 0 1XXXXXXX, the ARS table uses public trunk group 2 and sends the number 1XXXXXXX; the overflow operation allows the use of public trunk group 1 and sends the number 111 3333 1XXXXXXXX.

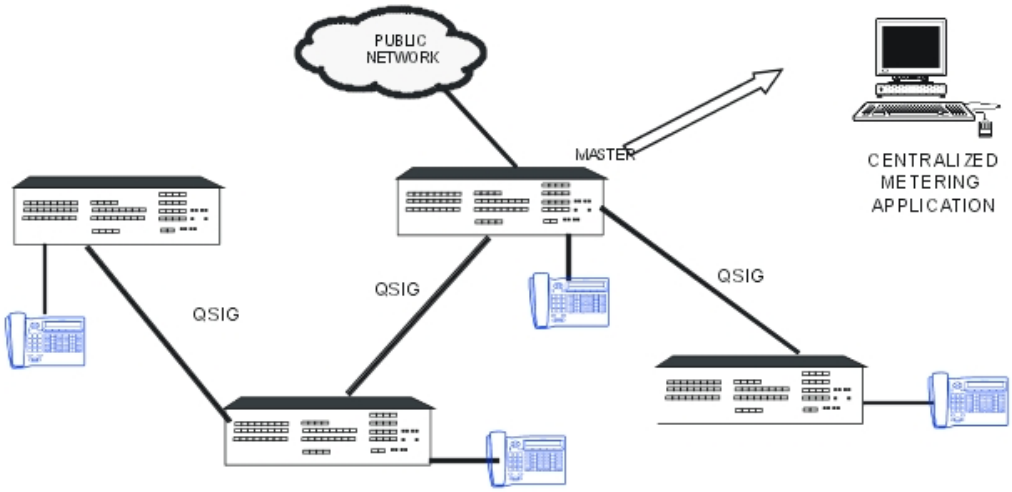
Any number beginning with 0X, where X is other than 0 or 1, uses public trunk group 1 (the default).

7.3 Metering - ISVPN+

7.3.1 Detailed description

ISVPN+ is used for a network of Alcatel-Lucent OmniPCX Office Communication Server systems linked together by digital leased lines with the QSIG-BC protocol.

The principal use of ISVPN+ is for centralized metering.



For all incoming and outgoing calls made within the network, the master system (the one connected to the public network) gathers the required information and sends it to a centralized metering application. The following information is transmitted to the master system:

- outgoing call: all the data presented in the following paragraph is managed at the caller's system level then transmitted to the master system. The flags characterizing the call are accumulated through the different systems during transmission to the master.
- incoming call: the number "transmitted" to the called party and the various flags are generated by the master system. During the setup of a communication with the called party, the flags characterizing the call are accumulated through the different systems. The number of the charged caller, the metering node number and the accumulated flags are forwarded to the master system with the connection message.

DATA TRANSMITTED

This paragraph describes the information which is transmitted to the master system by the other systems in the network; this data is conveyed by the QSIG protocol UUS.

Global data: Node number

This datum (unique value 0 to 127; by default: 255) identifies the system in the network.

- by OMC (Expert View), select: **External Lines** -> **Protocols** -> **ISVPN Protocol** -> **Node Number**. This information is only used by the metering application (not used in a telephone context). The node number indicated is the one to which the charged user is connected.

Data relative to each communication

- "transmitted" number: number resulting from the NMT conversion of the number dialed after analysis in the main numbering plan (or NMT conversion of the number received after analysis in the incoming public call numbering plan); it is thus possible to compare the number sent (to the ARS table) by the system with the original number dialed.
- charged user: This datum depends on the type of call:
  - outgoing call or break-out: caller
  - incoming call or break-in: user having answered the call; this user may be different to the called user (forwarding, call pick-up, etc.)

- transfer: user who is the destination of the transfer

- flags characterizing an ARS call:

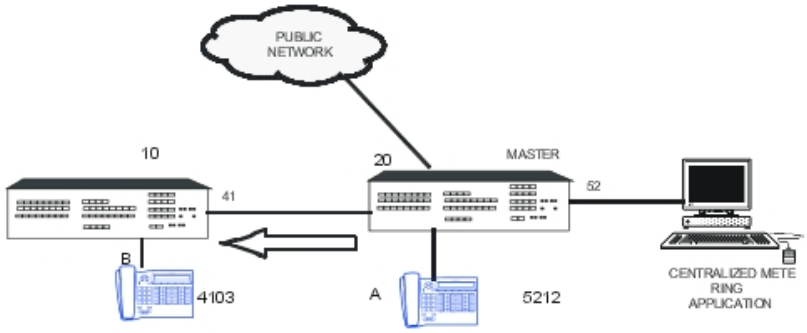
• by OMC (Expert View), select: **Numbering** -> **Automatic Routing Selection** -> **ARS Table** -> **Option: Metering**:
  • forcing onto private network (private): this flag indicates whether an outgoing call has been rerouted onto leased lines by the ARS.
  • overflow: this flag indicates whether the trunk group used for the current call has been obtained after overflow by the ARS.

- complementary services: This data indicates the services activated in order to carry out the current call:
  - substitution (DISA transit)
  - use of the ARS table
  - homogenous ISVPN call
  - VPN call (Transgroupe for example)
- supplementary network facility: indirect access to an operator
- on-line metering request in the event of break-out

EXAMPLES

Local call in the network

A (5212) calls B (4103) by dialing 4103.

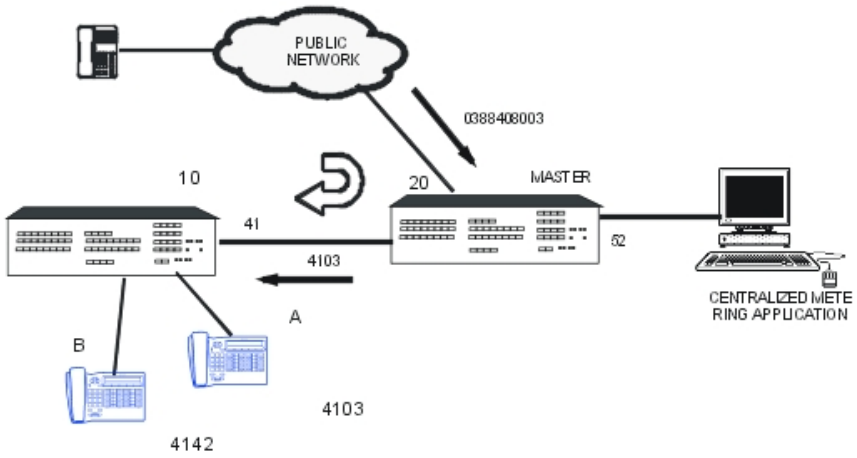


Information transmitted:

- Charged user: 5212
- Number of the metering node: 20
- Transmitted number: 4103

Break-in

A public network user calls A (4103) by dialing 0388408003. A is forwarded on B (4142).

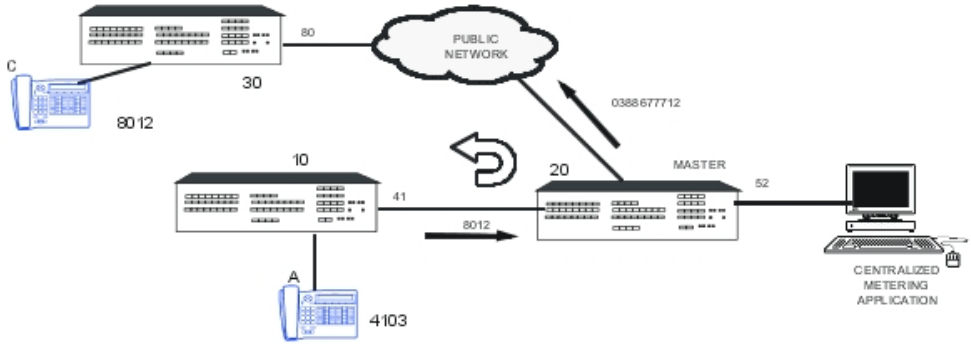


Information transmitted:

- Charged user: 4142
- Number of the metering node: 10
- Transmitted number: 4103

Break-out

A (4103) calls C (8012) by dialing 8012.



Information transmitted:

- Charged user: 4103
- Number of the metering node: 10
- Transmitted number: 8012

7.4 Clock Synchronization

7.4.1 Overview

7.4.1.1 SYNCHRONIZATION IN MODULES

Note:

The digital accesses (T0, T2, etc.) in an add-on module can under no circumstances serve as synchronizing accesses for the system (it is impossible to feed the clock back from an add-on module to the basic module CPU over an HSL link).

If the system includes digital accesses, then there are several eventualities:

- **Case 1:** No access in main module, all accesses are in an add-on module:
  - The accesses will try to supply the clock to the system, and the system will refuse.
  - System message 51 - Clock Problem; the system operates on the local clock.
- **Case 2:** There is a T2 in the add-on module and a non-permanent level 1 T0 in the basic module:
  - If the T0 is in communication, its level 1 is therefore established and it is the T0 which provides the clock for the system.
  - If the T0 is not in communication, the T2 access will attempt to supply the clock to the system when it synchronizes with the network public (as in case 1). The clock supplied by T2 will be refused; a message 51 is generated; the system operates on the local clock.
- **Case 3:** There is a permanent T0 or a T2 in the basic module. Regardless of the accesses present in the add-on modules, the clock is supplied by one of the accesses in the basic module.

Conclusion: You need to equip at least one digital access in the basic module (and if possible, a permanent level 1 T2) with a priority higher that that of all accesses present in the system.

(*) : Depending on countries, T0 accesses have a permanent or non permanent level 1. In case 2, if a T0 board (with access to a permanent level 1) is present in the main module and a T2 access is present in the add-on module, the system will take the clock provided by the T0 if the highest priority has been assigned to the T0. Reminder: 0 = highest priority, 254 = lowest priority.

7.4.1.2 SYNCHRONIZATION IN NETWORKS

To avoid loopbacks in the synchronization paths, you need to define a hierarchy of network nodes.

DEFINITIONS

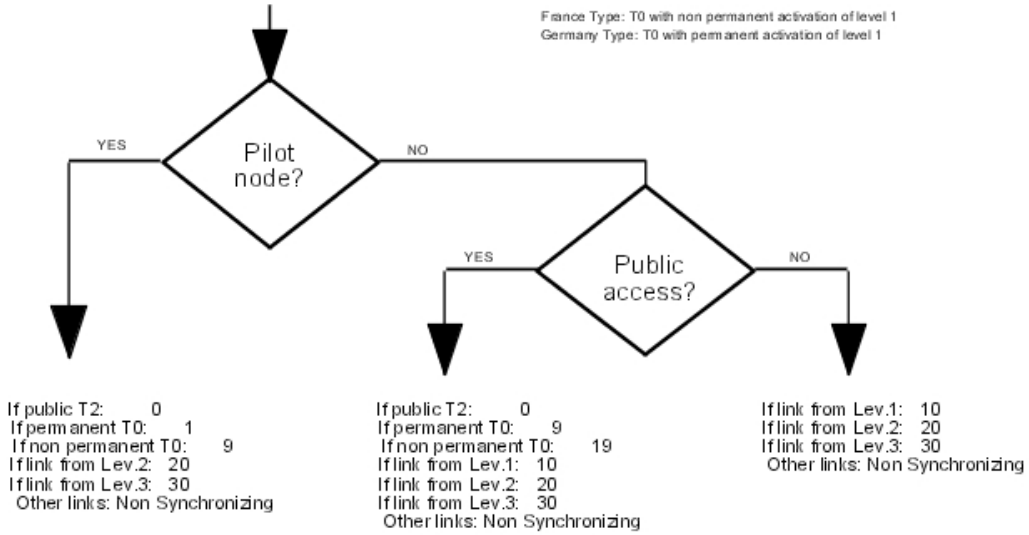
- Pilot node (= level 1): node with the most interfaces to the public network; preferably a T2.
- Level 2: node with at least one synchronizing link coming from a pilot node.
- Level 3: other nodes.

PRIORITY NUMBERS

To be able to modify and enlarge a network, you should construct a tree diagram for the synchronization of each node in the network.

A priority number must be assigned (P) to each node.

For the clock priority settings for the ISDN/QSIG boards to be taken into account, the system requires a warm reset.



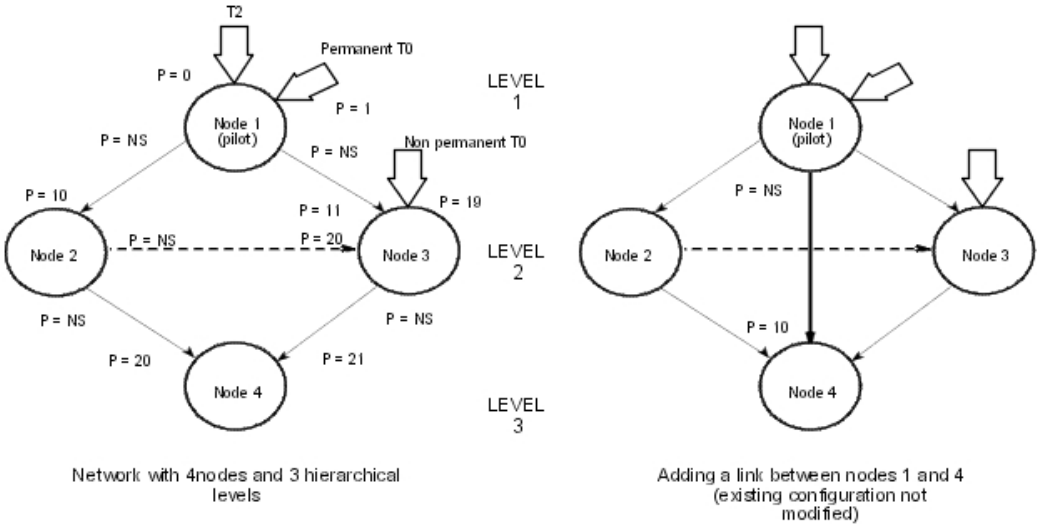
Note:

A "Non synchronising" access (OMC -> External lines -> Digital access details -> field "synchronising clock" not validated) means that the access receives the system clock and transmits it to the remote equipment.

Principles which must be respected:

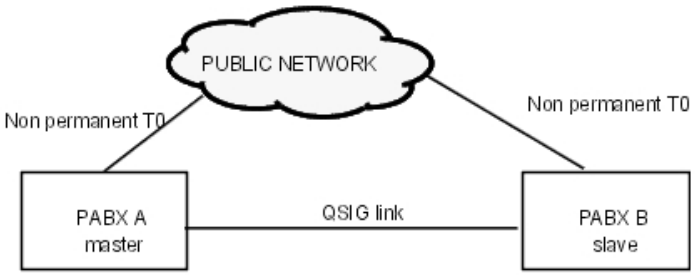
- to avoid 2 nodes from the same level synchronizing each other, assign priority 255 to the links between the 2 nodes on the system (synchronizing) side and a smaller priority value on the slave (synchronized) side.
- a node can only be enslaved on another node having an identical or lower hierarchic level.
- for any given node, assign a single priority number to links of the same type (T2, T0, leased lines).
- for any given node, a T2 link must always be assigned a smaller priority number than a T0 link.

EXAMPLES



NS: Non Synchronizing

7.4.2 Restrictions



The synchronisation of the QSIG on PCX B has priority over the synchronisation of the T0 on PCX B:

- a user belonging to A is on an external call (simultaneously or not with users on B) -> no problem.
- no external call on A: A operates on the internal clock.
  A user belonging to B makes an external call: B remains synchronised on A and is therefore not synchronous on the public network -> no data transmission from B to the network.

The synchronisation of the T0 of PCX B has priority over the synchronisation of the QSIG:

- a user belonging to A is on an external call (simultaneously or not with users on B) -> no problem.
- a user belonging to B is on an external call: A operates on the internal clock -> no data transmission between B and A via the QSIG link.
- no external call in A or B: A and B operate on their internal clocks -> no data transmission

between B and A via the QSIG link.

Synchronisation of DECT/PWT:

- if DECT/PWT are in use on a system, never use a non permanent T0 synchronisation but the internal clock -> no data transmission to the network.

7.5 Basic Accesses Configuration

7.5.1 Detailed description

From R2.0 version, digital accesses of BRA boards can be configured in T0 (with EDSS1 protocol on public lines) or DLT0 (with Q-SIG protocol on transparent private lines or public lines).

Note:

Digital accesses of MIX boards cannot be configured in DLT0.

All the accesses of the same DLT2/DLT0 board (digital leased lines) can be used to connect several PCXs as long as they are all masters or slaves.

The German ISDN network provides a particular S0-FV (S0-FestVerbindung) access (similar to using a DLT0 access) to establish private connections between 2 PCX: levels 1 and 2 are managed as BRA accesses (the PCX is always in User mode) while the protocol is managed at level 3.

7.5.1.1 INITIALISATION

7.5.1.1.1 T0

- Number of B-channels: 2 bi-directional, 0 incoming, 0 outgoing ; cannot be modified
- Protocol :EDSS1 ; may be modified in QSIG to create a DLT0 basic access on a BRA board or a S0-FV access on a MIX board of the German market.
- Layer 1 / Layer 2 Mode: User (TE); cannot be modified while Protocol = EDSS1.
- Synchronisation priority: 10 ; modifiable
- TEI Management: Point-to-point ; fixed TEI = 0 ; modifiable
- Network type: Public ; modifiable.

7.5.1.1.2 DLT0

Initialisation in DLT0 mode occurs when TO (EDSS1) accesses switch to DLT0 (QSIG) via OMC.

- Default number of B-channels: 1 bi-directional, 0 incoming, 0 outgoing
- Protocol: QSIG; may be modified in EDSS1 to redefine a T0 basic access on a BRA board.
- Layer 1 / Layer 2 Mode: User (TE); modifiable in network (NT).
- Synchronisation priority: 210 ; modifiable
- TEI Management: Point-to-point ; fixed TEI = 0 ; modifiable
- Network type: Private; modifiable.

Note:

When access is configured in network, synchronisation parameters are no longer modifiable. Access is synchronised by its system and transmits the clock to the remote system.

7.5.1.2 CONFIGURATION

All configurations are carried out by OMC (Expert View): **External lines -> External Access Table -> Digital Access: Details**

7.5.1.2.1 Conversion of a T0 access into a DLT0 access

When booted up, all accesses by BRA boards are configured as T0 accesses. Conversion of a T0 access into a DLT0 access is carried out by OMC (see screen below) in modifying the following parameters for each access:

- Protocol = QSIG
- Layer 1 / Layer 2 Mode = User (default value if the QSIG protocol is used) or Network.

This change results in the following parameters:

- Synchronising clock: Yes if User, or No (in grey) if Network.
  - If User: Yes
  - If Network: No (in grey)
- Synchronisation priority:
  - If User: 210
  - If Network: No (in grey)
- B-channels specialisation:
  - If User: Allocation = Descending; Collision = Slave
  - If Network: Allocation = Ascending; Collision = Master
- Number of B-channels: 1
- Public Network: No (in grey)
- TEI Management: Point-to-point (in grey)
- Automatic TEI negotiation: Non (in grey)
- Fixed TEI: 0 (in grey)

In User, validation (OK key) only relates to the selected access while in Network, validation also relates to the associated access.

7.5.1.2.2 Conversion of a DLT0 access into a T0 access

The return of a DLT0 access to a T0 access is carried out by OMC (same screen as before) in modifying the following parameters:

- Protocol = EDSS1
- Layer 1 / Layer 2 Mode = User (in grey).

This change results in the following parameters:

- Synchronising clock: Yes.
- Synchronisation priority: 10
- B-channels specialisation: Allocation = Ascending; Collision = Master (in grey)
- Number of B-channels: 2

- Public network: Yes
- TEI Management: Point-to-point
- Automatic TEI Negotiation: No
- Fixed TEI: 0

Note:
Some modifications require a warm reset (must be performed at the OMC prompt).

7.6 Interoperability with Extended Communication Server

7.6.1 Overview

7.6.1.1 Introduction

The Extended Communication Server is used in association with an OmniPCX Office to provide the OmniPCX Office with additional services:

- The Extended Communication Server Telephone pack offering the following voice services:
  - Unified messaging (e-mail notification)
  - Making calls directly from contact sheets
  - Click-to-call
  - Call forwarding management
  - Nomadic mode set-up
  - Downloading a pre-configured PIMphony Team Application
  - Calls notification
- From the Extended Communication Server Release 4.1, the following features based on the SIP protocol, using the user's virtual desktop:
  - Free Remote Worker
  - Peer to Peer communication
  - WEB accessibility

These services are available when the communication between the OmniPCX Office and the Extended Communication Server is established. The system is then called a converged system.

The solution usually proposed is an Extended Communication Server associated with an OmniPCX Office (Business).

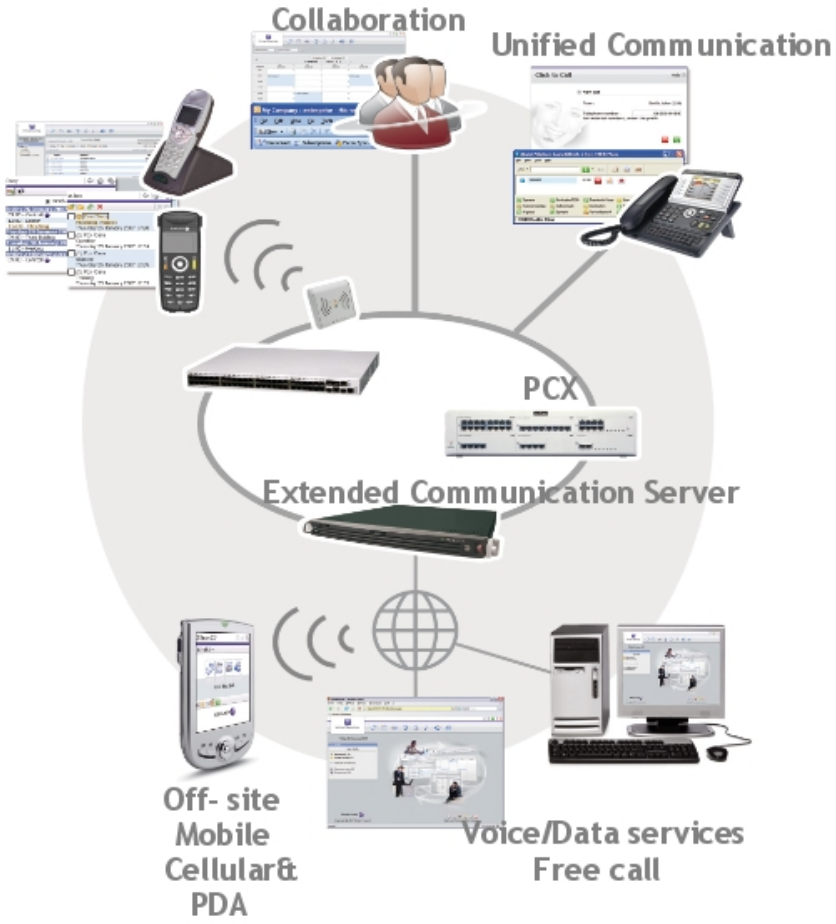


Figure 7.8 : OmniPCX Office/Extended Communication Server converged Services (Global Overview)

7.6.1.2 OmniPCX Office and Extended Communication Server Compatible Versions

	OmniPCX Office version 4.1	**OmniPCX Office version 5.0**	**OmniPCX Office version 5.1**	**OmniPCX Office version 6.0**	**OmniPCX Office version 6.1**	**OmniPCX Office version 7.0**
Extended Communication Server version 3.14	Compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible
Extended Communication Server version 3.14 + patch	Compatible	Compatible	Compatible	Compatible	Compatible	Not compatible

	OmniPCX Office version 4.1	OmniPCX Office version 5.0	OmniPCX Office version 5.1	OmniPCX Office version 6.0	OmniPCX Office version 6.1	OmniPCX Office version 7.0
Extended Communication Server version 3.15	Compatible	Compatible	Compatible	Compatible	Compatible	Not compatible
Extended Communication Server version 4.0	Compatible	Compatible	Compatible	Compatible	Compatible	Compatible
Extended Communication Server version 4.1	Not compatible	Compatible with restriction (1)	Compatible with restriction (1)	Compatible with restriction (1)	Compatible with restriction (1)	Compatible

(1) Restrictions:

- The virtual Nomadic sets are not created automatically, the OmniPCX Office administrator must define them
- The Extended Communication Server administrator must define the Recall Prefix
- The OmniPCX Office 5.1 release should be equal or greater than 033.001
- The OmniPCX Office 6.1 release should be equal or greater than 004.001

7.6.1.3 Activating the Convergence

On OmniPCX Office:

A licence is required to activate the convergence between the OmniPCX Office and the Extended Communication Server.

In Computer-Telephone Integration licence, the PIMphony unified service must be activated.

- Activate the voice/data convergence service

On Extended Communication Server:

1. Detect the OmniPCX Office
2. Activate the voice/data convergence service

7.6.1.4 Synchronizing the OmniPCX Office Phones

7.6.1.4.1 CREATING A USER GROUP

Manual User Creation

The administrator of the Extended Communication Server can create manually user accounts and can associate them with one of the synchronized OmniPCX Office sets. Therefore, OmniPCX Office subscribers will have a user account created into the Extended Communication Server that allows them to manage their set through their Virtual desktop.

Each user account includes an identifier and a password requested to open the virtual desktop.

Note:

It is possible to create a user account without any OmniPCX Office set being associated with it.

Automatic User Creation

The user import operation retrieves information about the telephone terminals available in the OmniPCX Office and automatically creates the corresponding users in the Extended Communication Server directory. The users created will be in the group indicated in the Group name text field.

- Click **Import** now
  The following actions will be performed automatically:
  - A new group is created in the directory. The name of this group will be that entered in the Group name text field
  - The Appliance polls the OmniPCX Office in order to retrieve the appropriate information, such as the internal extension number, and the name and first name associated with this terminal
  - This list is used to create the users automatically in the Extended Communication Server LDAP directory.

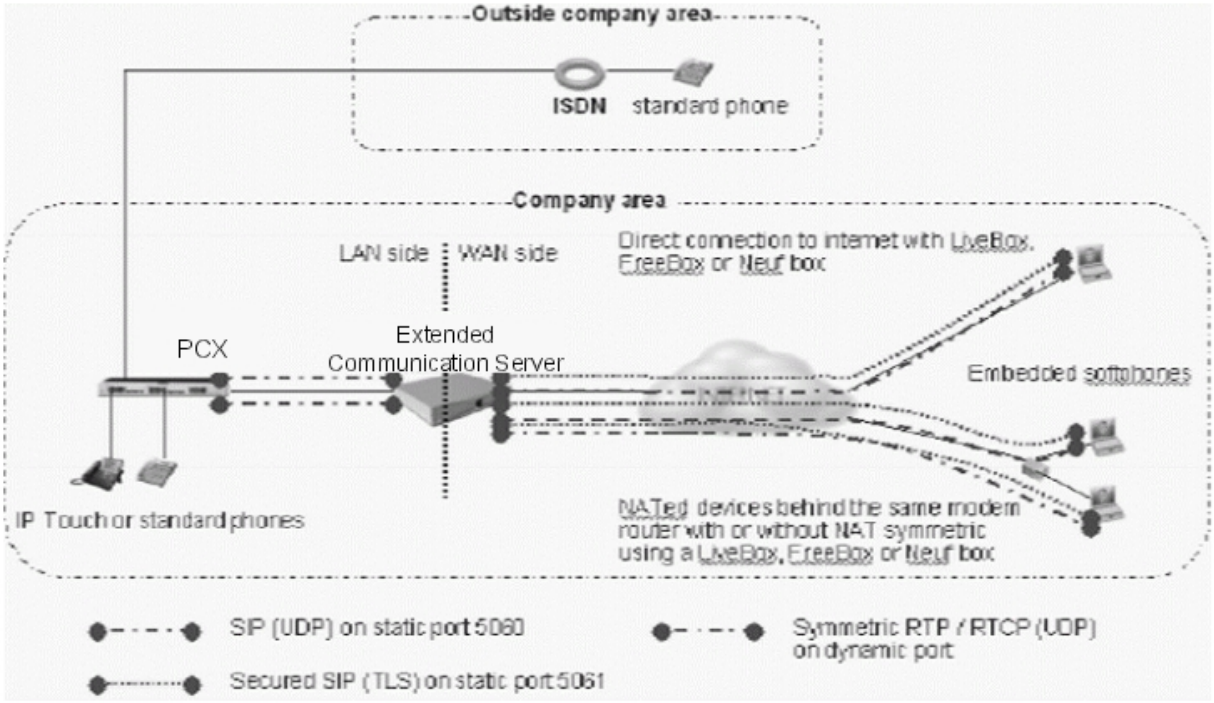
  Note:
  It is then possible to change the name of the group and the properties of each user.

7.6.2 SIP features on Virtual Desktop

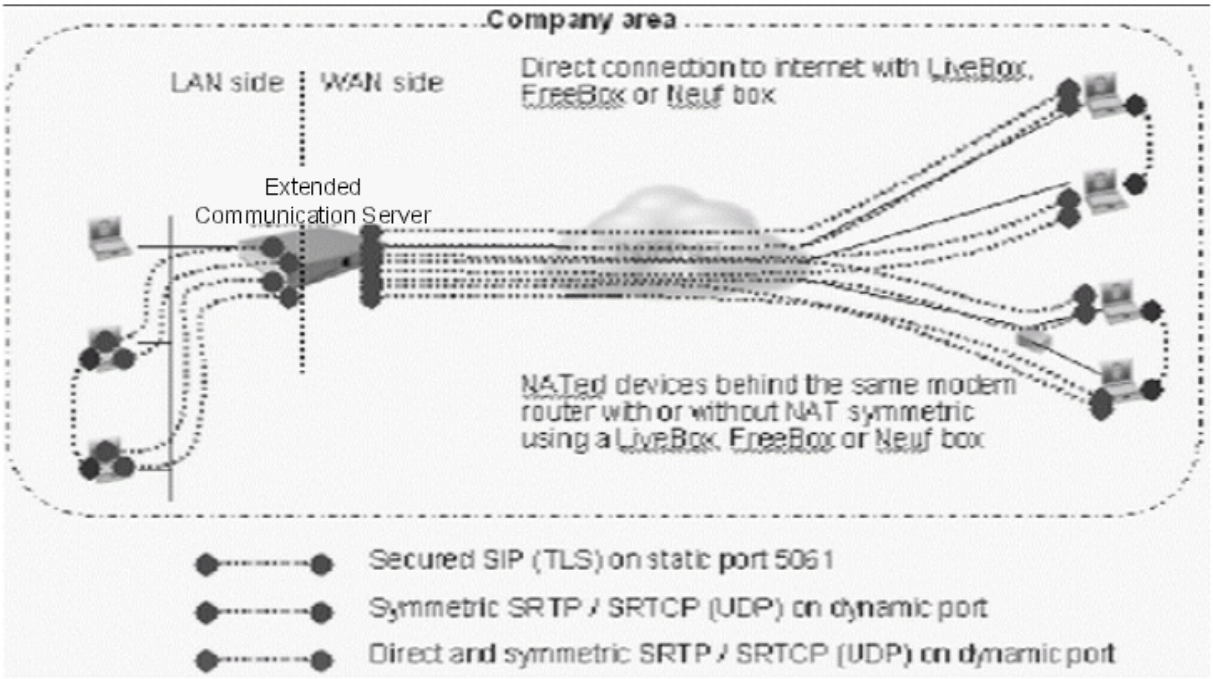
7.6.2.1 Introduction

Extended Communication Server Release 4.1 offers the following new telephony features based on the SIP protocol:

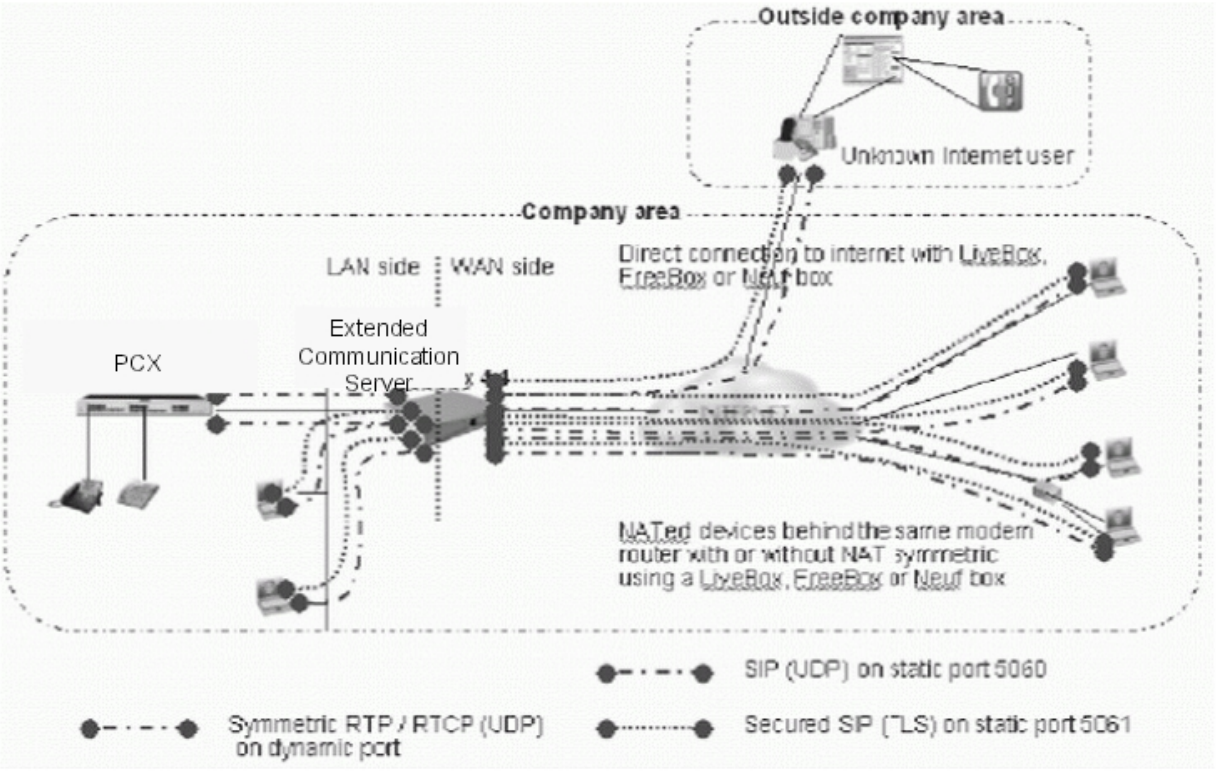
- **Free Remote Worker**: A user of the virtual desk can now make free calls through the Internet using the embedded softphone. He can also be called over this phone, as long as the nomadic feature is correctly configured



- **Peer to Peer communication**: Two users logged in on the Virtual desk can talk directly and securely with the embedded softphone
  To enable these two use cases, the virtual desk now features the notion of presence that relies on the embedded softphone, and from this notion of presence, export means to make secure calls to "present" users. The Telephony Integration Pack has also been improved to allow Extended Communication Server users to benefit from the presence information to update their nomadic configuration dynamically.



- **Web accessibility**: An Internet user can make calls through the Internet using a temporary embedded softphone. An Internet user can call directly company employees (OmniPCX Office devices or embedded softphones) through the company Website, by clicking a URL



7.6.2.2 Remarks

- The SIP communications are secured only within a Peer to Peer communication
- The browser must allow the ActiveX to run on the PC
- The Firewall must be configured in order to allow SIP communications

7.6.3 Configuring the OmniPCX Office

To be able to use the features (Free Remote Worker, Peer to Peer communication, WEB accessibility) offered by the Extended Communication Server, OmniPCX Office must be configured:

- The VoIP feature must be activated.

  The communications are based on IP trunking over SIP instead of H.323. For this reason, the usual ARS must be configured to activate the SIP protocol

7.6.3.1 Enabling SIP as VoIP Protocol and Setting VoIP Parameters

Refer to module Public SIP Trunking - Configuration procedure

7.6.3.1.1 Configuring the Number of VoIP Trunk Channels

By default, H.323 is the VoIP protocol enabled on the OmniPCX Office and the number of DSP channels reserved for VoIP (H.323 or SIP) is equal to 0.

VoIP protocol must be switched to SIP and the number of channels for VoIP trunks must be increased to a non-null value.

1. By OMC (Expert View):

System > Voice over IP > VoIP: Parameters > General tab

2. Review/modify the following attributes:

Number of VoIP-Trunk Channels	Enter the number of channels used for SIP trunking
VoIP Protocol	Select **SIP**
Quality of IP service	Select the QoS type used for the remote SIP gateway VoIP calls

3. Do not check the "RTP Direct" box
4. Confirm your entries
5. If the **VoIP Protocol** has been switched from **H323** to **SIP**, you are requested to reset the VoIP boards.

7.6.3.1.2 Configuring the Gateway Timers (Optional)

Refer to module Configuring H323 Gateway - Hardware configuration § Configuring the Gateway timeouts (optional)

1. By OMC (Expert View):

System -> Voice on IP -> VoIP: Parameters -> Gateway tab

2. The parameters have standardized values, do not change them without prior analysis

RAS Request Timeout	Maximum authorized response time for a RAS request ("Registration, Admission, Status") made to the gatekeeper; between 10 and 180; default value = 20
Connect Timeout	Maximum authorized time interval between initialization and connection; value between 10 and 1200; default value = 500
Gateway Presence Timeout	Determines the presence of a remote Gateway; value between 10 and 600; default value = 50
Connect Timeout	Maximum authorized time interval between initialization and connection; value between 10 and 1200; default value = 500
H.245 Request Timeout	Maximum authorized response time for an H.245 request; value between 10 and 60; default value = 40
SIP: End of dialing Timeout	Default value = 5

The "**End of Dialling table used**" box can be checked or not (optional).

The "**End of Dialling table used**" is checked to define the end of dialing detection. The system uses the end of dialling prefix table to ascertain the length (number of digits) of the

numbers transmitted. A counter, equal to or superior than 0, is associated with each prefix. When a prefix has not been configured in this table, the system uses a reference counter (see paragraph § Configuring the “End of Dialling Table”).

7.6.3.1.3 Configuring the SIP Parameters

Configuring the Local Domain Name (optional)

By default, the **Local Domain Name** field is empty.

It is not mandatory to enter a **Local Domain Name**. It is used only when the OmniPCX Office has a subscription to an Internet access provider.

1. By OMC (Expert View):

System -> Voice on IP -> VoIP: Parameters -> SIP tab

2. Review/modify the following parameter:

Local Domain Name	This name is used in the domain part of the FROM header. It can be, for example, the domain name of the provider.

Configuring the Timer

Refer to module Public SIP Trunking - Configuration procedure § Configuring Timers

1. By OMC (Expert View):

System -> Voice on IP -> VoIP: Parameters -> SIP tab

2. Review/modify the following parameters:

Timer T1	Retransmission timer: waiting duration before re-sending a request. Default value: 1000 ms
Timer T2	Response timer *Note:* *T1 and T2 timers are defined in the RFC3261.*
Number of Retries	Maximum number of retries.

Configuring the Registration Parameters

Refer to module Public SIP Trunking - Configuration procedure § Configuring Registration Parameters

1. By OMC (Expert View):

System -> Voice on IP -> VoIP: Parameters -> SIP tab

2. In the **Registration** pane, check the **Requested** box
3. Review/modify the following parameters:

Registered User Name	Enter the name provided by the provider. This can be for example the installation number. In this field is left empty, the name of the main VoIP board is used.
Expiration Time	Enter the validity time of the registration. Default value: 3600 s

4. If DNS SRV is not used, review/modify the following attributes:

Registrar IP Address	Enter the Registrar IP address.
Port	Enter the port number to be used for registration.
Outbound Proxy IP	Enter the Outbound Proxy IP address.

5. If DNS SRV is used, check the **DNS SRV** box and review/modify the following attributes:

Registrar Name	Enter the Registrar name.
Outbound Proxy	Enter the Outbound Proxy name.

6. OmniPCX Office supports the Digest authentication scheme (MD5). If OmniPCX Office must authenticate to the provider, enter the authentication parameters:

User Name	Enter the user name (login) for authentication.
Shared Secret	Enter the password associated with the user name for authentication.
Registered Realm	Enter the realm name.

7.6.3.2 *Configuring the "End of Dialling Table"*

If the "**End of Dialling table used**" box has been checked in the **Gateway** tab (see paragraph § Configuring the Gateway Timers (Optional) , the "**End of Dialling Table"**must be configured.

1. By OMC (Expert View):

System -> Numbering -> End of Dialling Table

2. Configure the **Prefix** and the **Counter** with the desired embedded softphone dialling number.

7.6.3.3 *Configuring the IP Trunking traffic sharing and baring*

Refer to module Link Categories - Configuration procedure .

- Selecting the VoIP trunk and setting the traffic sharing and the barring
  - By OMC (Expert View):

for access: **System -> External Lines-> List of accesses -> Details -> Link Cat**

- Adding the VoIP trunk in the trunks group and setting the traffic sharing and the barring
  - By OMC (Expert View):

for the trunk groups: **System -> External Lines -> List of Trunk Groups -> Details -> Add -> Link Cat**

- Selecting the "Traffic Sharing Matrix"
  - By OMC (Expert View):

System -> Traffic Sharing and Barring-> Traffic Sharing Matrix

- Selecting the "Barring Matrix"
  - By OMC (Expert View):

System -> Traffic Sharing and Barring-> Barring Matrix

- Creating restriction tables
  - By OMC (Expert View):

System -> Traffic Sharing and Barring-> Barring Tables

The traffic sharing and barring must be consistent with the OmniPCX Office.

7.6.3.4 Configuring the LAN/IP Parameters

OmniPCX Office and Extended Communication Server belong to the same private network (LAN). If the Extended Communication Server is the default gateway to the Internet, then it must be set as the default gateway of the OmniPCX Office.

1. By OMC (Expert View):

System -> Hardware and Limits -> LAN/IP Configuration -> LAN Configuration tab

2. Modify the **Default Router Address** parameter

7.6.3.5 Configuring the Numbering

7.6.3.5.1 Configuring the Internal Numbering Plan

- Configuring the numbering plan in order to be able to call the embedded softphone.

.

- By OMC (Expert View):

System -> Numbering -> Numbering Plans -> Internal Numbering Plan tab

7.6.3.5.2 Configuring the Private Numbering Plan

The private numbering plan must be configured for the embedded softphone to access the Alcatel-Lucent OmniPCX Office.

- By OMC (Expert View):

System -> Numbering -> Numbering Plans -> Private Numbering Plan tab

7.6.3.5.3 Configuring the ARS Table

For the SIP Trunking, the ARS table must be configured in order to allow the internal user to call the embedded softphone.

Configuring the “Automatic Routing: Prefixes”

1. By OMC (Expert View):

System -> Numbering -> Automatic Routing Selection -> Automatic Routing: Prefixes

2. Right-click in the ARS OMC window and select **IP parameters** to display the IP parameters fields
3. Right-click in the ARS OMC window and select **Add**
4. Enter the following parameters:

table 7.92 : Common fields

Activation	Enter **yes**
Prefix	Enter the same value as the value used in the internal numbering plan
Ranges	For example, enter 00 - 99: SIP sets numbers range used in the Extended Communication Server
Substitute	Enter the replacement prefix
TrGpList	Enter the index of the VoIP trunk group list used to make SIP trunking calls (Trunk group configured with the VoIP trunks)

table 7.93 : IP parameters fields

Destination	Select **SIP Gateway**
IP Type	Enter **Static**
IP Address	Enter the Extended Communication Server public IP address
Gateway Alive Protocol	Enter **ICMP**
Gateway Alive Timeout/s	Enter **300** (default value)
Gateway Bandwidth	Enter a bandwidth value, reserved for voice on IP to the remote gateway, depending on network traffic
Gateway Parameters Index	Enter the index to connect you to the "Gateway parameters" window. It enables you to configure authentication for SIP

Configuring the Gateway Parameters (Optional)

The **Gateway Parameters** entry is a new entry added in the ARS configuration to configure the SIP authentification.

1. By OMC (Expert View):

System -> Numbering -> Automatic Routing Selection -> Gateway parameters

2. Enter the following parameters:

Login	see module Interoperability with Extended Communication Server - Configuring the Extended Communication Server § Information necessary for ARS configuration
Password	see module Interoperability with Extended Communication Server - Configuring the Extended Communication Server § Information necessary for ARS configuration
Domain name	see module Interoperability with Extended Communication Server - Configuring the Extended Communication Server § Information necessary for ARS configuration
Realm	see module Interoperability with Extended Communication Server - Configuring the Extended Communication Server § Information necessary for ARS configuration
RFC3325	Enter **Yes**
SIP Port Distant	Enter **5060**

Configuring the Trunk Group Lists Parameters

1. By OMC (Expert View)

System -> Numbering -> Automatic Routing Selection -> Trunk Group Lists

2. Enter the following parameters

Index	Enter the trunk group index configured with IP trunk
Provider/Destination	Enter **None**
Auth.Code ID	Enter **None**
Tone/Pause	Enter **None**

7.6.4 Configuring the Extended Communication Server

7.6.4.1 Prerequisites

Before converging an Extended Communication Server with an OmniPCX Office, some minimum mandatory configurations must be set on the Extended Communication Server side.

- Activating the software licence
- Synchronizing Extended Communication Server with OmniPCX Office
  - Setting the system clock

    The clock must be in conformity with the OmniPCX Office "**Date and Time**" parameters.

    In the "system clock setting" menu:
    - Enter the **Date and Time**
- Setting the network parameters
  When an Extended Communication Server is implemented in an OmniPCX Officeprivate

network, the network parameters must be configured to enable the communication with the OmniPCX Office.
Usually, the Extended Communication Server and the OmniPCX Office belong to the same network.

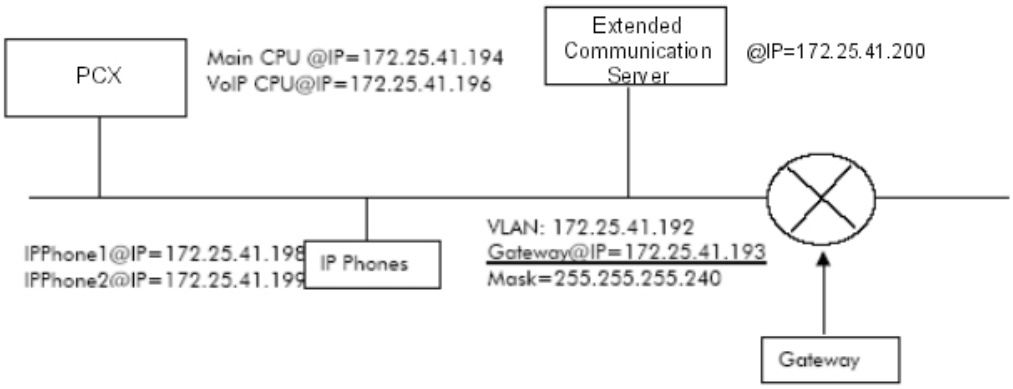
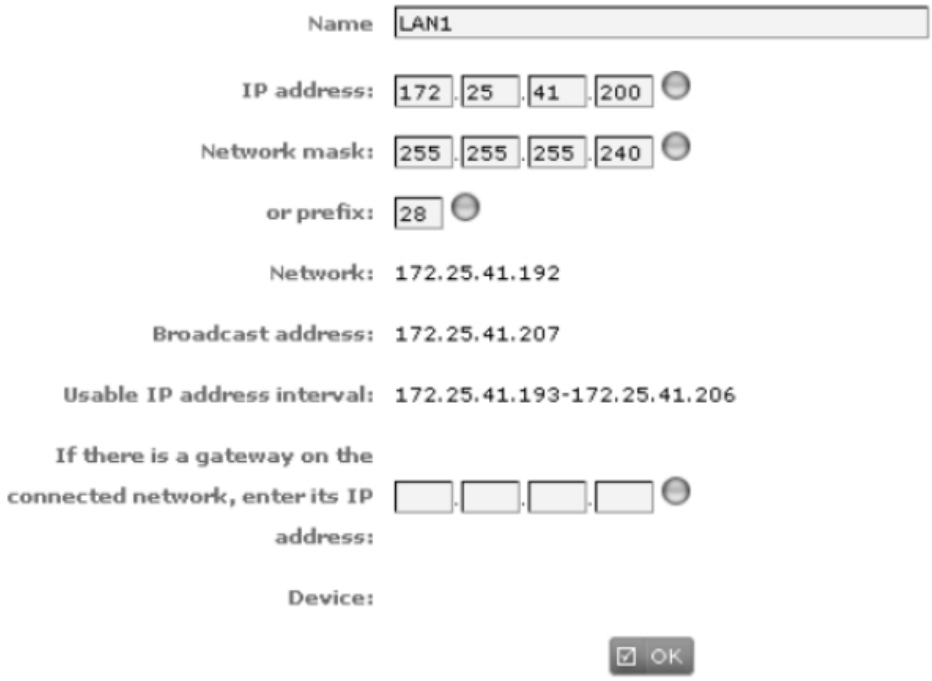


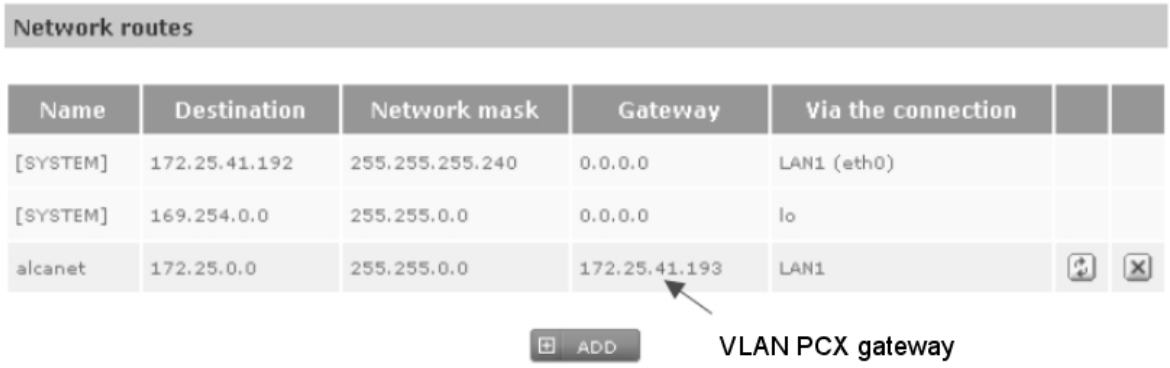
Figure 7.12 : Network topology example

- Configure the Extended Communication Server IP address
  In our example:



- If a gateway is present on the connected network, set a default route to communicate with the other network

  In the "Network routes" menu, enter the gateway IP address.
  In our example:



7.6.4.2 Configuring the Extended Communication Server

To communicate with the OmniPCX Office, some parameters on the Extended Communication Server side must be set.

7.6.4.2.1 Extended Communication Server Identity Number Parameter

The Extended Communication Server Identity Number is available in the administration interface

- In the administration interface, select:

Appliance management ->Licences & Releases -> Software Releases -> Id number

7.6.4.2.2 VoIP - SIP Parameters

Prerequisite

Before setting the SIP parameters, the following services must be activated:

- Firewall
- Data convergence service
- DNS server

Configuring the SIP Parameters

Setting the Extended Communication Server SIP Connection Parameters

1. "Configuration" menu

Service management -> Telephony over Internet (VoIP - SIP) -> Configuration -> Basic configuration tab

2. Set the following parameters:

table 7.100 : Extended Communication Server VoIP configuration

SIP domain name	Enter the domain name provided by a "DynDNS" service account
Automatic creation of the associated DNS zone	Check the box
Server public IP	Enter the public IP address
Prefix of the VoIP station numbers	Enter 3, for instance, to define the number prefix of SIP sets embedded in the Extended Communication Server
VoIP stations numbering range	Enter 00 - 99, for instance to define the numbers range of SIP sets embedded in the Extended Communication Server

table 7.101 : OmniPCX Office VoIP configuration

Use this server to do VoIP-SIP	Check the box
IP Address	Enter the OmniPCX Office VoIP address
Login	Enter the OmniPCX Office login to enable the OmniPCX Office to connect to this service
Password	Enter the OmniPCX Office password to enable the OmniPCX Office to connect to this service

3. Click **OK**.
4. In the management interface, select:

Service management ->Telephony over Internet (VoIP - SIP) -> Configuration -> Advanced configuration tab

5. Set the following parameters

Port number for the SIP messages	Enter the port number used by this service to receive the VoIP data (SIP packets when using the UDP and/or TCP protocol (5060: default value)
Port number for the protected SIP messages	Enter the port number used by this service to receive the protected VoIP data (SIP packets when using the TLS protocol (5061: default value)
Protocol(s) used	Check the protocol used to send/receive the SIP packets e (UDP, DCP and TLS boxes checked (default values))
Quality of service (ToS field - hexadecimal value)	Enter 0xb8 (default value)
Definition of the port range used for the media flows (dynamic management)	Enter 8000 - 9000 (default values)

Maximum time for communications cut-off on no answer	Enter the waiting time before automatic cut-off if the called person does not answer (60: default value)
Maximum number of simultaneous VoIP connections	Enter the appropriate bandwidth (5: default value)
Maximum number of external users	Enter the maximum number of external users (this number cannot be higher than the maximum number of simultaneous VoIP connections) (5: default value)

6. Click **OK**.

Configuring the Extended Communication Server SIP Sets Parameters

1. "VoIP stations configuration" menu

Service management -> Telephony over Internet (VoIP - SIP) -> VoIP stations configuration

2. Set the following parameter

Activated	Enter "**Yes**" or "**No**" to activate or not the SIP set associated to each user account

Information necessary for ARS configuration

To set/modify the "**login, password and domain name**" parameters:

- In the management interface, select:

Service management -> Telephony over Internet (VoIP - SIP) -> Configuration -> Basic configuration tab

Refer to § Setting the Extended Communication Server SIP Connection Parameters

To set the "Realm" parameter: it is the Extended Communication Server Identity number:

- In the administration interface, select:

Appliance management ->Licences & Releases -> Software Releases -> Id number

Chapter 8

General Applications

8.1 PIMphony

8.1.1 Overview

Alcatel-Lucent PIMphony is a personal productivity tool that connects your phone terminal (dedicated set, analog or DECT wireless set) with your computer, providing enhanced usage of your telephone.

PIMphony IP is an IP phone that provides the same level of features as PIMphony associated with an actual terminal. PIMphony IP is based on Voice over IP technology (VoIP). No physical terminal is required.

Alcatel-Lucent PIMphony also provides tight integration with the most popular PIMs (Personal Information Managers) on the market, enabling them for Computer Telephony.

PIMphony also provides the following features (from OmniPCX Office R4.0 and PIMphony 5.0 and higher):

- Extended Dial by Name mode: it is possible to use the dial by name feature to search for contacts in the OmniPCX Office directory or on an external LDAP server (Lightweight Directory Access Protocol server)
- Quality of Service on PIMphony IP with the support of the G729A codec
- Embedded centralised call log feature
- Configuration of PIMphony using OMC
- PIMphony on-line updates
- Availability of PIMphony with all phone sets including the Alcatel-Lucent xAlcatel-Lucent 8 series and xAlcatel-Lucent 9 series sets.

8.1.2 Documentation

8.1.2.1 Detailed description

8.1.2.1.1 Documentation

For information and details (Installation, User Manual) about PIMphony, refer to the PIMphony On Line Help.

The PIMphony On Line Help is available either:

- from the PIMphony CD-Rom and Documentation CD-Rom: open the "aochelp.chm" file for access to the on-line help.

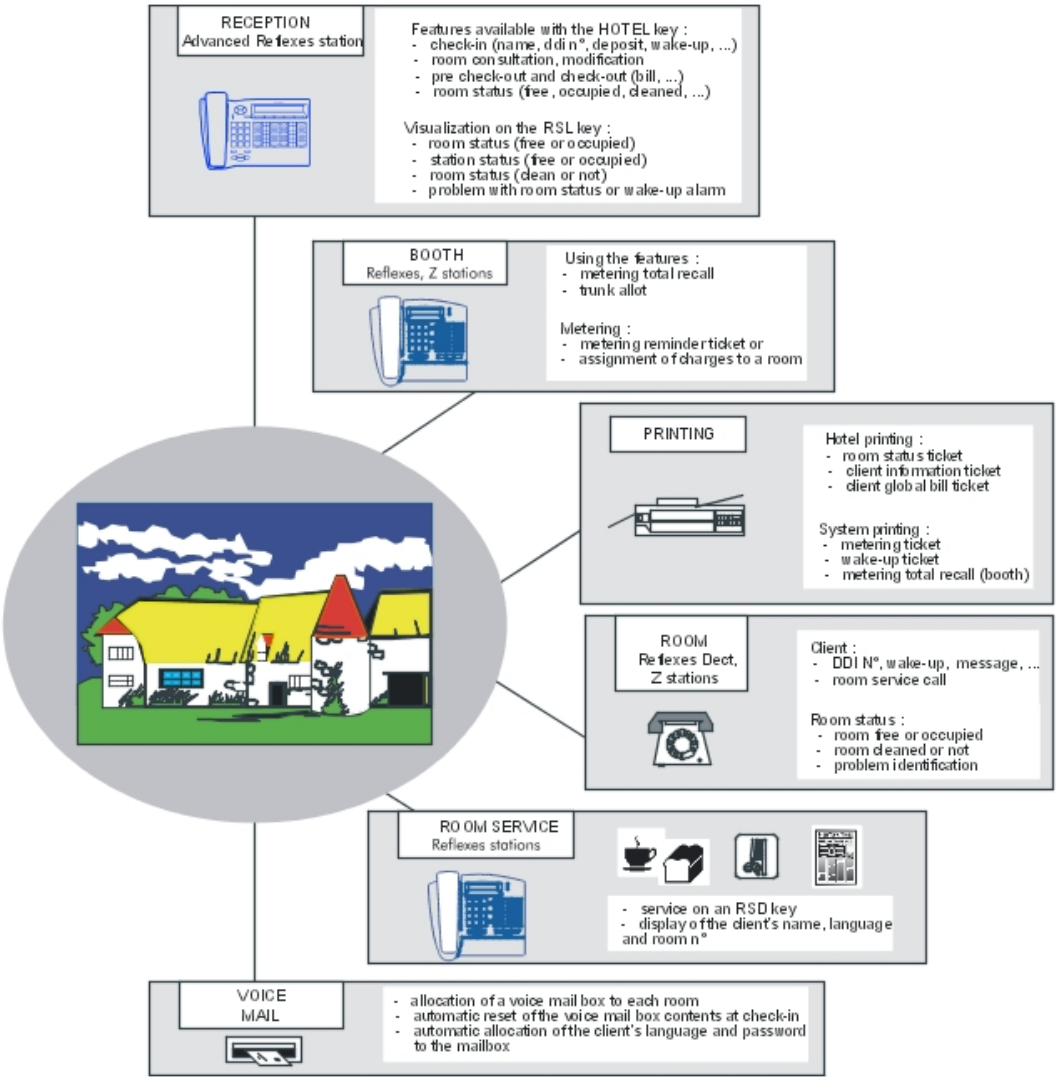
- from the PIMphony application: once the PIMphony application is installed on the PC, press the "F1" key to open the PIMphony On Line Help.

8.2 Hotel

8.2.1 General Presentation

8.2.1.1 Overview

8.2.1.1.1 ENVIRONMENT



Sets in the installation

The sets of the installation are divided up according to their types and roles:

- Reception and Attendant: Alcatel-Lucent 4039 Digital Phone, Alcatel-Lucent IP Touch 4038 Phone, Alcatel-Lucent IP Touch 4068 Phone or Advanced Reflexes sets mandatory, fitted with add-on modules
- Administration and Rooms: Alcatel-Lucent 8 series/Alcatel-Lucent 9 series or Reflexes, DECT, Z

- Room Service: Alcatel-Lucent 8 series/Alcatel-Lucent 9 series or Reflexes
- House phones: Alcatel-Lucent 8 series/Alcatel-Lucent 9 series or Reflexes, Z

Note:

Multiset is not available in Hotel mode

8.2.1.1.2 HOTEL INSTALLATION

When the system is brought into service, the OMC Easy View session allows you to specify that the installation is a hotel installation. By doing this, the system automatically creates predefined profiles (Reception set, house phone, room sets, administration sets, etc.) described below:

- the first set is the Operator Station; this Alcatel-Lucent 4039 Digital Phone/Alcatel-Lucent IP Touch 4038 Phone/Alcatel-Lucent IP Touch 4068 Phone/Advanced set in PCX mode belongs to all active operator groups as well as the default operator group.
  This set has the profile of a Reception set: it has a direct call key for the house phone and, on the add-on modules, a direct call key for each room set in the installation (up to 120 sets).
- The dedicated sets are administration sets.
- The analog (Z) sets (except fax machines and house phones) are room sets.
- Dynamic routing level 1 for administration sets: any unanswered call is routed to the voice mail unit after 12 seconds.
- Dynamic routing level 2 for administration sets: any unanswered external call is routed to the operator group after 24 seconds; for room sets, this operation only applies after customer check-in.
- Attendant station calls overflow to general level (default attendant group) after 24 seconds; for room sets, this operation only applies after customer check-in.
- The first analog (Z) interface is configured to connect a fax machine (VOICE and FAX2/3 services; no dynamic routing; protection against camp-on, barge-in and camp-on tone).
- The second analog (Z) interface is configured to connect a house phone (automatic call setup on going off-hook, delayed by 3 seconds, counter total recall at the attendant station).
- The internal dialling plan is programmed with the prefixes for "room status", "room service" and "wake-up programming".
- The public dialling plan (if the public dialling system is "open") contains 2 ranges of DID numbers: one for the attendant stations, the other for the administration sets, the house phone and the analog (Z) interface of the fax machine; the DID numbers correspond to the internal call numbers of the sets.
  The remaining ranges can be used for the room sets.
- The table of features in conversation is programmed with the default codes for the features "DND override", "trunk assign" and "counter total recall".
- all the programmable keys on dedicated sets are modifiable by the user (or by the installer).

Using the predefined profiles of the OMC Easy View session means you can avoid some of the system programming described in the "Configuration" section.

See the "Starting Up" section of the installation manual for a description of the OMC Easy View

session; this session also enables you to configure some of the key Hotel application parameters (the DDI numbers, for example) right from the initialisation stage.

8.2.1.2 Services provided

The main services proposed are listed below.

8.2.1.2.1 Administrative aspects:

Room Status

Room Status (free, occupied, cleaned, problem with room).

Check-in

Name, language, assignment of a DID No, opening of the line, restriction level (external outgoing calls), prepayment (charge credit), wake-up call, printout of a call detail record, etc.

Check an occupied room

Guest prepayment status (charge credit), review of the guest's mail box (text mail, voice mail, Reception callback request), printout of a call detail record, etc.

Pre-checkout and Check-out

Closing of the line, printout of a bill, room status, resetting of the parameters, etc.

The pre-checkout enables a guest to settle the telephone bill the day before an early morning departure, for example (external outgoing calls no longer possible), while at the same time keeping the features programmed on the phone (wake-up call, message, DID No, DND, etc).

METERING

Specific parameter settings for calculating the cost of calls on guest sets and house phones.

Standard parameter settings for calculating the cost of calls on administration sets.

Surcharge for guest communications set up with the help of Reception.

Printout of a charges record with VAT.

New voice mail integrating the hotel features

Assignment of a voice mailbox to each room.

Automatic reset of the contents of a voice mailbox at check-in.

Automatic assignment of the guest language and password to the voice mailbox.

8.2.1.2.2 Telephone aspects:

Programming of the wake-up call either by the guest or by Reception

Password

Service enabling Reception to assign guests a password.

The password can be used by guests to lock their set (prohibit external calls), to access their voice mailbox remotely and to make calls using protected account codes.

Room Service

Certain services are accessible by a simple call: for example, bar, dry cleaning, breakfast.

House phone (Phone booth)

Use of features: Trunk Assign (with counter recall) or Counting Total Recall.

During a counting total recall: printout of a charges record or assignment of charges to a set in the installation.

DND OVERRIDE

Service enabling Reception to override DND.

Account code with substitution

Service enabling a user to set up a call on one set with the account code assigned to another set.

The user makes a call in the following way: **account code prefix** + **account code** + **No. of the substitution set** (optional) + **password** (optional) + **prefix for accessing the trunk group** + **called party's No.**

8.2.2 Configuration

8.2.2.1 Configuration procedure

8.2.2.1.1 PARAMETERS TO BE CONFIGURED

This chapter presents the main parameters that need to be configured for the hotel application.

Installation numbers

- Enter the installation number, the intercity code and the international access prefix

Dialling plans

- Internal dialling plan, enter the:
  - station numbers: administration, rooms, house phones, fax, etc.
  - prefixes: wake-up call, main and secondary trunk group, Room status (see **System Parameters**), Reception call, etc.
- Public dialling plan, enter the:
  - station DID numbers: administration, Reception, fax, etc.
  - room set DID numbers (see the **VisFr** and **VisAl** features in **System Parameters**)
- Feature access codes, enter the suffixes for: consultation call, broker call, DND override (see **System Parameters**), conference, etc.

Set categories

- Declare the sets: "Administration", "Guest" or "House phone (Phone booth)" (see the **Class** feature in **System Parameters**)

Reception set

- Create a "Hotel" key (see the **Hotel** feature in **System Parameters**)
- Create the "RSL" keys for the sets: rooms, house phones, etc. (see the **RSL** feature in **System Parameters**)

Room service station

- Create the numbers for the service in the internal numbering plan

- Create a "RSD" key for each service on the Room service station (see the **RSD** feature in **System Parameters**)

House phone (Phone booth)

- Configure the house phone by using the features:
  - "Automatic call setup (on reception) on going off-hook" (or restrict the line in order to exclude outside calls. To call out, the user dials the call number for reception).
  - "Count total recall" in automatic mode (or using the manual mode from the Reception set)
- Configure the Reception set by using the features:
  - "Trunk assign" (use, for example, barring table No. 2 which only authorises internal calls)
  - "Trunk assign with count total recall" (use, for example, table No. 4 which authorises national and international calls)
  - "Count total recall" in manual mode
- Authorise the feature rights: "trunk assign" and "count total recall"
- Position the flag "count total recall if there is no charge" (see the **Count total recall** feature in **System Parameters**)

Analogue room sets

- Assign a "voice mail" virtual key to the analogue sets which will light the LED when there is a callback request from Reception or from the voice mail unit

Barring tables

- Check the link Class of Service on the sets installed
- Check the link Class of Service on the trunk group and network lines

Hotel Parameters

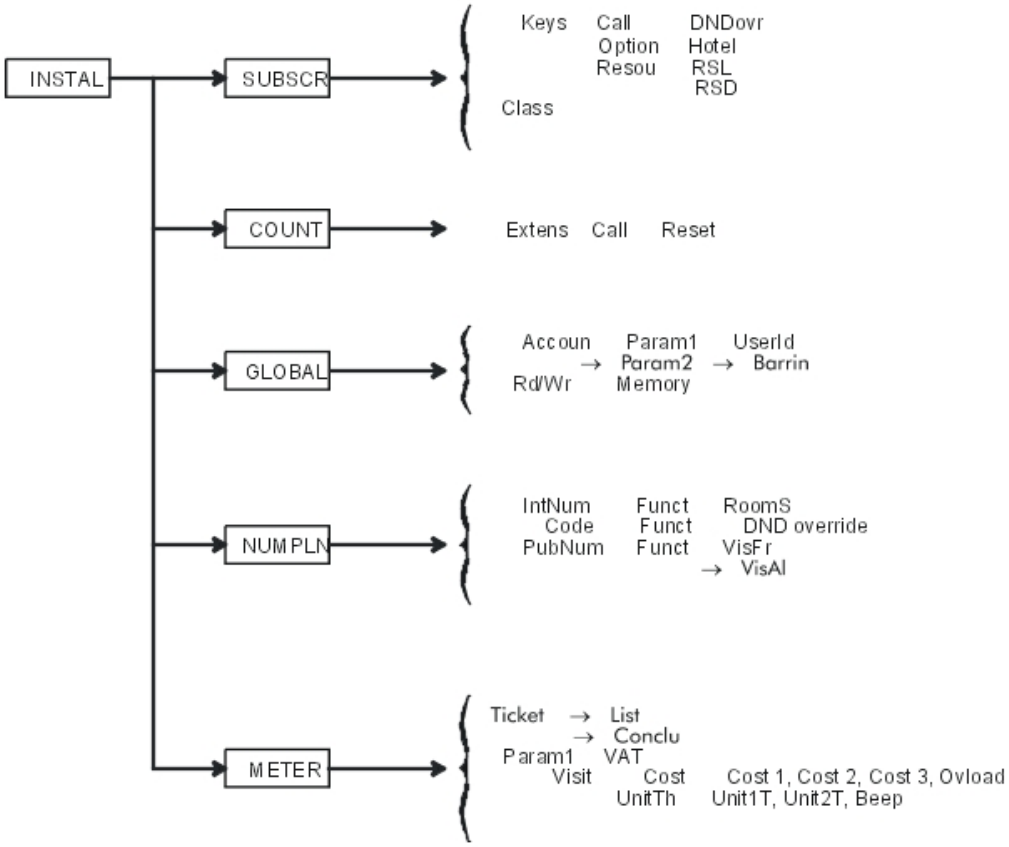
- Configure the parameters: "Wake-up", "DDI", "Language", "Restriction", "DND", "Exit time" and "Check-in" (see **Customising the configuration screens**)
- Configure the Room status parameters (see **Configuring room status**)

Guest account charging

- Configure the parameters: "Deposit", "Currency" and "VAT" (see **Customising the configuration screens**)
- Configure the parameters: "Room status" print out, Thank-you messages, VAT, Cost of calls, Surcharge and Cut-off (see the **Account charging** features in **System Parameters**)

8.2.2.1.2 SYSTEM PARAMETERS

The following flow chart shows the required system parameters; they are only accessible in the installer session.



DND override

This service enables an authorised user (Reception) to override a set's DND (Do Not Disturb) status. It is activated either with a function key or with a feature access code.

- To assign a feature access code to the service:

• by MMC-Station: **NumPln** -> **Code** -> **Funct** -> **DND override** • by OMC (Expert View): **Numbering** -> **Features in Conversation** -> **DND Override**

- To assign the service to a key:

• by MMC-Station: **User or Subscr** -> **Keys** -> **Call** -> **DNDovr** • by OMC (Expert View): **Users/Base stations List** ->

- Authorise the service on the calling party set:

• by MMC-Station: **User or Subscr** -> **SubPro** -> **Featur** -> **High** • by OMC (Expert View): **Users/Base stations List** -> **Subscribers** -> **Details** -> **Features** -> **Part2** -> check **DND override allowed**

- Protect the called party against the service:

- by MMC-Station: **User or Subscr** -> **SubPro** -> **Featur** -> **High** or **Middle**
- by OMC (Expert View): **Users/Base stations List** ->

Hotel key

This feature enables Reception to enter the hotel application in order to enter, review and/or print guest data.

- To assign the feature to a key:

- by MMC-Station: **User or Subscr** -> **Keys** -> **Option** -> **Hotel**
- by OMC (Expert View): **Users/Base stations List** ->

RSL key

The Reception set must be equipped with add-on modules. The modules are programmed with RSL resource keys (essentially room No.) which allow Reception:

- to call a set in the installation directly
- to receive a call on the resource from a set in the installation
- to see the busy status of a set in the installation
- to find out the occupation status of a room (free or occupied)
- to view a problem with a room wake-up call
- to view the status of a set's ringer (internal or external call)
- to find out the status of a room (cleaned or uncleaned)
- to view a problem with the room

Note:

The new features are accessible if the set has a Hotel key. They are detailed in "Reception set features".

- To assign RSL keys to the Reception set:

- by MMC-Station: **User or Subscr** -> **Keys** -> **Modify** -> **Resou** -> **RSL** -> enter a directory no. (that of a room set, for example)
- by OMC (Expert View): **Users/Base stations List** -> **Details** -> **Keys** -> **Resource Key** -> **Internal Call** -> enter a directory no. (that of a room set, for example)

RSD key

To call Room Service, the user dials a number corresponding to a service (the "breakfast" service for example). This number must be known by the system and must be assigned to the "Room Service" station.

- To assign service numbers to the "Room Service" station:

- by MMC-Station: **NumPln** -> **IntNum** -> **User or Subsc** feature-> no. of the service in **Begin** and **End** -> directory no. of the "Room Service" station in **Base**
- by OMC (Expert View): **Numbering** -> **Dialling Plans** -> **Internal Dialling Plan** -> **User** feature -> No. of the service in **Start** and **End** -> directory No. of the "Room Service" station in **Base**

The "Room Service" station is programmed with RSD resource keys which have the No. of the services. It has a display showing the name, directory No. and language of the caller.

- To assign RSD keys to the "Room Service" station:

- by MMC-Station: **User or Subscr** -> **Keys** -> **Modify** -> **Resou** -> **RSD** -> enter a service No. (the "breakfast" service, for example)
- by OMC (Expert View): **Users/Base stations List** -> **Details** -> **Keys** -> **Resource key** -> **DID call** -> enter a service No. (the "breakfast" service, for example)

Class

This feature assigns one of the following categories to each set in the installation: "Administration", "Guest" or "House phone (Phonebooth)".

- To assign a role to the set:

- by MMC-Station: **User or Subscr** -> **Class** -> assign **Administration set**, **Guest set** or **Phone booth**
- by OMC (Expert View): **Users/Base stations List** -> **Details** -> **Hotel** -> assign **Admin**, **Guest** or **House phone**

Default value: Administration

Call counters

This feature enables Reception to find out the number of charged calls made from a set in the installation and to reset the counter.

In the Hotel application, the call counter is automatically reset on check-in; the number of calls (charged calls) is given as a reminder on the printout of the "Guest Global Bill Record" and on the "Client Information Record".

- To read and reset a set's call counters:

- by MMC-Station: **Count** -> **Extens** -> **Call** to read the counter and -> **Reset** to reset it
- by OMC (Expert View): **Users/Base stations List** -> **Details** -> **Counting** to read the counter and -> **Reset** to reset it

This feature also allows you to edit, on the screen, the call and cost counters for sets.

- To read the call and cost counters for all the sets:

- by OMC (Expert View): **Counting** -> **Tracking Counters**

Account codes

Use of this service involves a new parameter, User ID, which makes it possible to perform "substitution" (charging to the account code of a set other than the one being used). This parameter means modifying the RESTRICTION field and specifying the PROTECTION field.

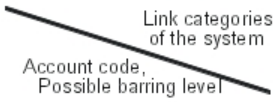
- To select whether or not to assign an identification request for substitution to the account code:

- by MMC-Station: **Global** -> **Accoun** -> **Param1** -> **UserId** ->select **NO** no identification or **YES** with identification
- by OMC (Expert View): **Traffic Sharing & Barring** -> **Account Code Table** -> **User ID** -> select **none** no identification or **User** with identification

- To assign a Class of Service Restriction to the account code (see also the table below):

• by MMC-Station: **Global** -> **Accoun** -> **Param2** -> **Barrin** -> select **None**, a category between **1** and **16**, **SET** or **GUEST** • by OMC (Expert View): **Traffic Sharing & Barring** -> **Account Code Table** -> **Bar.Lvl.** > select **none**, a category between **1** and **16**, **set** or **guest**

The table below shows, depending on the link COS assigned to the account code, the system reactions on the various link COS.

	**Traffic Sharing (LC3)**	**Barring Matrix (LC2)**	**Collective Speed Dial Rights (LC1)**
	LC3 of the set (*)	LC2 of the set (*)	LC1 of the set (*)
Guest	LC3 of the guest (*)	LC2 of the guest (*)	LC1 of the guest (*)
Forced restriction COS 1..16 1..16	LC3 of the set (normal service)	Fixed COS. 1..16	LC1 of the set (*)
None (no restriction)	LC3 of the set (normal service)	Call not restricted	LC1 of the set (*)

***** Link COS service operation: Normal or Restricted

Remarks:

- If the account code is with "Identification" then the no. of the substitution set is to be entered
- If the account code is with password, the password expected by the system is either that of the set in use or that of the substitution set

The user makes a call in the following way: **account code prefix** + **account code** + **No. of the substitution set** (optional) + **password** (optional) + **prefix for accessing the trunk group** + **called party's No.**

Count (meter) total recall

The count (meter) total recall (CTR or MTR) operation can recall the service beneficiary even if there is no charge.

- Recall the service beneficiary in all cases:

• by MMC-Station: **Global** -> **Rd/Wr** -> **Addres** ->enter 01 in **MtrNoCharg** -> **Memory** • by OMC (Expert View): **System Miscellaneous** -> **Memory Read/Write** -> **Other Labels** -> enter 01 in **MtrNoCharg**

Default value: "00" (no recall if no charge)

Wake-up call

In the case of a wake-up problem, the system alerts Reception by sending a message and a ringing tone to the set which is repeated approximately every 30 seconds.

- Inhibiting the ringing and visual alarm operation:

- by MMC-Station: **Global** -> **Rd/Wr** -> **Addres** ->enter 00 in **WakUpPrbRg** -> **Memory**
- by OMC (Expert View): **System Miscellaneous** -> **Memory Read/Write** -> **Other Labels** -> enter 00 in **WakUpPrbRg**

Default value: "01" (alarm activated)

Note:

With the hotel application, you can always view a guest wake-up problem on the RSL keys on the Reception set (see "Hotel Features").

Room status after check-out

After check-out the room is automatically switched to "uncleaned" status.

- Inhibiting the status changing mechanism:

- by MMC-Station: **Global** -> **Rd/Wr** -> **Addres** ->enter 00 in **UnclChkOut** -> **Memory**
- by OMC (Expert View): **System Miscellaneous** -> **Memory Read/Write** -> **Other Labels** -> enter 00 in **UnclChkOut**

Default value: "01" (switch to "uncleaned" status after check-out)

Dialling plans

Room Status

The "Room Status" feature in the internal dialling plan allows you to define the "Room Status" prefix for the installation.

- To create the "Room Status" prefix:

- by MMC-Station: **NumPln** -> **IntNum** -> **RoomS** feature
- by OMC (Expert View): **Numbering** -> **Dialling Plans** -> **Internal Dialling Plan** -> **Room Status** feature

DND override

The "DND Override" feature in the "Features in conversation" table serves to define the suffix for accessing the "DND Override" service.

- To create the "DND Override" service:

- by MMC-Station: **NumPln** -> **Code** -> **Funct** -> **DND Override**
- by OMC (Expert View): **Numbering** -> **Features in Conversation** -> **DND Override**

VisFr (Guest DID unassigned)

The "VisFr (Guest DID unassigned)" feature of the DID dialling plan groups together all the DID numbers available to be assigned to the rooms in the hotel. The feature's base is 9.

- To assign the DID no. to the Reception set:

- by MMC-Station: **NumPln** -> **PubNum** -> **VisFr** feature -> enter all the numbers in **Begin** and **End**, enter 9 in **Base**
- by OMC (Expert View): **Numbering** -> **Dialling Plans** -> **Public Dialling Plan** -> **Guest DID unassigned** feature -> enter all the numbers in **Start** and **End**, enter 9 in **Base**

Remarks:

- A DID no. assigned to a room at check-in automatically switches from "Guest DID unassigned" to "Guest DID assigned".
- Likewise, a DID no. which is no longer assigned to a room at check-out automatically returns to its initial function, "Guest DID unassigned". This operation allows you to route all the DID calls for free rooms to the Reception set.

VisAl (Guest DID assigned)

The "VisAl (Guest DID assigned)" feature in the DID dialling plan adds a DID no. to all the DID no. which are reserved for rooms and assigns it directly to a room.

- To add a room DID no.:

- by MMC-Station: **NumPln** -> **PubNum** -> **VisAl** feature-> enter the DID number in **Begin** and **End**, enter the directory no. of the room in **Base**
- by OMC (Expert View): **Numbering** -> **Dialling Plans** -> **Public Dialling Plan** -> **Guest DDI assigned** feature -> enter the DID number in **Start** and **End**, enter the directory no. of the room in **Base**

Note:

As the previous note states, this DID no. will automatically switch to "Guest DID unassigned" on check-out. It will rejoin all the DID no. reserved for rooms.

Metering

Room Status Rcords

This feature allows you to define whether a "Room Status Record" or "Statement" should be printed automatically when a room changes status.

- To select whether or not to print out a "Room Status Record" or "Statement" automatically:

- by MMC-Station: **Count or Meter** -> **Ticket** -> **List** -> select **RST** for automatic printout or **rst** for no printout
- by OMC (Expert View): **System Miscellaneous** -> **Hotel Parameters** -> select **Print Check-in/Check-out Ticket** for automatic printout

Default value: rst (no automatic printout)

A "Room Status Record" or "Statement" includes:

- the room no.
- the date and time of the status change
- the "Room status change" label
- a value (1 to 4 digits) representing the room status (free or occupied, problem no.)
- the name of the guest

Note 1:

The Hotel application allows you to:

- program a precise time at which all rooms (or only those which are occupied) switch automatically to the "uncleaned" status,
- automatic switching, after check-out, of a room to "uncleaned" status.

These two operations do not involve the transmission of a "Room Status Record" or "Statement".

PRINTING THE GUEST'S RECORD AUTOMATICALLY

The automatic print of the "Guest Information Record" after the guest has checked in or the "Guest Global Bill Record" after check-out can be deleted.

- Inhibiting the automatic print operation:

• by OMC (Expert View): **System Miscellaneous** -> **Hotel Parameters** -> deselect **Print Check-In/Check-Out Ticket**

Note 2:

It is always possible to print the records manually with the hotel application.

8.2.2.1.3 CUSTOMISING THE CONFIGURATION SCREENS

The application requires a customised configuration, dedicated to the environment in which it is situated, in order to present the check-in screens, the guest review screens and the check-out screens as well as to calculate the cost of calls and activate the default features.

The application is customised using the default screens, which must be configured. These screens are accessible from Reception sets with a "Hotel" key or through OMC (Expert View).

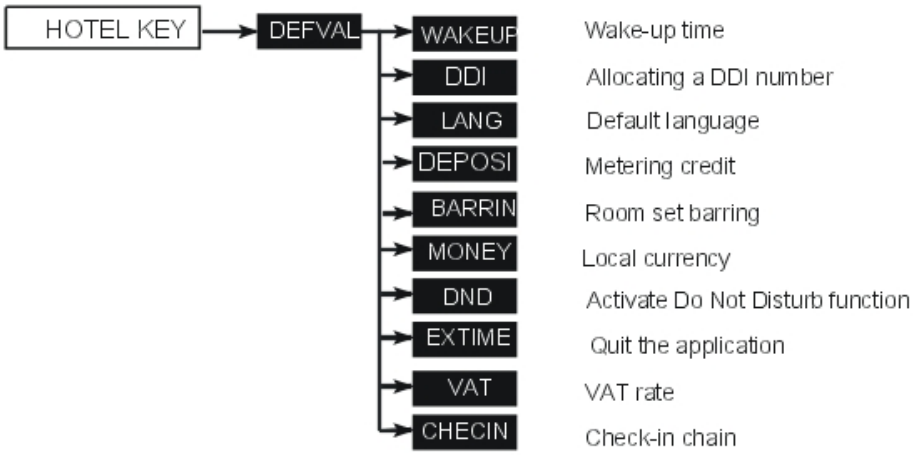
Note:

Only programming which is done via a terminal is presented in this document. In OMC (Expert View), the relevant data are proposed when you select **System Miscellaneous** -> **Hotel Parameters**.

- To configure the default screens:

Reception set: **Hotel key** -> **DEFVAL**

The display presents the following flowchart menu.



Wake-up time - WAKEUP

This feature allows you to choose whether or not to define a default time for a wake-up call.

Enter **06: 45** for example, or press CLEAR **--: --** so as not to have a default wake-up call.

Validate.

Allocating a DDI number - DDI

This feature allows you to assign a DDI no. by default.

Press CHOICE to select "DDI ALLOCATION BY DEFAULT" or "NO DDI BY DEFAULT". Validate.

Default language - LANG

This feature allows you to select a language by default.

Press CHOICE to select one of the languages offered. Validate.

Note: The language is automatically assigned to the guest's voice mailbox and set (if it has a display).

Charge credit - DEPOSI

This feature allows you to choose whether or not to activate the "prepayment request" (charge credit) menu and enter a total corresponding to a default prepayment.

Enter a total or press CLEAR to inhibit the menu. Validate.

Note:

When the menu is activated, a line reserved for the prepayment total is printed on the "Guest Global Bill Record" and on the "Guest Information Record".

Room set restriction (barring) - RSTRCT (BARRIN)

This feature allows you to define a default restriction for room sets.

Press CHOICE to select "INTERNATIONAL", " NATIONAL", "LOCAL" or "NO EXTERNAL". Validate.

Note:

By OMC, under **System Miscellaneous** -> **Hotel Parameters** -> **Default Restr/Barring Level**, the default restriction on room sets takes the values **1** for "INTERNAL", **2** for "CITY", **3** for "NATIONAL" or **4** for "INTERNATIONAL"

Local currency - MONEY

This feature allows you to enter the country's monetary unit.

Enter **USD** for example. Validate.

Note:

The monetary unit is printed on the "House phone Bill", the "Guest Global Bill Record" and on the "Guest Information Record".

Activate Do Not Disturb function - DND

This feature allows you to activate or deactivate the Do Not Disturb feature by default.

Press CHOICE to select "ACTIVE" or "INACTIVE". Validate.

Quit the application - EXTIME

This feature enables the Reception set to exit the Hotel application automatically, if no action is carried out during the set time.

Enter **20** (minutes) for example. Validate.

VAT rate - VAT

This feature allows you to enter the country's VAT rate.

Enter **20.60** for example. Validate.

Note:

The cost of calls with VAT, the total VAT, and the VAT rate are printed on the "House phone Bill", the "Guest Global Bill record" and the "Guest Information Record".

Check-in chain - CHECIN

This feature allows you to program the order in which six review screens – the ones most often used during check-in – appear (maximum of six from a choice of eight).

Position yourself on the field to be modified using NEXT or PREV, then press CHOICE to select "DEPOSIT", "NAME", "WAKEUP", "DND", "LANGUAGE", "DDI", "BARRING", "PASSWORD" or "__" (no screen). Validate.

Note:

The review screens which are not selected remain accessible at the end of check-in.

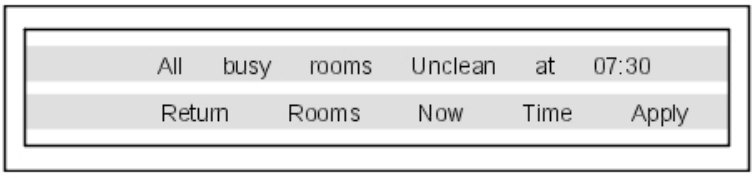
8.2.2.1.4 CONFIGURING ROOM STATUS

Configuring room status allows you to define whether all the rooms, or only those which are occupied, switch manually or automatically (at a programmed time) to "UNCLEANED" status.

- To enter the Room Status menu:

Reception set: **Hotel key** -> **Status** -> **Global**

The display below shows the possible functions.



The first line of the screen recalls the configuration of the Room Status which may be as follows: **Only occupied rooms switch to "Uncleaned" status at 7:30**

Rooms concerned- ROOMS

This feature allows you to define the rooms which will switch to "UNCLEANED" status.

Press ROOMS to select "ALL BUSY ROOMS" or "ALL ROOMS". Validate.

Conditions - NOW, TIME

This feature allows you to define whether the rooms concerned (those in the "ROOMS" menu)

switch to "UNCLEANED" status automatically or manually.

- Manual switch, press NOW.
- Automatic switch, press TIME, then enter **06: 30** for example, or press CLEAR **--: --** to cancel the time. Validate.

Validate the operation.

Note:

The feature is activated either immediately (manual mode), or at the time defined by the settings (automatic mode).

8.3 Hotel Reception Set Features

8.3.1 Check-in

8.3.1.1 Detailed description

8.3.1.1.1 CHECK-IN

- To select a free, cleaned room:

• Reception set: **Hotel key** -> **RSL** key or **directory nº** of the room

Depending on how the programmed consultation screens are chained, you must:

- fill in the "empty" fields (the NAME of the guest for example)
- modify the fields which do not correspond to the default values (the LANGUAGE for example)
- validate all the check-in screens as and when they are presented.

Validating the last consultation screen is equivalent to exiting CHECK-IN; the room is considered occupied, and a "Guest Information Ticket" is printed automatically.

Below are the screens which correspond to check-in (maximum of six screens from a choice of eight):

- Deposit : deposit total (metering credit) or select (no prepayment)
- Guest name : guest name (10 characters maximum)
- Wake-up time : wake-up time or select : no alarm
- DND Status : to activate (DND) or deactivate (dnd) the "Do Not Disturb" function
- Language : choice of language
- DDI number : allocation of a DDI Nº, select to allocate a new one
- External calls : line barring, select to allocate a new one
- Password : allocation of a password, select to allocate a new one

Note:

All the consultation screens, including those not selected, are grouped together in the room consultation screens once the check-in is completed.

8.3.2 Room

8.3.2.1 Detailed description

The application allows you to consult and modify a guest's data.

- Select an occupied room:

• Reception set: **Hotel key** -> **RSL** key or **directory nº** of the room

Note:

To exit the application, press the Release key .

To consult another room without quitting the application, select an **RSL** key or enter a directory **nº** .

The display presents the guest data for the selected room. The data is displayed over three screens.

The first line of each screen gives:

- the name of the guest
- the guest's language
- the guest's wake-up call time (if programmed) and warning of any problem with the wake-up call
- the guest's DND (do not disturb) feature status
- the guest's prepayment status (signs **+** for "credit" and **-** for "debit") and the monetary unit used
- the segment □, off or lit, representing the guest's mail status (text mail, voice mail and Reception call-back request)
- the directory number of the room

The second line of each display enables Reception to consult and/or modify guest data, or to print out an information ticket.

8.3.2.1.1 Print guest information ticket - PRINT

Press PRINT to print out the "Guest Information Ticket" which includes:

- the name of the guest
- the room nº
- the language
- the password
- the DDI nº
- the barring status
- the guest's overall deposit total (metering credit)
- the total remaining to be paid by the guest (debit) or to be reimbursed by the hotel (credit); total of the deposit paid minus the cost of the communications
- the VAT rate and the total VAT corresponding to the cost of the communications
- the number of communications made
- the active or inactive status of the DND feature
- the guest's mail status (messages present or not: text, voice and Reception call-back request)

8.3.2.1.2 Wake-up call time and status - WAKEUP

WAKE UP allows you to **read** and **modify** the guest's wake-up call time and **consult** the guest's wake-up call status.

Reading the wake-up call time:

The room consultation screen allows you to read the guest's wake-up alarm time.

Modifying the time:

Press WAKE UP . Enter **06: 45** for example or press CLEAR **--: --** so as not to have an alarm. Validate.

Consultation of the alarm status, several choices are possible:

- LEFT-HAND SEGMENT OF THE ROOM RSL KEY
  On the add-on module for example, the left-hand segment of a flashing room RSL key signals an undefined problem with the wake-up alarm.
- ROOM OCCUPATION SCREEN
  The consultation screen of a room signals whether a wake-up time is programmed or whether there is an undefined problem with the wake-up call. Example:
  - **06: 45**: programmed wake-up time; wake-up time active if **:** (colon) flashes
  - **06: 45**: programmed wake-up time; wake-up time inactive if no character flashes
  - **--: --**: no programmed wake-up time (problem with wake-up call if all segments flash)
  - **06: 45**: programmed wake-up time and problem with wake-up call if all characters flash
- WAKE-UP CALL STATUS
  Press WAKE UP ; the wake-up call status will then be one of the following:
  - **active**: the wake-up call is active
  - **--- (inactive)**: the wake-up call is inactive
  - **busy**: problem – the set was busy during the three attempts
  - **unanswered**: problem – the set did not answer during the three attempts

- **inaccessible**: problem – the set was inaccessible during the three attempts

- WAKE-UP CALL
  In the case of a wake-up problem, the system alerts Reception by sending a message and a ringing tone to the set, repeated approximately every 30 seconds.

8.3.2.1.3 Do Not Disturb - DND

This feature allows you to **read** the status of the guest's DND feature and **modify** it.

Reading the status of the DND (Do Not Disturb) feature:

The room consultation screen allows you to read the DND status directly:

- **DND** : feature active
- **dnd** : feature inactive

Modifying the DND feature:

Press DND -> ENTER to select "ACTIVE" or "INACTIVE". Validate.

8.3.2.1.4 Metering credit - DEPOSI

This feature allows you to read the guest's **credit** (after calculation of the cost of the guest's communications) and to enter the **amount** of a new deposit.

Guest credit (with use of metering credit only):

The room consultation screen allows you to read the guest's account. It is either:

- **+ xxxxx EUR** : positive (in credit)
- **- xxxxx EUR** : negative (in debit)

Amount of a new deposit (with use of metering credit only):

Press DEPOSI and enter a new amount.

Validate the operation; the system recalculates the total deposit and the remaining credit.

8.3.2.1.5 Checking out a guest - CHEOUT

See "Guest Check-out ".

8.3.2.1.6 Guest name - NAME

This feature allows you to **read** the name of the guest and **modify** it.

Reading the name:

The room consultation screen allows you to read the name of the guest.

Modifying the name:

Press NAME and modify the name (10 characters maximum); validate the operation.

8.3.2.1.7 Guest language - LANG

This feature allows you to **read** the guest's language and **modify** it.

Reading the language:

The room consultation screen allows you to read the guest's language.

Modifying the language:

Press [LANG] -> [ENTER] to select one of the languages offered. Validate.

Note: the language is automatically assigned to the guest's voice mail box and set (if it has a display).

8.3.2.1.8 Voice mail status - MESSAG

This feature allows you to **read** the guest's message status (message left or not), it enables the operator to leave the guest a **call-back request** (activation of the message LED) and find out the **type of message** left for this guest (operator call-back, voice mail or text mail).

Reading the guest's mail:

The room consultation screen allows you to find out whether a message has been left for the guest. To the right of the display and before the room nº, a segment provides information on this status:

- at least one message is waiting for the guest: ■
- no message is waiting for the guest: □

Operator call-back request:

The operator can leave a call-back request on the guest's set. Press [MESSAG] -> [ENTER] to:

- activate a call-back request: ■
- cancel the call-back request: □

Validate the operation.

Reading the type of message left:

The operator can find out the type (voice or text message) of message left for the guest.

Press [MESSAG] and analyze the display according to the headers presented:

- **OPERATOR** : operator call-back request: ■ or no call-back: □
- **VOICE** : voice message waiting: ■ or no message: □
- **TEXT** : text message waiting: ■ or no message: □

8.3.2.1.9 Guest DDI number - DDINUM

This feature allows you to **read** the guest's DDI nºand **select** another one.

Reading the DDI nº:

Press [DDINUM] , the screen displays the guest's DDI nº.

Selecting another DDI nº for the guest:

Press [DDINUM] -> [ENTER] , the system allocates another DDI nº. Validate.

8.3.2.1.10 Barring - BARRNG

This feature allows you to **read** and **modify** the barring for the guest's set.

Reading the barring:

Press [BARRNG] , the screen displays the guest's barring level.

Modifying the barring:

Press [MARK] -> [ENTER] to select "INTERNATIONAL", " NATIONAL", "LOCAL" or "NO

EXTERNAL". Validate.

8.3.2.1.11 Guest password - PASSWD

This feature allows you to **read** the guest's password and **select** another.

Reading the password:

Press , the screen displays the guest's password.

Selecting another password:

Press -> , the system assigns another password. Validate.

Note: The password is automatically assigned to the guest's voice mail box and set. The guest can use it to:

- lock the set (block outside calls)
- make calls using a protected account code (with or without substitution)
- read his or her voice mail remotely

8.3.3 Check-out

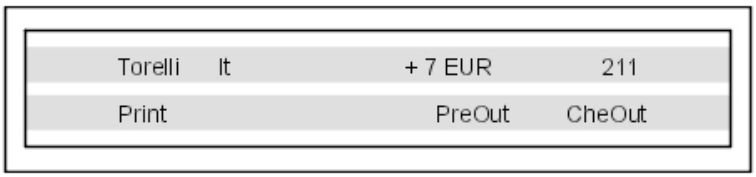
8.3.3.1 Detailed description

The application allows you to free a room.

- Select an occupied room then the Check-out menu:

• Reception set: **Hotel key** -> **RSL** key or **directory nº** of the room -> **CheOut** menu

The following appears on the display:



The first line shows:

- the name of the guest
- the guest's language
- the guest's prepayment status (signs " **+**"for credit and " **-**" for debit) and the monetary unit used
- the directory number of the room

The second line enables Reception to print out an information ticket and perform "Pre-checkout" as well as Check-Out.

8.3.3.1.1 Print out a guest's telephone bill - PRINT

Press ; the bill indicates:

- the name of the guest

- the room nº
- the guest's total deposit (metering credit)
- the number of communications made
- the total cost of the communications
- the VAT rate and the total VAT corresponding to the cost of the communications
- the total remaining to be paid by the guest (debit) or to be reimbursed by the hotel (credit); total of the deposit paid minus the cost of the communications

8.3.3.1.2 Pre-checkout of a guest - PREOUT

This feature enables a guest to settle the telephone bill the day before an early morning departure, for example, (external outgoing calls are then no longer possible) whilst at the same time keeping the features programmed on the phone (wake-up call, message, DDI Nº, DND, etc).

Press → PRE CHECK-OUT to activate the pre-checkout features. Caution: The pre-checkout cancels the guest's amount "Remaining to be paid", see the table below.

8.3.3.1.3 Check-out of a guest - CHEOUT

This feature enables Reception to make a room free; see the table below.

Press CHECK-OUT to reset the room's parameters; a "Guest Global Bill Ticket" is printed automatically.

The following table and analysis show the role of each of the features.

	Wake-up	Message	DND	Forward	DDI allocation	Barring	Room Status	Password	Name	Remaining to be paid
Pre-checkout	/	/	/	/	/	No external call	/	/	/	---
Check-out	Reset	1 hour	Reset	Reset	Reset	No external call	Free / Uncleaned	Reset	Room nº	---

Analysis of the table:

- **/** : this symbol means that the feature remains unchanged from the previous report.
- **No external call**: new room set barring. The set will return to its default configuration upon check-in.
  Active communications, ringing, calls on hold etc. are cut off immediately upon activation of "PRE-CHECKOUT" or "CHECK-OUT".
- **--- in the "Remaining to be paid" column**: the total remaining to be paid by the guest (debit) or reimbursed by the hotel (credit), resulting from the cost of the communications and the deposit given, is erased.
  The guest's call counters, partial metering counter and partial cost counter are reset only upon check-in (input of a new guest) or by system command.
- **Reset**: reset of the features. The Wake-up, DND and Barring features return to their default value upon check-in.

- **1 Hour**: new messages are kept for 1 hour. Check-in resets the voice mail box.
- **Free / Uncleaned**: the room is assigned "Free" and "Uncleaned" status.
- **Room nº**: the guest name is replaced by the room number (directory update).

8.3.4 Room Status

8.3.4.1 Detailed description

The Room Status feature enables:

- the Room Manager: to inform Reception of the status of rooms
- Reception to:
  - find out the status of a room
  - change the status of a room
  - see the status of the rooms on the Reception set (segments of an RSL key)
- print a Room Status ticket or statement

8.3.4.1.1 Use of Room Status by the Room Manager

The Room Manager informs Reception of the status of the rooms (cleaned, uncleaned, with or without problem) by using the room set to dial the "Room Status" code corresponding to its status.

- To enter the Room Status code for a room:

• On the room set: **Room Status prefix** + **0 (cleaned)** or **1 (uncleaned)** + if necessary, **no. of problem (3 digits max.;** enter **000** to cancel the previous code**)**.

8.3.4.1.2 Use of Room Status by Reception

Reception enters the Room Status menu then selects "Global" or a room RSL key.

- To enter the Room Status menu:

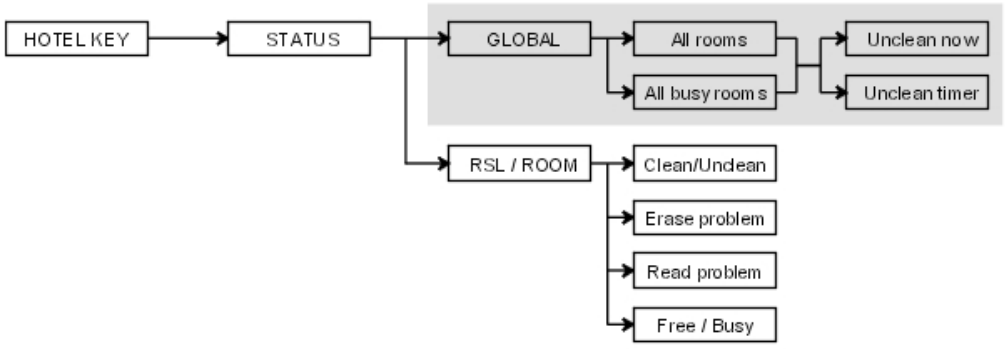
• Reception set: **Hotel key** -> **Status**

Note:

To exit the application, press the Release key.

To consult the status of another room, select an **RSL** key.

To return to room consultation, enter a **directory no.**.



8.3.4.1.3 Configuring Room Status - GLOBAL

The greyed area represents the Room Status configuration. On the use of this service to switch rooms to "Uncleaned" status immediately or at a preset time, see "Configuring Room Status" in the "Configurations" section.

ROOM STATUS – RSL KEY OR DIRECTORY No.

The RSL key or directory no. allows you to **read** and **modify** the Room Status of a room. There is:

- its "Cleaned" or "Uncleaned" status
- its problem number, if there is indeed a problem
- its free or busy status (read only).

Reading the status of a room:

The screen displays the three types of status above.

Note:

The CHECK-IN, PRE-CHECKOUT and CHECK-OUT operations do not reset the room problems.

Modifying room status:

- Press CLEANS to select "UNCLEANED" or "CLEANED"
- Press NOPROB to erase the problem
- Press PROBLM to enter a problem no. **012** for example, and validate

Validate the operation.

8.3.4.1.4 Printout of a Room Status Record or Statement

A **Room Status record** or **Statement** can be printed automatically when a room changes status.

Below is an example of a "Room Status Statement".

ALCATEL

USER	LINE	HOUR	TAXES	FACILITIES	--	USER NAME
TYPE	DATE	DURATION	SERV.	DIALLED NUMBER	--	
AI22	03/06/97	08:31		ROOM STATUS CHANGE 0034		TORELLI

The field ROOM STATUS CHANGE is specific and includes the following data:

- the first digit indicates the room status: **0** = room CLEANED or **1** = room UNCLEANED
- the other digits (3 maximum) represent the problem number, if there is one.

8.3.4.1.5 Function of the RSL key segments

The three-segment display associated with each RSL key not only allows you to see the telephone status (normal operation), but also provides at-a-glance information on the overall status of the room (free, occupied, cleaned, uncleaned or problem with wake-up call or room).

To access these types of status, the set must have a Hotel key. Each segment has a function:

- The first segment (on the left-hand side) indicates the free or occupied status of the room as well as a possible wake-up call problem
- The second segment indicates the telephone status of the room set
  Note: If the segment is flashing, this indicates an internal or external call
- The third segment indicates the "cleaned" or "uncleaned" status of the room as well as a possible problem with the room

The table below sums up this information.

Segment N° / Status	1st segment	2nd segment	3rd segment
Not lit	Room free	Station free	Room cleaned
Lit	Room occupied	Station busy	Room uncleaned
Flashing	Wake-up problem	Station ringing	Room problem

8.3.5 Room Service

8.3.5.1 Detailed description

8.3.5.1.1 ROOM SERVICE

To call Room Service, the user dials a number corresponding to a service (the "breakfast" service for example). This number, recognised by the system, is assigned to the "Room Service" station on an RSD key.

The "ROOM SERVICE" station has a display enabling the Room Service operative to read the name, directory no. and language of the caller.

8.4 Call Metering

8.4.1 Overview

8.4.1.1 Call metering

8.4.1.1.1 Selecting the type of metering

Alcatel-Lucent OmniPCX Office Communication Serversupports two types of call metering:

- V24 metering supports V24 printing for all call metering tickets.
- IP metering supports IP printing for call metering tickets originating from a 3rd party application (Business or Hotel) via an IP connection.

The type of metering must be specified when the Office Link driver is installed. The driver can be installed in one of two modes: **hotel** or **metering**.

You can use the OMC **Counting** function to specify the type of call metering for hardcopy printouts.

To set printing options for call metering tickets:

1. Open the **Counting** function window in the OMC console and select the **Accounting Printout** tab.
2. Select the metering type from the drop down box, **Ext. Accounting Activation IP**, or **Ext. Accounting Activation V24** and ensure that the associated checkbox is checked.
3. When finished, click **OK**.

Note:

English is used for IP printing and cannot be changed.

8.4.1.1.2 Call metering

The CALL DETAIL or COUNTING (METERING) module is used to collect specific information about telephone calls. This information can be printed in various formats, depending on the type of management selected.

This section describes the implementation and use of call metering statements or tickets that can be printed on any printer connected to a V24 4083 ASM or 4093 ASY-CTI or V24/CTI Interface Module option on a digital terminal.

Note 1:

For IP metering, the output information in XML format will have a different meaning.

It is also possible to display data related to a call.

Note 2:

For V24 metering, not all the call detail information supplied by the ISVPN+ protocol (attendant, node, services: transit, overflow, ARS, etc.) appear on the tickets; data can only be used from within a central management application (Alcatel-Lucent 4740, 4760 or other).

V24 call detail printout:

- Call detail printout parameters: format (information bits, parity, stop bits) and speed; by default: 8N1, 9600 bps).

By OMC (Expert View), select: **Users/Base stations List** -> select V24 access -> **Details** -> **V24**

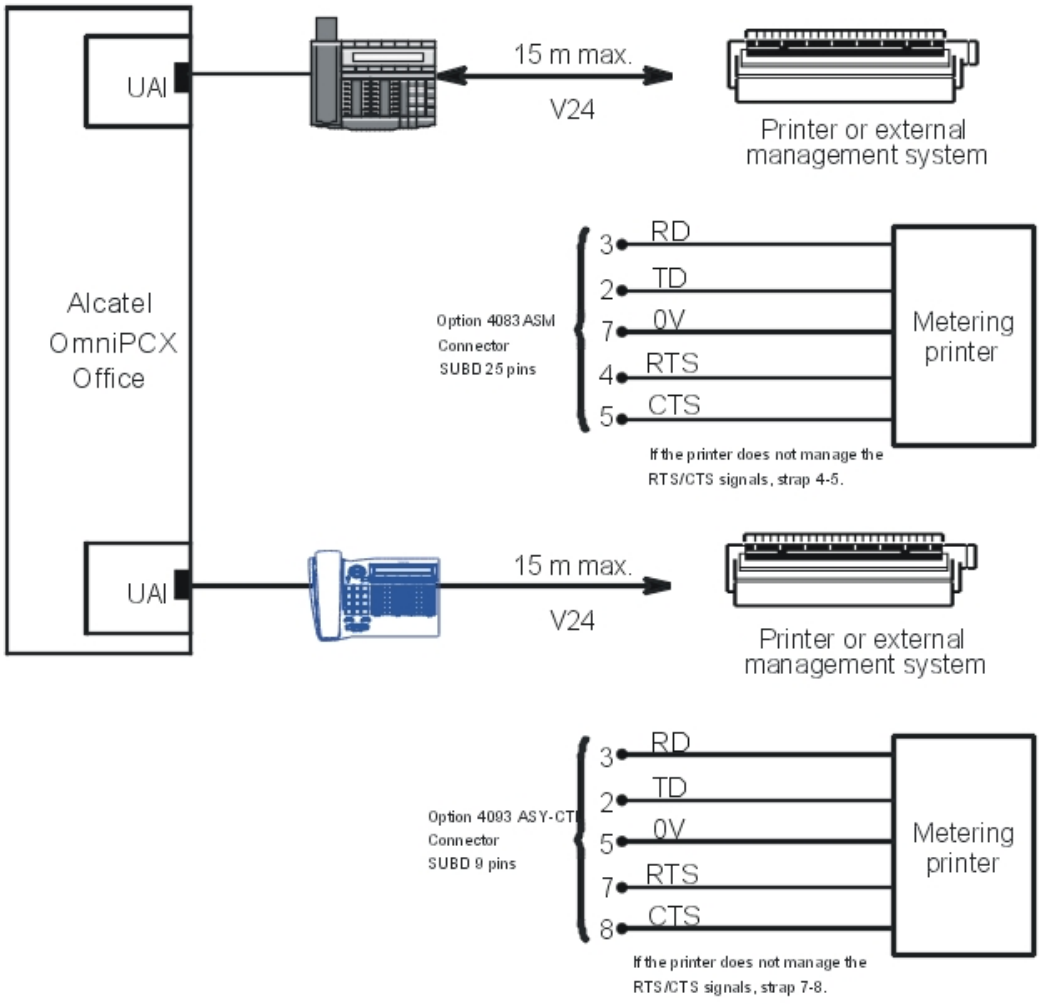
- Activating external call detail: printing of records/statements is or is not activated (default setting)

By OMC (Expert View), select: **Counting -> Counting** -> **Accounting Printout**->check **External Accounting Activation V24**

Note 3:
The details on configuring the V24 call detail printout can be found in the "Appendix" section.

8.4.2 External connections

Connection



8.4.3 Principles

8.4.3.1 Overview

Meter charging according to the operating phase

Operation	Meter charging method
Conversation	Metering units received on the line are charged to the subscriber in conversation with that line.
Park or Hold	Metering units received on a parked or holding line are charged to the subscriber who parked the call.
Retrieve from parking or hold	The metering units are charged to whomever activated the service. Subsequent metering units are charged to the user who retrieved the call.
Automatic forwarding	The system does not manage charges for external forwarding; this is managed by the public network.
Conference	Any conference costs are charged to the conference initiator.
Transfer	If a transfer takes place on an external call, the cost of the communication is charged to the initial user until the external user is put through to the new correspondent. When a call is transferred while ringing or on busy, metering units are charged to the transfer destination. No units are charged to the OS when external calls are transferred to a system user; all the metering units are charged to the destination subscriber. However, if a call is meant for the OS (by transfer or callback), the communication is charged to the OS.
Ext/Ext transfer	Metering units received after the transfer are charged to the user who made the second external call.
Transfer failure	A callback after a transfer failure is always treated as an incoming communication for the set to which the call is rerouted after the no-answer time-out.
External forwarding	When an internal call is made to a user whose calls are being diverted to an external number, the metering units are charged to the forwarded subscriber.

8.4.4 Duration and Cost

8.4.4.1 Operation

Duration

The system counts two types of duration:

- Duration of the communication: this corresponds to the time during which the system considers that a line is allocated to a subscriber; this accounting occurs after the first switch to conversation mode by the subscriber with the line.
- Call phase duration: the system counts the call phase duration of an incoming external communication from the moment when the system detects the call to when the line changes to conversation with a system terminal. This information is used during external management.

Cost

The cost of a communication is calculated according to the number of units charged:

- The value of the basic metering unit may be constant, regardless of the length of the communication.
- The value of the basic metering unit may be variable: the cost of the first x metering units is calculated according to an initial basic metering unit value. As soon as a threshold number of metering units is reached, the cost is calculated according to a second metering unit value.

Note 4:

The software allows the actual duration of the communication to be shown on the metering ticket:

- on receipt of a CONNECT message on digital networks
- on receipt of a polarity inversion or a metering pulse on analog networks.

In all other cases, the duration given is only approximate since it is calculated by an off-hook simulation mechanism.

Useful parameters for calculating the cost of a communication:

- Value of the basic metering unit before reaching the configured threshold (6 digits in the chosen monetary unit, of which 0 to 2 are decimals)

• By OMC (Expert View), select: **Metering -> Metering** -> **Metering Options for Active Currency**-> **1. Base Charge Rate**

- Threshold for using the second basic metering unit value (in metering numbers from 0 to 99)

• By OMC (Expert View), select: **Metering -> Metering** -> **Metering Options for Active Currency**-> **N# of units for cost threshold**

- Second basic metering unit value (6 digits of which 0 to 2 are decimals)

• By OMC (Expert View), select: **Metering -> Metering** -> **Metering Options for Active Currency** -> **2. Base Charge Rate**

- Number of decimals in the cost

• By OMC (Expert View), select: **Metering -> Metering** -> **Metering Options for Active Currency** -> **Fractional Part Length for Costs**

Note 5:

If it has been decided to operate with a single metering unit value, the same value must be given to the second metering unit value.

8.4.5 Cost of ISDN Services

8.4.5.1 Operation

Since the costs of some features are not transmitted by the public network, it is possible to assign a given value to the cost counter whenever such a service is activated.

Cost of ISDN services:

- Cost of online calculation (in counter units) in the case of manual activation (if the network does not add the cost of the service at the beginning of the call).

• By OMC (Expert View), select: **Counting -> Counting** -> **Counting Options for Active Currency**-> **Online Counting**

- Cost of user to user signalling (in the chosen monetary unit, 6 digits – of which 0 to 2 are decimal).

• By OMC (Expert View), select: **Counting -> Counting** -> **Counting Options for Active Currency**-> **User to User Information**

- Cost of PCX forwarding (in the monetary unit chosen, 6 digits – of which 0 to 2 are decimal).

• By OMC (Expert View), select: **Counting -> Counting** -> **Counting Options for Active Currency**-> **Diversion Charge Rate**

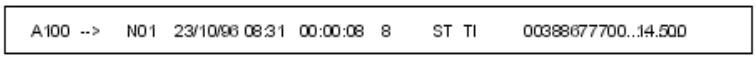
Example of the calculation of the cost of a call

This example shows the effect of using the "Online counting" and "UUS" services in terms of call costs.

Parameters configured:

- Basic counter unit value: 1.70 F
- Threshold: 1 counter unit
- Second basic counter unit value after threshold: 2 F
- Cost of online counting: 4 counter units
- Cost of UUS: 5.10 F

Example of a statement:



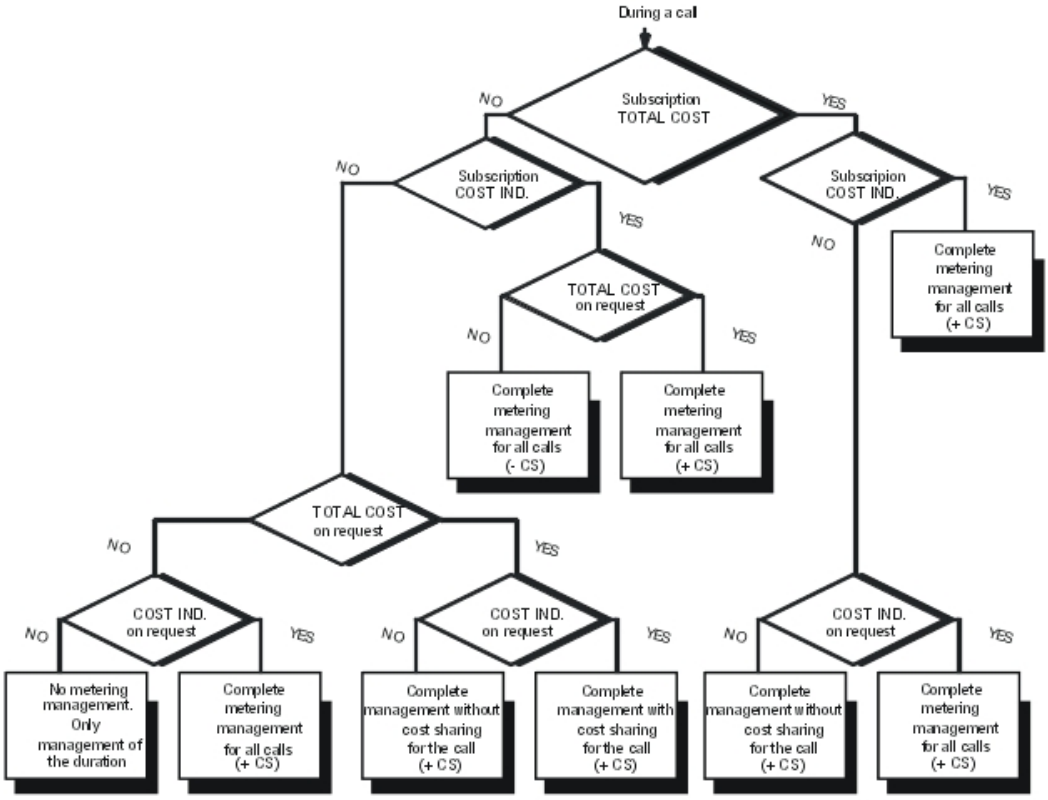
The 8 counter units are made up as follows:

- **1** counter unit for the call; cost = **1.70** F
- **4** counter units for activation of the online counting; cost = **7.70** F (1 x 1.70 F + 3 x 2 F)
- **3** counter units for UUS (number of counter units =UUS/first basic counter unit value cost, i.e. 5.10/1.70 = 3); cost = **5.10** F

8.4.6 Complementary Services

8.4.6.1 Operation

- **Online counting**
  This additional service includes the services TOTAL COST (display of the total cost on release of the call) and COST INDICATION (display of the cost during a call). Different cases are possible:



Subscription to the TOTAL COST or COST INDICATION service means that the additional service is activated on subscription to the network carrier.

TOTAL COST or COST INDICATION on request (call by call) signifies that the additional service is activated by system configuration (MMC) or by activation from an S0 set.

+ CS signifies that the cost of additional services (UUS, terminal forwarding) is managed by the system (-CS if not).

At each automatic or manual activation of an ONLINE COUNTING request, a charge unit is assigned to the caller.

- Activation of online counting during call

• By OMC (Expert View), select: **Counting -> Counting** -> **Counting Options for Active Currency** -> **Advice of Charge** -> check **During the Call** or **At the End of the Call**

Note:

The "At the end of the call" field (TOTAL COST on demand) is not used in France.

- **User to User Signalling (I)**
  The cost of this service is programmable by MMC.
  It does not depend on the length of the message. It is assigned as soon as the UUS is transmitted (even if the called party has not answered). The cost is assigned to the user who initiated the call: it therefore only applies to outgoing calls.
  Note: During such a call, the cost of outgoing and incoming messages is assigned to the

initiating user.

- **Terminal forwarding or external forwarding (R)**
  A ticket (record) or statement is printed whenever this feature is activated or deactivated.

8.4.7 Bearer Services

8.4.7.1 Basic description

One of the metering ticket fields mentions the "bearer service" used for the communication.

The following bearer services are provided:

- **ST**: voice, group 3 facsimile, teletext and videotex type services.
- **T+**: group 4 facsimile, transparent data transmission.

8.4.8 Information Displayed on Sets

8.4.8.1 Detailed description

Temporary counters keep track of information destined to be displayed during a network call.

Information which can be displayed on all system terminals with displays (except S0 sets):

- Duration
- Duration + number of counter units (including for additional services)
- Duration + cost

• By OMC (Expert View), select: **Counting -> Counting** -> **Counting Options for Active Currency** -> **Display on Sets**

Signal (pulse) counter

- This counter counts the number of units received on a line and assigns them to a specific user.
- It is reset when the line is released or the call is transferred to a new user.

Duration counter

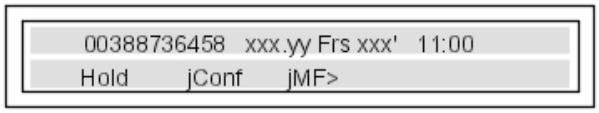
- This counter totals the duration (in minutes) during which a specific line connected to a subscriber (user).
- It is reset when the line is released or assigned to a new user.

Cost counter

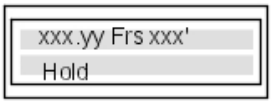
- This counter records the cost of a call (in local currency) between a specific user and a trunk line.
- It is reset when the line is released or assigned to a new user.

Examples of displays

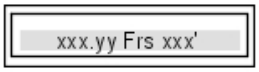
- Alcatel-Lucent IP Touch 4068 Phone set:



- Alcatel-Lucent IP Touch 4038 Phone and Alcatel-Lucent 4039 Digital Phone sets:



- Alcatel-Lucent IP Touch 4028 Phone and Alcatel-Lucent 4029 Digital Phone sets:



8.4.9 Metering Counters

8.4.9.1 Detailed description

Description of the counters

The recording of the number of counters units and the cost of calls is done by 12 counters, distributed as follows:

- **10 set counters:**
  - 2 adding counters (one for the number of counters units and one for the cost):
  - read only
  - no reset possible
  - the number of counter units displayed returns to zero when the maximum number is reached
  - 8 partial counters (4 signal counters, 4 cost counters) according to the online services defined:
  - read only
  - reset possible by MMC
  - the storage capacity of these counters is 65535 units
  - for a non S0 set, there is only one signal and cost counter.
- **2 line counters:**
  - one partial signal counter which can be reset
  - one adding signal counter which cannot be reset
  - the storage capacity of these counters is 4 thousand million units.

All of these counters can be read from MMC-Station or from OMC (the updating of metering counters at OMC level can only be done during a PCX -> PC backup in a new file).

Metering counters

- Reading and resetting set counters

• By OMC (Expert View), select: **Users/Base stations List** -> **Users/Base stations List** -> user identification -> **Details** -> **Counting**

- Reading and resetting line counters

• By OMC (Expert View), select: **External Lines** -> **List of Accesses** -> line identification -> **Details**

- Reading all the user adding counters

• By OMC (Expert View), select: **Counting** -> **Counters**

Counter changes in break-out/transit (transmission)

- normal break-out (leased line to public line): the line counter changes
- break-out by external forwarding (leased line to public line): the set counter changes
- normal transit (public line to public line): no counter change
- transit (transmission) by hunt group external forwarding (public line to public line): the hunt group counter changes

Counter printouts

Note 7:

Available for V24 printing only.

The contents of the counters can also be printed out by the counter printer (by MMC-Station: **Instal/Admin** -> **Count** -> **User/Subscr or Access**).

Set counters and attendant counters

TAXES AND COST COUNTERS PER SUBSCRIBER - 12/08/00 14:05

USER	TAXES COST :	C1 C1	C2 C2	C3 C3	C4 C4	TOTAL TOTAL
A101		1203	20	0	400	2645
		2467.50	422.32	0	53	23577.45
G1		23	0	2	0	60
		47.05	0	23.76	0	458.32

FIELD	DESCRIPTION
USER or SUBSCRIB.	Terminal number (max. 9 characters, right justified); the number format is: - AXXX for a user - GXX for a hunt group
C1-C2-C3-C4	Partial signal and cost meters per user/hunt group (5 characters)
TOTAL	Total cost meter per user/hunt group (5 characters)

Line counters

TAX METERS PER ACCESS - 12/08/00 14:05

ACCESS	PARTIAL	TOTAL
L01	12030	26452584
N01	23532	6052487
L03	24543	6503452

FIELD	DESCRIPTION
ACCESS	Access number (max. 5 characters, right justified); the number format is: - LXX for an analogue line during break-in/break-out - NXX in the case of a T0 basic access - PX in the case of T2 primary access
PARTIAL	Partial signal counters per access (10 characters)
TOTAL	Total signal counters per access (10 characters)

Note 8:

- Once a counter printout has been launched, no statement or record can be printed.
- A form feed is automatically performed before and after a counter printout.
- If the installer wants the USER (SUBSCRIBER) and the ACCESS counters to be printed on the same page, the second printout request must be done before the end of processing the first printout.
- Pressing successively on the User/Subscr (or Access) key results in printing the counters twice. A third request is only considered when the first request has been printed.
- If a printout problem occurs (for example no more paper), any printout request is ignored.
- There is no specific display on the set for printer problems; only a system message is generated.

8.4.10 Managing Metering Tickets and Statements

8.4.10.1 Detailed description

The system enables counter records and statements to be printed out.

Selecting the type of counter printout

Note 9:
Available for V24 printing only.

- Listing (line-by-line statement printout) or Ticket (record printout; 1 record per call)

By OMC (Expert View), select: **Counting -> Counting** -> **Accounting Printout** -> **Type of printout**

Every call that meets the tracking parameters defined for the various system terminals triggers

a record printout.

If a call is free of charge (incoming call for example) or if an incoming call remains unanswered, the transmitted record will specify the call history (ringing time, call duration, etc.).

Set tracking

- Definition of the tracking criteria values: cost threshold (monetary value), duration threshold (from 0 to 99 minutes), international prefix (4 digits maximum).

By OMC (Expert View), select: **Counting -> Counting** -> **Accounting Options for Active Currency**-> **Activation Criteria**

- Assigning the type of tracked calls for each set (parameter to be defined set by set): none (no tracking) or for all calls (outgoing and incoming) or all outgoing calls with tracking criteria active; if this is the case, define the active criteria: duration threshold (in minutes), cost threshold (6 digits of which 0 to 2 are decimals) or tracked (international prefix).

By OMC (Expert View), select: **Users/Base stations List** -> user identification -> **Details** -> **Counting**

- It is also possible to assign a profile defining the applied tracking criteria to a group of sets.

By OMC (Expert View), select: **Users/Base stations List** -> **Profiles**

- To print out a record or statement if an incoming call is unanswered (default setting = no)

By OMC (Expert View), select: **Counting -> Counting** -> **Accounting Printout**->check or uncheck **Print un-answered IC calls**

FUNCTION OF THE BUFFER MEMORY

This is used to temporarily store the various messages (output terminal not available, several simultaneous messages, etc.).

The maximum number of records or statements that can be stored is 1000.

Alarm activation threshold

- Percentage of records or statements printed before the alarm is activated (between 0% and 99%: 70% by default)

By OMC (Expert View), select: **Counting -> Counting** -> **Accounting Printout** -> **Printer alarms threshold**

As soon as the programmed threshold has been reached, an alarm is generated alerting the user (message in the call history + flashing of the attendant LED).

When the buffer memory is full, any new information is lost.

XON/XOFF TRANSMISSION PROTOCOL

Note 10:

Available for V24 printing only.

When the printer is ready to print, it transmits an XON control character. The data received is stored in a buffer. If there are only a certain number of bytes available in this buffer, the printer will transmit XOFF. It continues to receive characters and print before transmission halt. When part of the buffer is released, it transmits XON. The printer also transmits XOFF in the event of

the following problems: printer offline, no more paper, paper jam, etc.. It transmits XON when these problems have been resolved.

Note 11:

The printer DTR signal is connected to the interface CTS signal if XON is not received.

STATEMENTS PRINTED LINE BY LINE (LISTING)

Note 12:

Available for V24 printing only.

Each statement corresponds to a call (16 fields maximum, separated by a space.)

Statement output format

USER	LINE TYPE	TIME DATE	DURATION	TAXES SERV	ADD. SERVICES DIALLED NUMBER	MODE	COST RING	USER NAME BUSIN. CODE
A101-->	L04	23/10/00 08:31	00:02:40	6 ST	00388677700	M	00:00 1.000	

Definition parameters for a statement

- Language for the printout

By OMC (Expert View), select: **Counting -> Counting** -> **Accounting Printout** -> **Language**

- Company name: max. 16 characters

By OMC (Expert View), select: **Counting -> Counting** -> **Accounting Printout** -> **Company name**

- Masking the last 4 digits of the dialled number

By OMC (Expert View), select: **Counting -> Counting** -> **Accounting Printout** -> check or uncheck **Masking of 4 last digits**

- Maximum number of statements per page: 1 to 99 (by default, 50)

By OMC (Expert View), select: **Counting -> Counting** -> **Accounting Printout** -> **Proofs per page**

- Form feed at the end of the day: yes/no (by default, no)

By OMC (Expert View), select: **Counting -> Counting** -> **Accounting Printout** -> check or uncheck **Form feed permitted**

- Select printing of a header on each page, on the first page or not at all

By OMC (Expert View), select: **Counting -> Counting** -> **Accounting Printout** -> **Head printout**

Note 13:

If the form feed is active, it will be performed:

- when the maximum number of statements per page has been reached
- at the end of the day: the number of statements printed in one day is indicated at the bottom of the page on the right-hand side (5 digits maximum)
- during startup if the header printing parameter is active

- Fields to be printed on the statement; if none of the fields below have been defined, a default counter statement is printed. It includes all the fields preceded by an asterisk (*): Selecting:

By OMC (Expert View), select: **Counting** -> **Counting** -> **Accounting Printout** -> **Printed fields** -> select each field:

- (*) charged user (yes/no)
- (*) call type (yes/no)
- (*) trunk No (yes/no)
- (*) date (yes/no)
- (*) time (yes/no)
- (*) duration (yes/no)
- (*) number of units (yes/no)
- (*) services (yes/no)
- (*) features (yes/no)
- (*) number dialled (yes/no)
- dialling mode (yes/no)
- ringing duration (yes/no)
- cost of call (yes/no)
- business code (yes/no)
- user name (yes/no)
- account (business) code name (yes/no)
- initial user (yes/no)
- carrier (yes/no)
- initial user – 8 digits (yes/no)
- charged user – 8 digits (yes/no)
- 4-digit line (yes/no)
- node (yes/no)

DESCRIPTION OF FIELDS IN A STATEMENT

FIELD	DESCRIPTION
USER (1)	5 characters (left justified) Outgoing call: empty field indicated by **** Incoming call: called number (hunt group or set) - AXXXX for a user (2, 3 or 4-digit dialing plans, or the last digits in the case of 8-digit dialling plans) - GX for a hunt group (G9 for the attendant group)

CHARGED USER (2)	5 characters (left justified) Outgoing call: caller Incoming call: user who answered the call Trunk identity not supplied: access number - AXXXX for the calling or called user * (2, 3 or 4-digit dialling plans, or the last digits in the case of 8-digit dialling plans) - LXX for an analogue line during break-in/break-out - NXX for T0 access (no private/public distinction) - PXX for T2 primary access (no private/public distinction)
TYPE	3 characters (left justified) Type of call: -->: outgoing call on public network <--: incoming call on public network CS+: request additional service CS-: cancel additional service
LINE	3 characters Number of the line: - LXX for a public analogue line - NXX for a public or private T0 base access - PXX for a public or private T2 primary access For wake-up calls: R (for room)
DATE	8 characters Date of the call, made up of 3 x 2 numbers separated by "/"
TIME	5 characters Start time of the call, made up of 2 x 2 numbers separated by ":"
DURATION	8 characters Duration of the call, 3 x 2 numbers separated by ":" For wake-up calls: programmed time
UNITS or PULSES	5 characters Number of counter units
SERV.	2 characters Bearer services: - ST: telephone service (voice, G3 fax, teletex, videotex) - T+: G4 fax, transparent data transmission
ADD. SERVICES	Max. 6 characters (each character indicates one additional service; all 6 additional services can thus be activated together) Additional service: - I: user to user signalling - R: terminal forwarding (external forwarding) - T: online counting - S: substitution (DISA transit) - X: change party (transfer) - N: PCX forwarding

EXTERNAL CORRESPONDENT NUMBER	26 characters (left justified) Dialled number: - outgoing call: the number transmitted on the line (public or private) - incoming call: the number received on the line (public or private) - the destination number for external forwarding For wake-up calls: WAKE-UP PROGRAMMED, WAKE-UP CANCELLED, WAKE-UP ACKNOWLEDGED, WAKE-UP NOT ACKNOWLEDGED: FREE or BUSY, SET NOT AVAILABLE
MODE	1 character Dialling mode - M: manual dialling - I: individual (or personal) speed dial numbers - R: system (common) speed dial numbers
RING	5 characters Duration of the ringer, for all incoming ringing phases, made up of 2 x 2 numbers separated by ":"
COST	10 characters Cost of the call including ISDN service activation, where applicable
BUSINESS CODE	16 characters (right justified) Charge account code specific to the call
USER NAME	16 characters User name: - outgoing call: caller - incoming call: called party - name associated with the account code
NODE	Field not used
CARR.	1 character Attendant identifier
INITIAL USER	9 characters (left justified) Same functions as field 1; employed when using an 8-digit dialling plan
CHARGED USER	9 characters (left justified) Same functions as field 2; employed when using an 8-digit dialling plan
LINE 4	Field used instead of LINE when identification requires 4 characters; in this case, the NXX and VXX identifiers from the LINE field are replaced by N** and V**.

EXAMPLES OF STATEMENTS (LISTINGS)

Outgoing call

USER	LINE TYPE	TIME DATE	TIME DURATION	TAXES SERV	FACILITIES DIALLED NUMBER	MODE	COST RING	USER NAME BUSIN CODE
A101-->	NI	23/10/00	08:31 00:02:40	6 ST	00388677700	M	00:00 1.000	DUPONT

Transfer of an outgoing call

A101 calls an external number then transfers the communication to 125.

USER	LINE TYPE	DATE	TIME DURATION	TAXES SERV	FACILITIES DIALLED NUMBER	MODE	COST RING	USER NAME BUSIN CODE
A101 -->	N1	23/10/00	08:31 00:02:40	6 ST	00388677700	M 00:00	1.000	DUPONT
A125 -->	N1	23/10/00	08:31 00:03:20	8 STX	00388677700	M 02:00	1.000	MARTIN

Transit call

A101 is forwarded on the private external number 751234.

USER	LINE TYPE	DATE	TIME DURATION	TAXES SERV	FACILITIES DIALLED NUMBER	MODE	COST RING	USER NAME BUSIN CODE
A101 CS+		23/10/00	08:31 00:00:00	0 ** R	751234	M 00:00	0.000	DUPONT
A101 I->	N1	23/10/00	08:31 00:03:20	1 ST	751234	M 00:00	1.000	DUPONT
A101 <-I	N1	23/10/00	08:31 00:03:20	0 ST		M 00:00	1.000	DUPONT

Incoming user call

Incoming call answered by the called subscriber.

USER	LINE TYPE	DATE	TIME DURATION	TAXES SERV	FACILITIES DIALLED NUMBER	MODE	COST RING	USER NAME BUSIN CODE
A101 A101 <--	N1	23/10/00	08:31 00:02:40	0 ST	00388677700	M 00:04	0.000	DUPONT

Incoming call answered by a subscriber (A125) other than the called subscriber (dynamic forwarding, interception, monitoring, immediate forwarding).

USER	LINE TYPE	DATE	TIME DURATION	TAXES SERV	FACILITIES DIALLED NUMBER	MODE	COST RING	USER NAME BUSIN CODE
A125 A101 <--	N1	23/10/00	08:31 00:02:40	0 ST	00388677700	M 00:04	0.000	MARTIN

Incoming hunt group call

Incoming answered hunting group call.

USER	LINE TYPE	DATE	TIME DURATION	TAXES SERV	FACILITIES DIALLED NUMBER	MODE	COST RING	USER NAME BUSIN CODE
G50 A125 <--	N1	23/10/00	08:31 00:02:40	0 ST	00388677700	M 00:04	0.000	MARTIN

External forwarding

The operator is forwarded on the external number 0388677700; 125 calls the operator.

USER	LINE TYPE	DATE	TIME DURATION	TAXES SERV	FACILITIES DIALLED NUMBER	MODE	COST RING	USER NAME BUSIN CODE
G9	CS+	23/10/00	08:31 00:00:00	0 ** R	00388677700	M 00:00	0.000	PO
G9	--> N1	23/10/00	08:31 00:03:20	1 ST	00388677700	M 00:00	1.000	
G9	CS-	indicates forward cancelled						

CALL DETAIL RECORDS (TICKETS)

Note 14:
Available for V24 printing only.

Printout format of a record

Definition parameters for a record

- Language for the printout

By OMC (Expert View), select: **Counting -> Counting** -> **Accounting Printout** -> **Language**

- Company name: max. 16 characters

By OMC (Expert View), select: **Counting -> Counting** -> **Accounting Printout** -> **Company name**

- Masking the last 4 digits of the number dialled

By OMC (Expert View), select: **Counting -> Counting** -> **Accounting Printout** -> check or uncheck **Masking of 4 last digits**

Description of fields in a counter record

FIELD	DESCRIPTION
USER/SUBSCRIB or TERMINAL	Number of the set or terminal (max. 8 characters) This number is preceded by A if it corresponds to a set
DATE	Current date. 8 characters: 3 x 2 digits separated by "/"
LINE	3 characters Number of the trunk line used (2 characters) - LXXX for a public analogue line - NXXX for a public or private T0 base access - PXXX for a public or private T2 primary access - VXXX for an IP trunk
TIME	Start time of the call, made up of 2 x 2 numbers separated by "H".
NUMBER	Number dialled (max. 26 characters)
COST	Cost of the call or additional service

XML TICKET

Note 15:
For IP metering only.

Example of an XML ticket

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSPY v5 rel. 2 U (http://www.xmlspy.com) by ALCATEL BUSINESS SYSTEM (ALCATEL
BUSINESS SYSTEM) -->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
   <xs:element name="CallAccounting">
      <xs:annotation>
         <xs:documentation>OmniPCX Office Call Acounting ticket</xs:documentation>
      </xs:annotation>
      <xs:complexType>
         <xs:sequence>
            <xs:element name="UserInitial" type="userField" minOccurs="0"/>
            <xs:element name="UserCharged" type="userField"/>
            <xs:element name="Date" type="xs:date">
               <xs:annotation>
                  <xs:documentation>Begin of Communication or action date</xs:documentation>
               </xs:annotation>
            </xs:element>
            <xs:element name="Time" type="xs:time">
               <xs:annotation>
                  <xs:documentation>Begin of Communication or action date</xs:documentation>
               </xs:annotation>
            </xs:element>
            <xs:choice>
               <xs:element name="Metering">
                  <xs:complexType>
                     <xs:sequence>
                        <xs:element name="Type">
```

Definition parameters for an XML ticket

- Language: English is the only language supported.
- Company name: max. 16 characters

By OMC (Expert View), select: **Counting -> Counting** -> **Accounting Printout** -> **Company name**

By OMC (Expert View), select: **Counting -> Counting** -> **Accounting Printout** -> check or uncheck **Masking of 4 last digits**

Description of fields in an XML document

An XML schema has been defined to provide the structure of a call accounting ticket.

The schema definition of an XML ticket is published via an XSD file: CAPTicket_Vxxx.yyy.xsd

WAKE-UP

Conditions for printing a record/statement for wake-up calls or temporary appointment reminders:

- Wake-up activated
- Wake-up cancelled
- Wake-up failed
- Wake-up answered

By OMC (Expert View), select: **Counting -> Counting** -> **Accounting Printout**-> **Appointment printout for**

Printout format for a record

```
N 19              ALCATEL
SUBSCRIBER     A122
DATE       :     25.12.2000
TIME       :     08:35
ALARM ACKNOWLEDGED
```

Printout format for a statement

USER	LINE TYPE	TIME DATE	DURATION	TAXES SERV	FACILITIES DIALLED NUMBER	MODE RING	COST BUSIN CODE	USER NAME OPERAT.	NODE
A122 -->	R	25/12/00	08:31	07:45	ALARM PROGRAMMED				
A122 -->	R	25/12/00	08:31		ALARM CANCELLED				
A122 -->	R	25/12/00	08:35		ALARM ACKNOWLEDGED				
A140 -->	R	25/12/00	08:31		ALARM NOT ACKNOWLEDGED : FREE				
A145 -->	R	25/12/00	08:35		ALARM NOT ACKNOWLEDGED : BUSY				
A146 -->	R	25/12/00	08:35		ALARM STATION NOT AVAILABLE				

The fields TYPE, PULSES/UNITS, MODE, RING, COST, BUSINESS CODE and USER NAME are not significant. The DURATION field is only filled in if the time is programmed.

R = room.

XML output

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- generated by OmniPCX Office -->
<CallAccounting xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="CAPTicket_V001.001.xsd">
<OmniPCXOffice>
<SoftwareVersion>3EH30368ASAA ALZFR500/aaa.bbb</SoftwareVersion>
<CPUIPAddress>123.45.678.900</CPUIPAddress>
</OmniPCXOffice>
<Checksum>781229559</Checksum>
<TicketType>Wake-up</TicketType>
<CompanyName>Barnett Telecom</CompanyName>
<ChargedUserType>A</ChargedUserType>
<ChargedUserID>109</ChargedUserID>
<SubscriberName>Georges Newton</SubscriberName>
<Date>2005-11-22</Date>
<Time>15:30:00</Time>
<WakeUpAction>ACKNOWLEDGED</WakeUpAction>
</CallAccounting>
```

8.4.11 Using the Euros

8.4.11.1 Operation

This paragraph describes the configurations which need to be carried out to accommodate for the integration of the Euro in several European countries.

The following parameters need to be configured:

- The conversion rate with the current currency of the country:

• By OMC (Expert View), select: **Counting** -> **Currency Conversion** -> **Exchange Rate**

- Specify whether the public network carrier carries out this conversion at the same date.

• By OMC (Expert View), select: **Metering** -> **Currency Conversion** -> **check ? No Conversion, ? User Defined or ? Immediately**

- The label used ("EUR", for example):

• By OMC (Expert View), select: **Counting -> Counting** -> **Counting Options for Inactive Currency** -> **Currency Name**

- the date and time of the conversion:

• By OMC (Expert View), select: **Metering** -> **Currency Conversion**-> **Conversion Date & Time (only on selecting ? User Defined**

At the date and time specified, the system will manage the following Euro conversions:

- partial counters and accumulated counters of sets and meter credit for Hotel clients.
- basic counter charge cost and cost thresholds (Business and Hotel), cost of VAT (Hotel).
- cost of counter reminder.

If the public carrier carries out the conversion, then the conversion report between the system currency and the public network currency is equal to 1, and the following parameters are to be configured:

- real cost of the counter unit.
- cost of UUS and PCX forwarding.

8.4.12 Metering on IP

8.4.12.1 Operation

8.4.12.1.1 Driver installation procedure

There are two ways to install the Office Link driver:

- **Interactive** (graphic) mode installation - installs the driving using the InstallShield Wizard running on a client PC.
- **Silent** mode installation - allows you to run the installation program in the background without interactive input. This method is based on a previously configured input file that feeds configuration parameters to the installation program. The input file can later be used for future driver modifications or remote updates.

Note 1:

Before installing the Office Link driver, you must meet the following password requirements:

- *You must have administrator privileges on the local PC.*
- *The local PC administrator password must be the same as the OMC administrator password.*
- *The Alcatel-Lucent OmniPCX Office Communication Server administrator password must be entered into the input file.*

If you are installing the Office Link driver on a system that is already running an OHL driver, the installation program will recognise the existing driver and will inform you that the old driver and all associated files will be removed before the new driver is installed.

Interactive installation

To install the Office Link driver using the InstallShield Wizard:

1. Configure the Alcatel-Lucent OmniPCX Office Communication Server to enable the taxation over IP feature.
2. Verify that you have a valid licence for the taxation over IP feature.
3. Install the driver by runing the `setup.exe` file located in the ????????? directory on the provided CD-ROM.
   Follow the Wizard's instructions to complete the driver installation.

   Note 2:
   *The installation program will ask you to select one of two driver modes: **metering** or **hotel**. The InstallShield will also install a driver configuration program on the PC. A shortcut to the configuration program will be placed on the PC desktop.*

Silent installation

You can use the command line or "silent" mode installation procedure to install the Office Link driver in the background without need for user interaction. This method uses a previously generated input file to store configuration information. The input file must first be generated by running the `setup.exe` program with an `/r` (record) switch. Driver configuration parameters are then written to a `setup.iss` file stored in a user-specified location.

To install the driver in silent mode:

1. Run the installation program to record configuration parameters to the`setup.iss` configuration file:
   `setup.exe /r /f1 c:\setup.iss`
   Where the `/r` switch creates the configuration file and the `/f1` argument allows you to specify a location for the `setup.iss` file.
2. Use the InstallShield Wizard to enter configuration parameters according to the requirements of your site.
   When you have finished, the configuration parameters are written to the `setup.iss` file which can then be edited to modify parameters for future driver modifications and updates.
3. Once you have verified driver configuration parameters in the `setup.iss` file you can run the driver installation program in silent mode by entering:
   `setup.exe /f1 c:\setup.iss`
   The installation program applies the recorded parameters to the driver configuration.
4. Upon completion of the driver installation you must restart the system in order to load the drive as a Windows startup service.
   The driver is installed and running and you can now configure the driver with the driver

configuration utility.

Configuration file settings

The `setup.iss` configuration file can be customised by editing specific fields. Fields that can be edited include:

- **szDir** : indicates the name of the target installation directory.
- **szFolder** : indicates the name of the Program folder where the driver will be installed.
- **UpdateOption** : used to enable internet updates.

Uninstalling the driver

You can uninstall the driver at any time using one of the following methods:

- Use MS Windows **Add/Remove Programs** function.
- Use the **Uninstall OHL driver** shortcut located on the desktop and in the Programs folder.
- Launch the installation program and select the **Remove** checkbox.

8.4.12.1.2 Driver configuration procedure

Once the Office Link driver is installed and running you can launch the provided OHL driver configuration program to set various driver parameter values. Driver configuration parameters are stored in the `OhlDriver.conf` file located in the driver installation directory. This file contains all Office Link driver parameter which are set with default values when the driver is first installed. The file can be edited to update certain parameters that are not configured by the OHL driver configuration program.

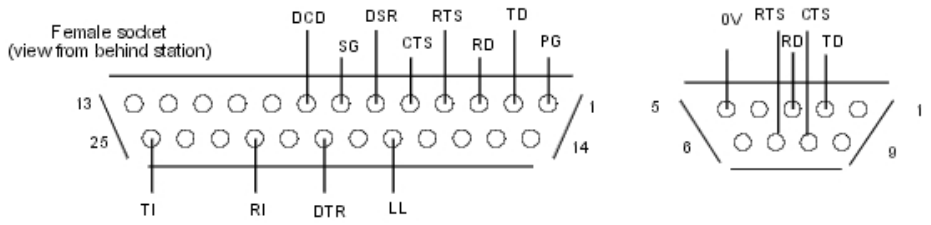
To configure an installed and running Office Link driver:

1. Run the OHL driver configuration program by clicking on the desktop shortcut or by selecting the OHL driver configuration program located in the driver installation folder.
   The OHL driver configuration window is displayed with information about the driver version and the installation mode. This window contains various functions to start/stop the driver and to test the driver connection. An **Autodetect** feature automatically detects the Host name address of the Alcatel-Lucent OmniPCX Office Communication Server. The **Default** button can be used to set all fields to default values.
2. Once you have verified that all fields contain the desired parameter values, click **Quit** to save the values to the `OhlDriver.conf` configuration file and quit the OHL configuration program.

8.4.13 Appendix

8.4.13.1 ANNEX: V24 CONFIGURATIONS

8.4.13.1.1 V24 Signals



Functions performed by the various managed circuits (indications for 25-point connectors)

No of pin	No of circuit	Meaning	Abbreviation		Direction
			CCITT	EIA	
1	101	Protection Ground	TP	PG	
7	102	Signal Ground	TS	SG	
2	103	Transmit Data	ED	TD	DTE --> DCE
3	104	Receive Data	RD	RD	DTE <-- DCE
4	105	Request To Send	DPE	RTS	DTE --> DCE
5	106	Clear To Send	PAE	CTS	DTE <-- DCE
6	107	Data Set Ready	PDP	DSR	DTE <-- DCE
20	108/1 108/2	Connect Data Set Data Terminal Ready	CPD TPD	(*) DTR	DTE --> DCE DTE --> DCE
8	109	Data Carrier Detect	DS/DP	DCD	DTE <-- DCE
22	125	Ring Indicator	IA	RI	DTE <-- DCE
18	141	Local Loop	BL	LL	DTE --> DCE
25	142	Test Indicator	IT	TI	DTE <-- DCE

(*): pin not assigned in standard EIA-RS232

101 (1) : Protection Ground (PG)

This pin ensures continuity between the earth on the cable and on the optional board (the protection and signal grounds are in this case connected to a joint reference).

102 (7) : Signal Ground (SG)

Reference potential for the junction circuits.

103 (2) : Transmitting Data (TD)

The data signals from the DTE are transmitted to the DCE on this circuit.

104 (3) : Receiving Data (RD)

The data signals from the DCE are transmitted to the DTE on this circuit.

105 (4) : Request To Send (RTS)

This circuit commands the DCE to prepare to transmit on the data channel.

Closed status forces the DCE into transmission mode.

Open status forces the DCE into non transmission mode on the data channel once all the data transferred on circuit 103 has been transmitted.

When connecting a DTE without a circuit 105, you should loop circuits 105 and 106 on the DCE socket.

106 (5) : Clear To Send (CTS)

This circuit indicates whether the DCE is ready to receive data signals on circuit 104 and to transmit them on the data channel.

Closed status indicates that the DCE is ready to receive data signals from the DTE on circuit 103.

Open status indicates that the DCE is not ready to receive data signals from the DTE on circuit 103.

In full-duplex mode, this circuit, in association with circuit 105, enables flux control during the data transfer phase. Closed status means that the remote unit authorizes transmission.

107 (6) : Data Set Ready (DSR)

The closure of this circuit indicates that the DCE is ready to operate. This acknowledges the data channel trunk seizure.

In addition to the trunk seizure, this circuit indicates that the DCE is ready to exchange other signals to trigger the data exchange (initialize the dialog).

108/1 (20) : Connect data set to line (CDSL)

This signal, transmitted by the DTE, forces the DCE to connect to the data channel.

Incoming call: As a general rule, the DTE emits this signal in response to an incoming call defined by the closure of circuit 125 on the DCE. The DCE then closes circuit 107 as soon as the line is seized, which triggers the dialog initialization phase. This circuit enables the DTE to remain in control of the response to incoming calls, postponing or barring trunk seizures during critical operating phases.

Outgoing call: The closed status of this circuit can be used to initialize an outgoing direct call with an automatic call DCE.

108/2 (20) : Data Terminal Ready (DTR)

The DTE closes this circuit to tell the DCE it is ready to operate.

Incoming call: closing circuit 108/2 authorizes the DCE to take an incoming call. The DTE is advised accordingly by the closure of circuit 107 to indicate the trunk seizure. The dialog initialization phase now begins.

Outgoing call: the outgoing call is initialized between the DTE and the DCE by a local dialog exchanged on circuits 103 and 104.

109 (8) : Data Carrier Detect (DCD)

Closing this circuit indicates that the carrier signal received on the data channel meets the relevant specifications.

This circuit can also be used in the closed state for DTE-DCE data exchanges when programming or controlling serial automatic call DCEs.

125 (22) : Ring Indicator (RI)

This circuit is closed to tell the DTE that a call signal has been received by the DCE.

141 (18) : Local Loop (LL)

This circuit controls type 3 test loops in the DCE.

The closure of the circuit loops the DCE transmission channel back to the reception channel, on the data channel side. On detecting that circuit 142 is closed, the DTE can then, in full-duplex mode, test the DCE transmission interfaces. This looping function is not yet available in the current state of development of the product.

142 (25) : Test Indicator (TI)

The closure of circuit 142 indicates that the DCE is in test mode, which precludes any transmission with a remote DTE.

8.4.13.1.2 V24 metering printouts: configuration details

Physical characteristics

- Type of interface: V24
- Operating mode: asynchronous
- Interface function: DCE

Transmission characteristics

- Number of significant characters: 5, 6, 7 or 8 (default value)
- Parity: even, odd, no (default value), marked (set at 1) or spaced (set at 0)
- Number of stop bits: 1 (default value), 1.5 or 2
- Baudrate: 50, 75, 150, 300, 600, 1200, 2400, 4800, 9600 (default value), 14400, 19200
- Rate adaptation: V110 (default value), X31, V120 or V14E (for 57600 bps)

Flux control

Possibilities available in either instance – flux control of the terminal by the adapter and vice versa:

- Mode: none (no flux control), inband (control with 2 characters - XON and XOFF by default) or circuit (control with the RTS and CTS signals)
- If Mode = inband, then decimal value for XON (17 by default) and XOFF (19 by default)

Implicit number of XON characters

This field defines the number of XON characters required to boot the equipment:

- Zero
- One
- Two
- Three
- Four
- XANY (non-significant option)

Echo

Check the box for a local or character by character echo in Command mode.

No input acknowledgement

Check the box to operate without V24 device input acknowledgements at the terminal.

Display caller address

Check the box to send the caller address to the terminal or DCE.

Escape sequence

This field defines a sequence of 3 characters maximum for switching the V24 device from CONNECTED (data transmission) mode to COMMAND mode. Each character is defined by entering its decimal value: the hexadecimal value and the character are displayed automatically.

Communication protocol

- Hayes

- Automatic
- V25 bis 108/1
- V25 bis 108/2

DSR option

This field defines the operating mode for the DSR signal:

- Always active
- Active during the call
- Inactive in release phase

DTR option

This field defines the reaction of the DTR signal:

- Normal
- Forced

RTS option

This field defines the reaction of the CTS signal when the RTS signal changes state:

- CTS tracks RTS
- RTS ignored, CTS ON

Inactivity timeout

This field defines, in 30-second increments, the period of inactivity after which the call is released.

Loopback mode

This field defines the test loopback employed:

- no loop
- loop 1 (as defined by the V54 recommendation)
- loop 2 (as defined by the V54 recommendation)

8.5 Local Call Metering

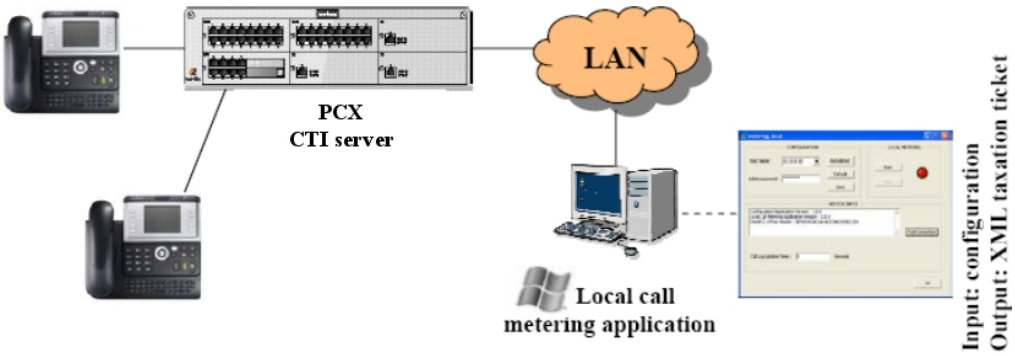
8.5.1 Overview

The following information only applies to the China market.

8.5.1.1 Basic Description

The "local call metering" application is an external application on a PC that allows to:

- Retrieve all local call log tickets from the Alcatel-Lucent OmniPCX Office Communication Server via the Open Telephony Service
- Generate metering data
- Store these tickets in an XML output file



8.5.2 Operation

8.5.2.1 Presentation

8.5.2.1.1 Call Log Information in the Open Telephony Server Service

The "local call metering" application retrieves call log tickets via the Open Telephony Server service.

- The Open Telephony Server service can save up to 200 tickets in a buffer
- Local call log tickets are deleted when they are sent to the "local call metering" application
- Unsuccessful calls (busy, unanswered call, etc.) are not logged in the Open Telephony Server service
- One local call in conversation generates one ticket

8.5.2.1.2 Local Call Metering Application Structure

The "local call metering" application consists of the following blocks:

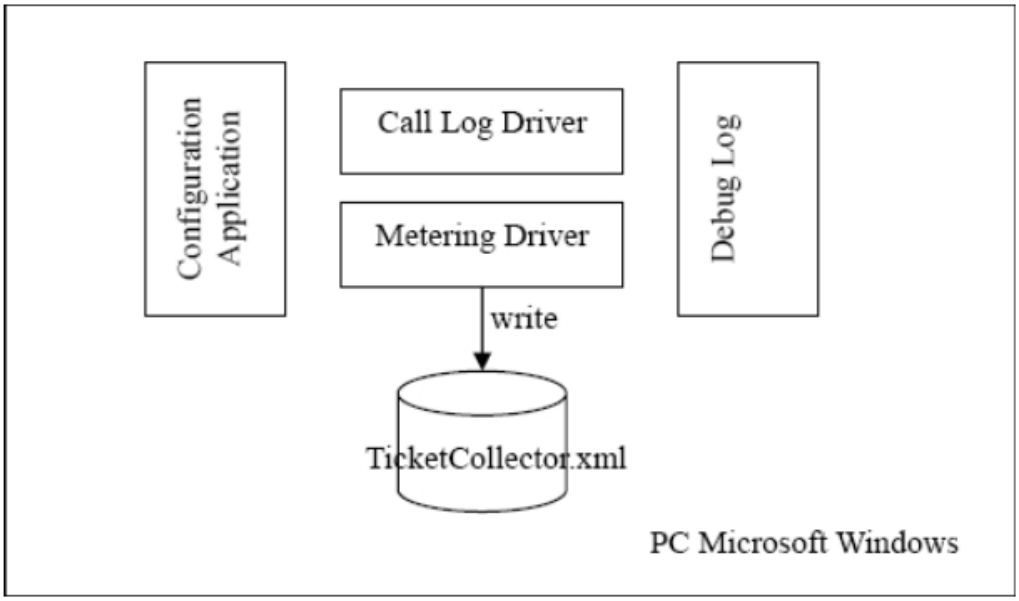


Figure 8.34 : Local Call Metering Application structure

- The **Configuration application** is a user-friendly interface used to configure the local metering file
- The **Call Log Driver** retrieves all call log events from the Alcatel-Lucent OmniPCX Office Communication Server and presents these log events in an orderly manner
- The **Metering Driver** stores the local call log tickets in the output file (TicketCollector.xml)
  - The **TicketCollector.xml** is the output file for tickets on the PC
- **Debug/Log** is a global log text file, where all traces are stored

Log File

The global log file, located in the "Local call metering" application installation directory, contains the following information:

- "Local call metering" interface information
- Alcatel-Lucent OmniPCX Office Communication Server information
- Warning/Error information

XML File

When installing the "Local call metering" application, the Open Telephony Server interface must be active.

When the "local call metering" application is running, call log information (metering tickets) is extracted via the Open Telephony Server. These metering tickets are stored in an XML local file, located in the application installation directory (by default) and named "TicketCollector.xml" (by default).

The maximum number of tickets stored in the XML file can be changed by modifying the

configuration file.

The call log information includes:

- Call date, call start time and call end time
- Initial number: initial called party in case of transfer, pick-up, or other similar operation
- Caller number
- Called number and name (if available)

Note:

When the tickets number limit is reached, the "TicketCollector" file is emptied and its content is copied on the local directory to an archive file as: TicketCollector_yyyymmdd_hhmmss.xml:

where "yyyymmdd" is the archive date and "hhmmss" is the archive time.

8.5.2.2 Installation

8.5.2.2.1 Installing the "Local Call Metering" Application

Prerequisite: Before installing the "local call metering" application, the user must have administrator privileges on the local PC.

There are two ways to install the "local call metering" application:

- **Interactive** (graphic) mode installation - installs the application using the InstallShield Wizard running on a client PC.
- **Silent** mode installation - allows you to run the installation program in the background without interactive input. This method is based on specific command line parameters.

If installing the "local call metering" application on a system that already includes a "local call metering" application, the installation program acknowledges the existing application and offers a "Modify" mode, and a "Remove" mode, so as to remove the old application and all associated files before the new application is installed.

The "local call metering" application includes a configuration application and a "local call metering" service.

Interactive installation

From the CD-ROM/DVD or from the download page of the WEB site:

To install the "local call metering" application using the InstallShield Wizard:

1. Install the application by running the `setup.exe` file located in the installation directory
2. Follow the Wizard's instructions to complete application installation
3. Restart the system in order to load the "local call metering" application as a Windows startup service

   It appears in the Windows "Services" list with an automatic (default value) `Startup Type`.

Note 1:

The InstallShield also installs an application configuration program on the PC. A shortcut to the configuration application is available from the PC desktop.

Silent installation

You can use the command line or "silent" mode to install the "local call metering" application in

the background with no need for user interaction.

To install the "local call metering" application in silent mode:

1. Run the following command: `setup.exe /S /v"/qn INSTALLDIR=product_folder USERNAME="username""`
   Where:
   - The product_folder is the user target folder
   - The user name must be entered within quotation marks.

   Note 2:
   The `setup.exe` file extracted from ZIP file "lcma_7.0.0_X.X.X_XX_Alcatel.zip.

   Caution:
   Do not add any space character between the option and its parameter:

   Example:

   - ***`setup.exe /S /v"/qn INSTALLDIR=c:\PCXTools USERNAME="Tom""`: The command is correct.***
   - ***`setup.exe /S /v "/qn INSTALLDIR=c:\PCXTools USERNAME="Tom""`: The command is not correct.***
2. Restart the system in order to load the "local call metering" application as a Windows startup service

   It appears in the Windows "Services" list with an automatic (default value) `Startup Type`.

Upon completion of installation

The "local call metering" application and its associated configuration application are installed on the PC.

Note 3:
The files included in the installation directory are the following:

- *metering local.exe*: "local call metering" application configuration files
- *metering service.exe*: "local call metering" service files
- *LCMA. conf*: configuration files (once the application has been run)
- *TicketCollector. xml*: output files (once the application has been run)

The "local call metering" application is installed and running.
You can now configure the "local call metering" application with the "local call metering" application configuration program.

Note 4:
In case of a PC crash while the "local call metering" application is running, the application restarts automatically.

8.5.2.2.2 Uninstalling the "Local Call Metering" Application

You can uninstall the "local call metering" application at any time using one of the following methods:

- Use the MS Windows **Add/Remove Programs** feature and select the "local call metering" application.
- Use the **Uninstall "local call metering" application** shortcut located on the desktop or in

the Programs folder.

- Launch the installation program via `setup.exe` and select the **Remove** checkbox.

8.5.2.2.3 Updating the "Local Call Metering" Application

You can update the "local call metering" application at any time using one of the following methods:

- Launch the installation program via `setup.exe` and select the **Modify** checkbox.
- Uninstall the "local call metering" application and install the new "local call metering" application.

8.5.2.3 Configuration

8.5.2.3.1 Configuring the "Local Call Metering" Application

This is used to:

- Configure the Alcatel-Lucent OmniPCX Office Communication Server name/address
- Configure the password
- Start/stop the application

Once the "local call metering" application is installed and running, you can launch the "local call metering" application configuration program to set various driver parameter values.

"Local call metering" application configuration parameters are stored in the `LCMA.conf` file located in the "Local call metering" application installation directory.

This file contains all "Local call metering" application parameters which are set with default values when the "Local call metering" application is first installed. The file can be edited to update certain parameters that are not configured by the "Local call metering" application configuration program.

To configure an installed and running "local call metering" application:

1. Run the "local call metering" application configuration program by clicking the desktop shortcut or by selecting the "local call metering" application configuration program located in the "local call metering" application installation folder.

   The "local call metering" application configuration window is displayed with information about the application version and the installation mode.

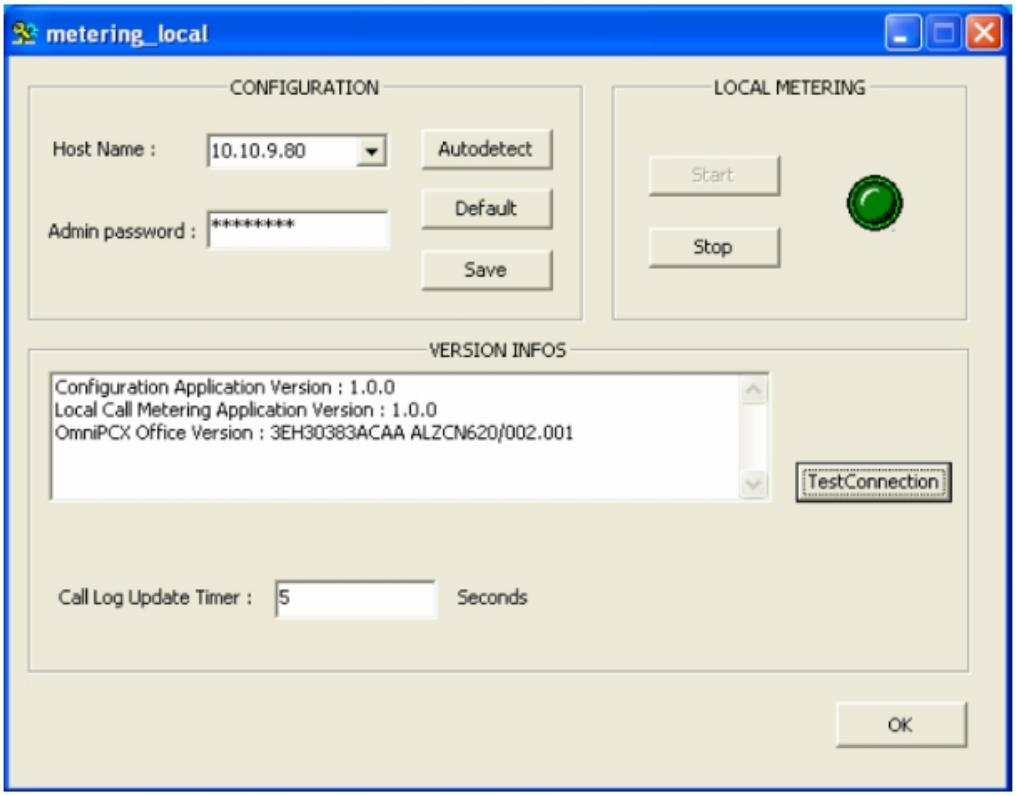


Figure 8.35 : Configuring the "Local Call Metering" application

- Click **Save** to save the Alcatel-Lucent OmniPCX Office Communication Server *Host Name* address and the *Admin password* to the `LCMA.conf` configuration file.
- Click **Default** to set all fields to their default values.
- Click **Autodetect** to detect automatically the Alcatel-Lucent OmniPCX Office Communication Server host name address.

  Note 1:
  *If the **Autodetect** feature fails, the field can also be filled in manually.*
- Click **TestConnection** to test the Alcatel-Lucent OmniPCX Office Communication Server *Host Name* address, the *Admin password* and the application version.
- Click **Start** /**Stop** to start or stop the "local call metering" service.

  Note 2:
  The current application status is indicated by a green or red icon.
- The **Call Log Update Timer** is a timer mechanism to read in time the call log from the Alcatel-Lucent OmniPCX Office Communication Server.

  The number of Open Telephony Server logs is limited to 200 in the Alcatel-Lucent OmniPCX Office Communication Server. The "CALLLOG_UPDATE_TIMER" parameter must be managed according to the number of users and traffic in order to avoid any loss of logs.

2. Once you have verified that all fields contain the desired values, click **OK** to save the values to the `LCMA.conf` configuration file and quit the "local call metering" application

configuration program.

8.5.2.3.2 "LCMA.conf" Configuration File

The `LCMA.conf` configuration file can be customized by editing specific fields. Fields that can be edited include:

- Alcatel-Lucent OmniPCX Office Communication Server parameters:
  - **OXO_PASSWORD**: Alcatel-Lucent OmniPCX Office Communication Server administrator password.
  - **OXO_LOG_LEVEL**: Alcatel-Lucent OmniPCX Office Communication Server log level (up to 4).
  - **OXO_TIMEOUT**: "Local call metering" application inactivity connection time limit (in second) (default value: 30s).
  - **OXO_IP_HOSTNAME**: Alcatel-Lucent OmniPCX Office Communication Server host name identifier (IP address or host name identifier).
- Proxy parameters:

  The "local call metering" application can connect to the Alcatel-Lucent OmniPCX Office Communication Server via a proxy server.
  - **PROXY_IP_HOST_NAME**: Hostname or proxy server IP address.
  - **PROXY_PORT_NUMBER**: Proxy server port number.
  - **PROXY_USER_NAME**: User name used to login to the proxy server.
  - **PROXY_USER_PASSWORD**: User password.
  - **LCMA_NETWORK_LOG_LEVEL**: Log level (up to 4): network status trace level between the "local Call Metering" application and the Alcatel-Lucent OmniPCX Office Communication Server.
- Metering parameters:
  - **METERING_COLLECTOR_DIR**: Tickets collector file directory name.
  - **METERING_COLLECTOR_FILE**: Tickets collector file name (by default: TicketCollector (without extension)).
  - **METERING_COLLECTOR_MAX_TICKET**: Metering tickets maximum number stored in the TicketCollector file (by default: 2000).
- Call log parameters:
  - **CALLLOG_UPDATE_TIMER**: Duration to send read call log request to the Alcatel-Lucent OmniPCX Office Communication Server.
  - **CALLLOG_LOG_LEVEL**: CALLLOG Log level (up to 4 levels).
- Global parameters:
  - **GLOBAL_LOG_FILE**: Global Log file name (by default: LOG.txt).
  - **GLOBAL_LOG_LEVEL**: Global information trace level.
  - **LOG_FILES_MAX_SIZE**: Log file maximum size (in bytes) (by default: 1 000 000).

8.6 CTI

8.6.1 Overview

8.6.1.1 Overview

Computer Telephony Integration (CTI) allows for the interaction of computer applications and telephony features (for example, call centres and PC-based telephony). The Alcatel-Lucent OmniPCX Office Communication Server provides a CTI application protocol called CSTA that conforms to the EMCA CSTA Standard Phase 1. Using a client-server model, CSTA implements a set of services for applications including:

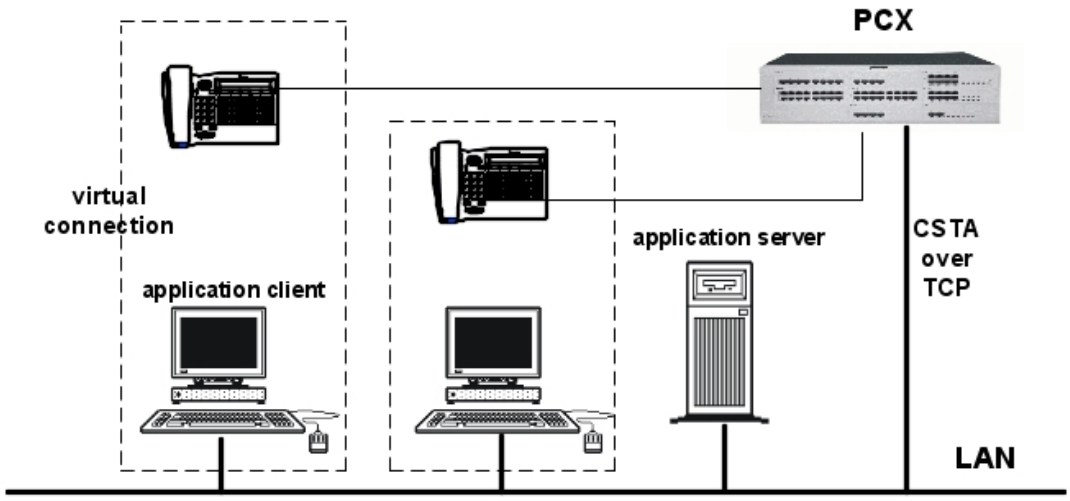
- Service requests: Direct function calls which support a specific service.
- Service responses: Confirmation events or universal failures.
- Unsolicited Events: Provided when external events occur.

A list of specific applications supported by CSTA can be found on the Web under AAPP (Alcatel-Lucent Application Partner Program).

8.6.1.2 Topology and Configuration

The CSTA protocol is delivered on an Ethernet TCP/IP link via the Alcatel-Lucent OmniPCX Office Communication Server system CPU board. CSTA is available on all Alcatel-Lucent OmniPCX Office Communication Server systems.

A CTI application can use CSTA for many different architectures including first-party and third-party CTI. The following figure shows one possible application architecture: third-party CTI in a client-server environment.



A CSTA link is made over TCP between the CTI application computer and the Alcatel-Lucent OmniPCX Office Communication Server CSTA server on the PCX.

Alcatel-Lucent OmniPCX Office Communication Server CSTA supports multi-session CSTA: several applications can open a CSTA session at the same time. The CSTA switching domain is limited to the terminals and trunk lines directly connected to the Alcatel-Lucent OmniPCX Office Communication Server.

The IP address, subnet mask, and gateway address of the Alcatel-Lucent OmniPCX Office Communication Server CPU board must be correctly configured in **OMC -> Hardware and Limits -> LAN/IP Configuration -> Boards.**

8.6.1.3 Capacities

The CSTA processing capacities of the Alcatel-Lucent OmniPCX Office Communication Server are listed in the following table:

Processing capacities	Maximum
Number of simultaneous CTI application connections	75 (Advanced) 200 (Premium)
Number of simultaneous monitoring requests for a terminal	208
Number of active simultaneous supervisions per Alcatel-Lucent OmniPCX Office Communication Server system	208
Number of CSTA requests that can be queued in the PCX for all devices	30
Number of CSTA events per second	10
Number of CSTA switching requests per second	2

8.6.1.4 Supported Devices

The Alcatel-Lucent OmniPCX Office Communication Server CSTA services support the following devices:

- Alcatel-Lucent IP Touch 4018 Phone, Alcatel-Lucent IP Touch 4008 Phone, Alcatel-Lucent IP Touch 4028 Phone, Alcatel-Lucent IP Touch 4038 Phone, Alcatel-Lucent IP Touch 4068 Phone
- Alcatel-Lucent 4019 Digital Phone, Alcatel-Lucent 4029 Digital Phone, Alcatel-Lucent 4039 Digital Phone
- Alcatel-Lucent Mobile IP Touch 300/600
- Alcatel Reflexes multiline sets with or without headset: 4010 (Easy), 4020 (Premium), 4035 (Advanced)
- Alcatel Reflexes monoline sets: 4004 (First)
- Alcatel Reflexes wireless sets: DECT Reflexes
- Alcatel Reflexes monoline and multiline sets with wireless link (TSC–DECT)
- Wireless GAP terminals (must be registered in PCX in "Enhanced Mode")
- Analog sets
- Virtual terminals
- IP Subscribers on a PC

Note:
Devices not supported can be involved in communications with supported devices. In these communications, the supported device must make the CSTA service request.

8.6.2 CSTA Services

This section describes the implementation of the CSTA protocol on the Alcatel-Lucent

OmniPCX Office Communication Server. CSTA switching services are built on the basic switching features of the PCX. Therefore, the behaviour of the CSTA services will be similar to the that of the manual implementations.

The services implemented in the Alcatel-Lucent OmniPCX Office Communication Server CSTA are described below. The definition according to the ECMA CSTA standard is given, plus any details specific to the Alcatel-Lucent OmniPCX Office Communication Server.

Note:
Particularities of monoline and multiline sets can have consequences for CSTA. Some CSTA services may be relevant for only one type of set, or the behaviour of the service may vary according to the type of set. The number of simultaneous calls allowed for a set impacts the number of CSTA connections a device may have. For example, the system cannot answer a queued call on a monoline set if another call is on hold.

8.6.2.1 ECMA CSTA Services

8.6.2.1.1 Alternate Call

The Alternate Call service combines the Hold Call and Retrieve Call services. It places the current call on hold and then retrieves a previously held or alerting call to the same device.

The service supports monoline and multiline sets.

8.6.2.1.2 Answer Call

The Answer Call service connects an alerting or queued call. The Answer Call is allowed depending on the type of set and the current state of the set. When answering an alerting call, the behaviour is identical to a manual answer call. When answering a queued call, the behaviour is identical to a manual answer of a queued call: the current connection will either be released, put on hold, or queued.

Note:
In rare cases during heavy traffic conditions, a set with an alerting connection will be in hands-free mode after the Answer Call service request.

8.6.2.1.3 Call Completion

The Call Completion service invokes features (for example Callback or Intrude) to complete a call which might otherwise fail. Callback and Intrude are supported.

8.6.2.1.4 Change Monitor Filter

The Change Monitor Filter service changes the monitoring filter on an existing monitoring process. Private filters may be configured to filter the CSTA private events.

8.6.2.1.5 Clear Connection

The Clear Connection service releases a device from a specified call and leaves the connection in the null state. The behaviour is identical to hanging up a manual call. Clear Connection is supported for the current connection when it is in a connected, initiated, or failed state. The service supports Callback and Make call prompts, ringing and queued calls.

8.6.2.1.6 Conference Call

The Conference Call service creates a conference from an existing held call and another

active call at a conference device. The two calls are merged into a single call and the two connections are merged into a single, new connection. Three parties are involved: The Conference Master party is the device activating the conference. The Conference Master must have at least one call on hold (Conference Held party), and one call in conversation (Conference Active party).

The end of conference behaviour depends on who ends the conference:

- If the Conference Master hangs up or clears the connection, all connections in the conference are cleared.
- If the Conference Held party hangs up or clears the connection, the connection at the Conference Held party side is cleared, and the Conference Master and Conference Active parties return to conversation state.
- If the Conference Active party hangs up or clears the connection, the connection at the Conference Active party side is cleared. Depending on the configuration of the Alcatel-Lucent OmniPCX Office Communication Server, either the Conference Master and Conference Held parties return to a conversation state, or the Conference Held party returns to hold and a new call is initiated for the Conference Master.

Note:

The maximum number of simultaneous conference calls on the Alcatel-Lucent OmniPCX Office Communication Server is two.

8.6.2.1.7 Consultation Call

The Consultation Call service combines the Hold Call and Make Call services. It places an active call on hold and initiates a new call from the same device.

The behaviour is identical to a manual New Call and Automatic Hold on multiline sets, and to an enquiry call on monoline sets.

Since the system does not check the validity and state of the called device, the new call is initiated as soon as the active call has been put on hold.

8.6.2.1.8 Divert Call

The Divert Call service moves a call from one device to another.

Details specific to the Alcatel-Lucent OmniPCX Office Communication Server for the Divert Call service are:

- The connection to be diverted may be in the alerting or queued state.
- The connection to be diverted and the destination of the diversion may be either internal or external calls.
- The PCX requires the devices to be monitored:
  - the destination device must be monitored for individual pickup or group pickup
  - the device with the connection to be diverted must be monitored for call deflection

8.6.2.1.9 Escape

Escape

The Escape service allows for the installation of private services not defined in the ECMA CSTA protocol. See § Private Services for a description of private services defined for the Alcatel-Lucent OmniPCX Office Communication Server.

8.6.2.1.10 Hold Call

The Hold Call service places an existing connection on hold. The behaviour is identical to a manual Hold. The service supports multiline and monoline devices.

8.6.2.1.11 Make Call

The Make Call service creates a CSTA call between two devices.

Details specific to the Alcatel-Lucent OmniPCX Office Communication Server for the Make Call service are:

- The Make call service is allowed if the originating device is in the idle state, or has one call initiated, or is in the disconnected state (the remote party has cleared the connection).
- The system does not check the validity of the called device's number or state.
- If the device supports on-hook dialling, the service can be configured to start calls immediately without prompting.
- If no called number is provided, the device goes into hands-free or dialling mode.

Make Call sequence of events when device is in the idle state:

1. The originating device is in the idle state.
2. The service rings the originating device (local ringing). The service is unaware of the device's active features (for example, forwarded, monitored, do not disturb). If the device has a display, it displays "Automatic call".
3. The user can:
   - refuse the service using soft keys, the fixed release button, or, if the device is not in auto-answering mode, by waiting for the time-out (20 seconds).
   - accept the service by picking up, using soft keys, the hands-free button, or, if the device is in auto-answering mode, waiting for the time-out (5 seconds).

   Note 1:
   The auto-answering mode can be enabled only for sets having the broadcasting facility. It is not enabled for analog or GAP sets.
4. In the case where:
   - the service is accepted, the application dials for the user. The subsequent call progress information (tones, display, LEDs and soft keys) is identical to that of a manual call.
   - the service is refused, the device goes into the idle state. The initiated connection is cleared.

Note 2:

The Make Call prompt cannot be overloaded by another call.

Make Call sequence of events when device is in initiated state:

1. The originating device has one call in the initiated state.
2. The application immediately launches the call using the initiated connection and dialling for the user. The subsequent call progress information (tones, display, LEDs and soft keys) is identical to that of a manual call.

8.6.2.1.12 Monitor Start

The Monitor Start service provides event reporting for a CSTA device. Only device type

Monitor Start service is supported. Private filters may be configured to filter the CSTA private events.

8.6.2.1.13 Monitor Stop

The Monitor Stop service stops the monitoring process for a device initiated by the Monitor Start service.

8.6.2.1.14 Query Device

The Query Device service provides indications of the state of the device's features or static attributes. It is not necessary for the device to be monitored.

8.6.2.1.15 Reconnect Call

The Reconnect Call service combines the Clear Connection service and the Retrieve Call service. It clears an existing connection and then retrieves a previously held connection at the same device. The behaviour is identical to a manual consultation cancellation. The service supports monoline and multiline devices.

8.6.2.1.16 Retrieve Call

The Retrieve Call service connects to an existing call on hold. The behaviour is identical to a manual retrieve. The service supports monoline and multiline devices.

8.6.2.1.17 Set Feature

The Set Feature service sets the device's features. It is not necessary for the device to be monitored.

8.6.2.1.18 Single Step Transfer Call to Voice Mail

The Single Step Transfer Call to Voice Mail service transfers an active call at a device to the Voice Mail of another device. The service supports transfer of a call only to the Voice Mail of another device. Single step transfer call service to another device is not supported.

8.6.2.1.19 Snapshot Device

The Snapshot Device service provides call information for a specified CSTA device. The information includes the list of calls involving the device and the state of each connection.

8.6.2.1.20 Transfer Call

The Transfer Call service transfers a call on hold to an active call on the same device. The on-hold and active calls are merged into a new call. The behaviour is identical to a manual supervised or unsupervised transfer. An unsupervised transfer is accepted in the alerting or queued state. Calls to be transferred can be internal or external. On multiline devices, any call on hold can be transferred.

If the device is busy or on-hook/hands-free, the service sends an indication (display or audio) that a transfer has been performed. In order to do this, the system initiates a new temporary call which is automatically cleared after a time-out.

8.6.2.2 Private Services

The Escape service provides for the installation of private services not defined in the ECMA CSTA protocol. The following private services are available in the Alcatel-Lucent OmniPCX Office Communication Server CSTA through use of the Escape service.

8.6.2.2.1 Associate Data

The Associate Data service associates information (project code, authorization, code, etc.) with a specific call. The service does not affect the state or progress of the call.

8.6.2.2.2 BLF (Start/Stop/Snapshot)

The BLF (Busy Lamp Field) service allows an application to start or stop a BLF observation, and to request a BLF snapshot (basic occupation status, forward type, forward destination) for a device. A BLF observation reports the basic occupation status for all devices on the PCX that are monitored. The four possible basic occupation states are:

- device idle
- device busy
- device alerting/queued
- device out of service

Note:
The four basic occupation states are mutually exclusive.

8.6.2.2.3 Device Status

The Device Status service allows an application to:

- Start monitoring of the creation and deletion of devices in the PCX
- Stop monitoring
- Request the status of a device
- Request the status of all devices

Device status reports the following information: external directory number, physical device type, whether the device is in-service or out-of-service.

8.6.2.2.4 Dial Digits

The Dial Digits service allows a dialling sequence to be associated with a previously initiated call. The service is also used to perform dialling sequences for completing a multi-stage dialled call.

8.6.2.2.5 Get Config

The Get Config service returns information about the PCX configuration, including:

- PCX identification
- PCX major and minor software version
- CSTA major and minor software version
- Number of CSTA devices monitored on the PCX
- External directory number of the PCX Voice Mail

8.6.2.2.6 Get Name

The Get Name service returns the name of a device or all devices as they are defined in the system directory.

8.6.2.2.7 Pickup EDN

The Pickup EDN service picks-up a ringing or queued call on the device's External Directory Number (EDN). If there are several ringing or queued calls for the EDN, the PCX will choose the call to pick-up. The picked-up device does not need to be monitored.

8.6.2.2.8 Send DTMF Tones

The Send DTMF Tones service enables DTMF tones to be added after a call is connected. Allowed digits are: 0 1 2 3 4 5 6 7 8 9 A B C D # * , T t ;

8.6.2.2.9 Get Button Info

The Get Button Info service requests button information for one or all buttons on a device.

8.6.2.2.10 Set Lamp

The Set Lamp service specifies the state of a lamp associated with a button on a device. Sixteen states are possible.

8.6.3 CSTA Link

8.6.3.1 CSTA Link

To create the CSTA link, the CTI application host computer must connect to TCP port number 2555 of the Alcatel-Lucent OmniPCX Office Communication Server CSTA server.

Once this connection is made, the application identifies itself using the Association Control Service Element (ACSE) method, the OSI method for establishing a call between two application programs. In the association request, the CTI application specifies the list of CSTA versions supported and the list of CSTA services and events used.

The association can be rejected by the Alcatel-Lucent OmniPCX Office Communication Server CSTA server if the ACSE versions are incompatible, or no common CSTA version is available.

When the association is accepted, the Alcatel-Lucent OmniPCX Office Communication Server replies with the chosen CSTA version and the list of usable CSTA services and events.

The CTI application initiates a connection release by sending an association cancellation request. Once the PCX acknowledges, the CTI sends an EXIT message. Each side then releases the TCP connection.

8.6.3.2 Surveillance

A surveillance procedure is installed at the application level, to detect TCP link failures. This procedure enables the CTI application to detect a reboot of the PCX, and inform the client. This surveillance procedure has a faster reaction time than the default TCP mechanism.

If no message has been received from the CTI application for 30 seconds, the Alcatel-Lucent OmniPCX Office Communication Server CSTA server sends system status requests every 30 seconds. These requests must be acknowledged by the CTI application. The Alcatel-Lucent OmniPCX Office Communication Server CSTA server considers the link to be broken after two messages have been sent with no reply.

8.6.3.3 Recovery

The following describes the recovery procedures in the event of PCX reboot, link failure, or CTI

application computer reboot. In all cases, after the failure, the CTI application restarts the connection and monitoring.

- When the PCX reboots or loses the TCP connection, all calls are released. When the CTI application reconnects, the PCX sees this as a new session.
- When the TCP link fails, all monitoring requests are cleared.
- When the Alcatel-Lucent OmniPCX Office Communication Server CSTA server restarts (but the PCX does not reboot), all monitoring requests are cleared, but calls are not released. When the CTI application reconnects, the PCX sees this as a new session.
- When the CTI application computer reboots, the TCP connection is released, and so the monitoring data is cleared. There is no impact on calls. When the CTI application reconnects, the PCX sees this as a new session.

8.6.4 TAPI

8.6.4.1 Supported Environments

Third Party CTI connectivity relies on a server/client model:

- TAPI 2.0: The application developer has to program the link between client and server
- TAPI 2.1: Microsoft provides the link (via Microsoft Windows Remote Service Provider) between the client PC and a server PC (an NT 4.0 server belonging to the NT domain) that hosts the Third Party TAPI service provider.

The Alcatel-Lucent Third Party TAPI service provider is implemented like a CSTA and uses the Alcatel-Lucent OmniPCX Office Communication Server CSTA API.

Operating system	Microsoft TAPI version	Alcatel-Lucent TAPI Third party SPI	Notes
Windows 3.x	1.3 *	/	Not possible
Windows 95	2.1 *	5.0x	
Windows 98	2.1	5.0x	
Windows 98 Ed. 2	3.0	5.0x	
Windows Millennium	3.0	5.0x	
Windows NT 4.0 SP4	2.1 *	5.0x	TAPI 2.1 is included in SP4
Windows 2000 Prof.	3.0	5.0x	
Windows XP Prof.	3.0	5.0x	

* TAPI version not delivered with Operating System but can be downloaded from http://www.microsoft.com.

Applications available

- PIMphony Basic, PIMphony Pro, PIMphony Team, and PIMphony Operator, all capable of monitoring sets (analog, dedicated or cordless) and of acting as an IP phone.

Supported terminals

- All the terminals supported by CSTA.

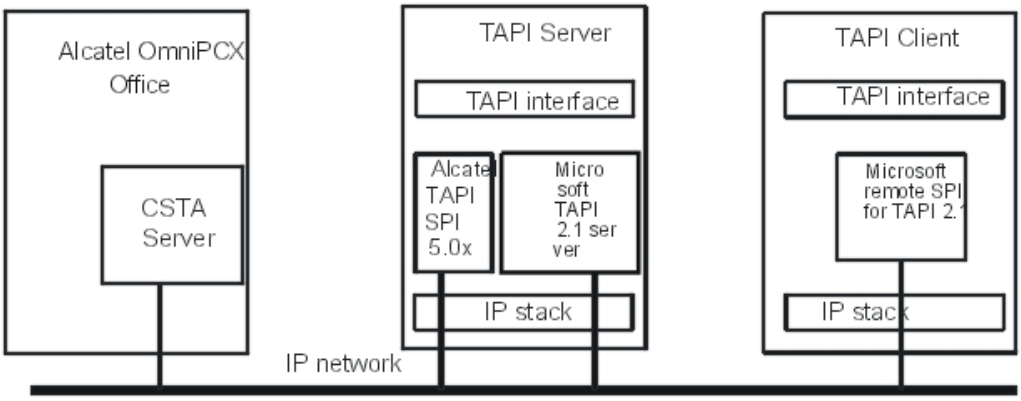
*8.6.4.2 **TAPI SERVER/CLIENT CONNECTIVITY***

Microsoft TAPI 2.1 server

Various architecture solutions are available:

This architecture requires:

- Microsoft remote service provider on the client PC
- Microsoft TAPI 2.1 server and Alcatel-Lucent TAPI SPI 5.0x on the server PC
- the CSTA server on Alcatel-Lucent OmniPCX Office Communication Server



Alcatel-Lucent TAPI Server

In this case no TAPI server is required: the CPU board acts as a TAPI server. As each Alcatel-Lucent TAPI SPI 5.0x requires a CSTA session, the number of clients is limited by the number of possible CSTA sessions.

Comparison between the 2 architectures

Service	Microsoft TAPI 2.1 server	Alcatel-Lucent TAPI Server
Constraints on the client PC	- TAPI 2.1 remote SPI must be installed - Must belong to an NT domain - User must log into the NT domain	- Must have TAPI 2.0 or later installed - Must have Alcatel-Lucent TAPI SPI 5.0x installed on each client
Constraints on server PC	- Must have TAPI 2.1 installed - Must be an NT 4.0 server - Must belong to an NT domain - Must have Alcatel-Lucent TAPI SPI 5.0x installed	No server PC
Security	Yes	No
Centralised management	Yes	No
Mandatory configuration	- Client PC must be configured as a client of the TAPI 2.1 server - Server PC must be configured as a TAPI 2.1 server - Alcatel-Lucent TAPI SPI 5.0x must be configured with the IP address of the Alcatel-Lucent OmniPCX Office Communication Server CPU board	Alcatel-Lucent TAPI SPI 5.0x must be configured with the IP address of the Alcatel-Lucent OmniPCX Office Communication Server CPU board
Number of client PCs	No limit (except server PC load)	Limited by number of CSTA sessions
Number of CSTA sessions used	1	Number of client PCs
Impacts on customer IT organization	Can be high	Very low
Cost	Can be expensive	Cheap

8.6.5 Virtual Terminals

8.6.5.1 Description

A virtual terminal does not physically exist, is not visible, and can only be managed from a CSTA application. Created using MMC-PC (Expert View), it is assigned an internal directory number and has the same characteristics as adedicated set.

A virtual terminal can receive internal and external calls. Incoming calls can be answered via CSTA service requests; outgoing calls are also made in response to a CSTA service request.

A virtual terminal can form part of hunt group or an attendant (operator) group.

Default parameter setting:

- intercom profile (one resource key for each network access)
- 2 RGM keys for local calls
- 1 dedicated key for outgoing calls

A virtual terminal can have a maximum of 104 keys.

8.6.5.2 Configuration

- To create virtual terminals, in OMC (Expert view):

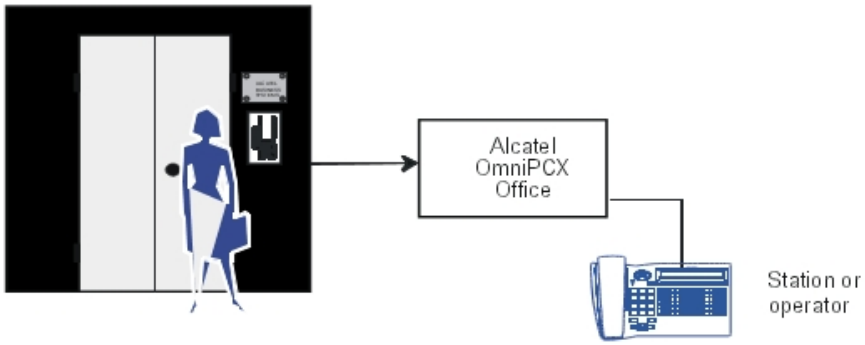
Users/Base Stations List -> **Users/Base Stations List** -> **Add** -> **Custom. Set: Add** -> **Virtual Terminals** -> specify the number of virtual terminals you want to create.

The system assigns the available directory numbers to the virtual terminals.
All the set parameters (accessible by **Users/Base Stations List** -> **Users/Base Stations List** -> **Details**), with the exception of the individual directories and passwords, can be modified.

8.7 Doorphones

8.7.1 Overview

With the doorphone, it is possible to identify the person who has pressed the button before opening the door. Identification is made after a call has been set up between a set connected to the system and the doorphone.



2 doorphone types are available, depending on the operating mode used:

- Type A: relay-controlled doorphones (e.g. NPTT)
- Type B: doorphones controlled by MF Q23 signals (e.g. TELEMINI and UNIVERSAL DOORPHONE)

These doorphones are mutually exclusive on the same system. **A flag must be placed to define the operating mode in use**.

By OMC (Expert View), select: **System Miscellaneous** -> **Memory Read/Write** -> **Misc. Labels** -> flag **DPHMode** -> enter 00 (default value) for a TELEMINI or UNIVERSAL DOORPHONE or 01 for an NPTT doorphone.

A doorphone call is managed in the same way as all internal calls:

- It is indicated on the destination set display as another call
- A doorphone call may be intercepted, forwarded, put in a conference with other individuals and camped on if the destination set is busy.

Note:

The destination of a doorphone call can be an external number (defined using a system speed dial number); in this case, the set in question cannot control the door opening operation.

8.7.2 Using a Telemini Doorphone

8.7.2.1 Operation

These doorphones must only be connected to an analog (Z) station interface.

Basic characteristics of these doorphones:

- Recognition of the opening and closing of the loop and passing into conversation.
- No detection of the ringing current (incoming call) except for those that are MF Q23 (DTMF) programmable.
- Recognition of MF Q23 (DTMF) signals or tones transmitted by the system (system -> doorphone dialog).
- Possibility of configuring a directory no. (programmed in the memory) transmitted to the system.

Several doorphones may be connected to the system; the limit is defined by the maximum number of analog set interfaces that the system can contain.

A system cannot have TELEMINI and UNIVERSAL doorphones at the same time.

8.7.2.1.1 Operating principle

Pressing the doorphone call button sends an MF code (START) which, after validation by the system, maintains the call and triggers an off-hook signal on the doorphone destination set or group.

There is a specific key for answering the call, while another controls the automatic doorstrike (latch) by sending an MF code (LOCK).

8.7.2.1.2 Hardware requirements

- a free Z device on an SLI board
- 2 free keys on one or morededicated sets
- a Telemini doorphone with doorstrike

8.7.2.1.3 Programming

- Defining the Z interface (for subscriber 111, for example).

By OMC (Expert View), select:
Users/Basestations List -> **Users/Basestations List** ->**111** -> **Details** -> **Misc.** -> **Special Function = Door Phone** -> **Hotline = Immediate** -> **destination n° = set or group Subscribers** -> **Subscriber** -> **111** -> **Details** -> **Features = protection against camp-on tone and intrusion (optional)**

- The feature access code for controlling the doorstrike

By OMC (Expert View), select:
Numbering -> **Features in Conversation** -> **XX = Doorphone Unlock**

- To create specific keys on the set(s) linked to the doorphone
  - Supervision keys

By OMC (Expert View), select:
Users/Basestations List -> **Users/Basestations List (select doorphone destination set)** -> **Details** -> **Keys** -> **select a key** -> **Type = Resource Key** -> **Function = RSL** -> **Number = 111**

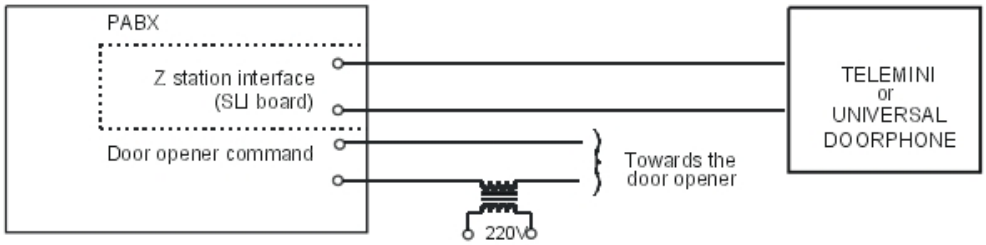
  - Doorstrike key

By OMC (Expert View), select:
Subscribers/Basestations List -> **Subscriber (select set)** -> **Details** -> **Keys** -> **select a key** -> **Type = Function Key** -> **Function = Doorphone Unlock**

- Specific programming instances
  If the doorphone uses other MF command codes, refer to its instructions.

By OMC (Expert View), select:
System Miscellaneous -> **Doorphone Signals** -> **change MF code values (start/stop signal)**, **if desired, add the ringing tone to the doorphone using Alert Signal / Tone**

8.7.2.1.4 Connection diagram



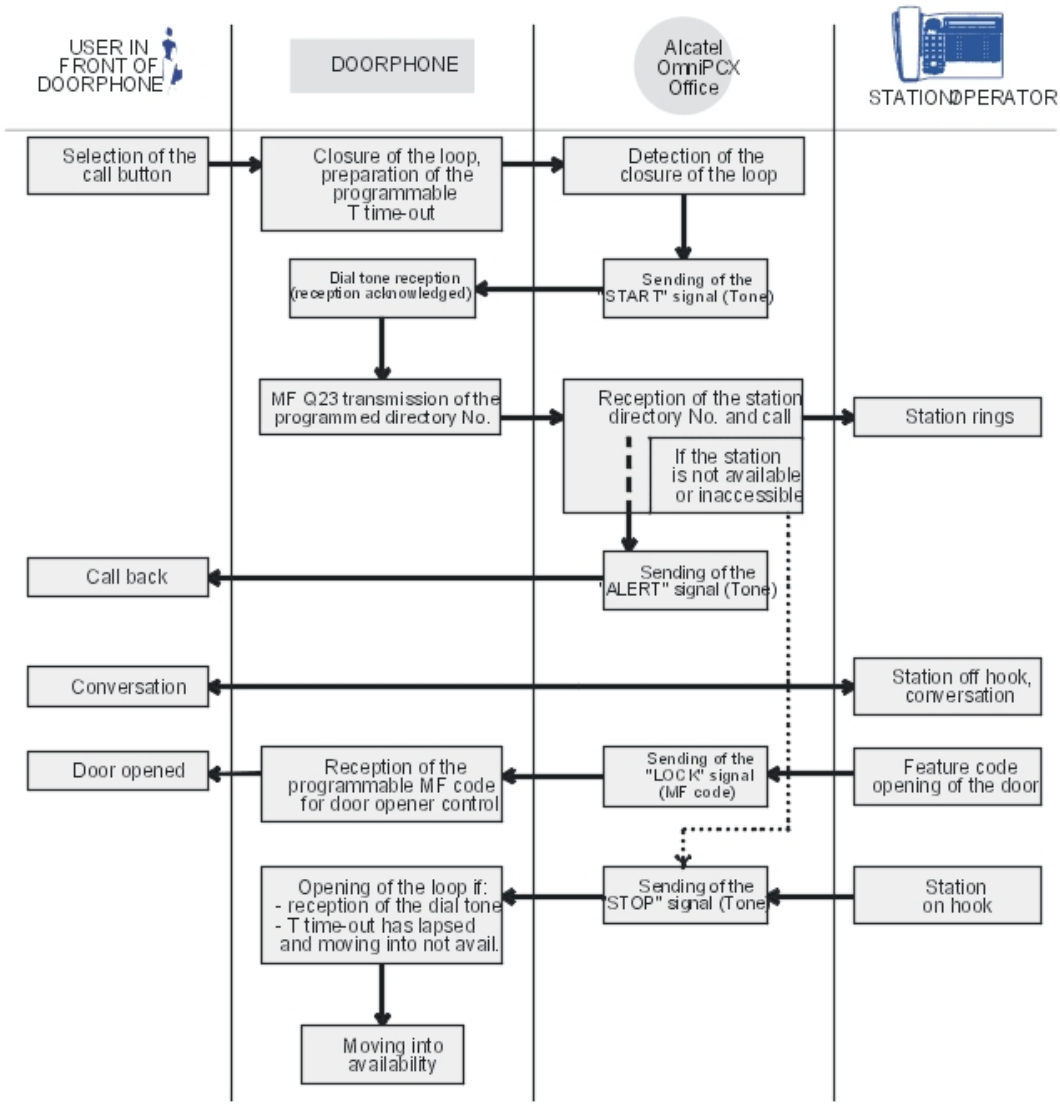
Functional description

Setting up a doorphone requires a functional analysis of the device (expected signals or tones, system open to programmable signals), before moving on to the system configuration, or that of the doorphone.

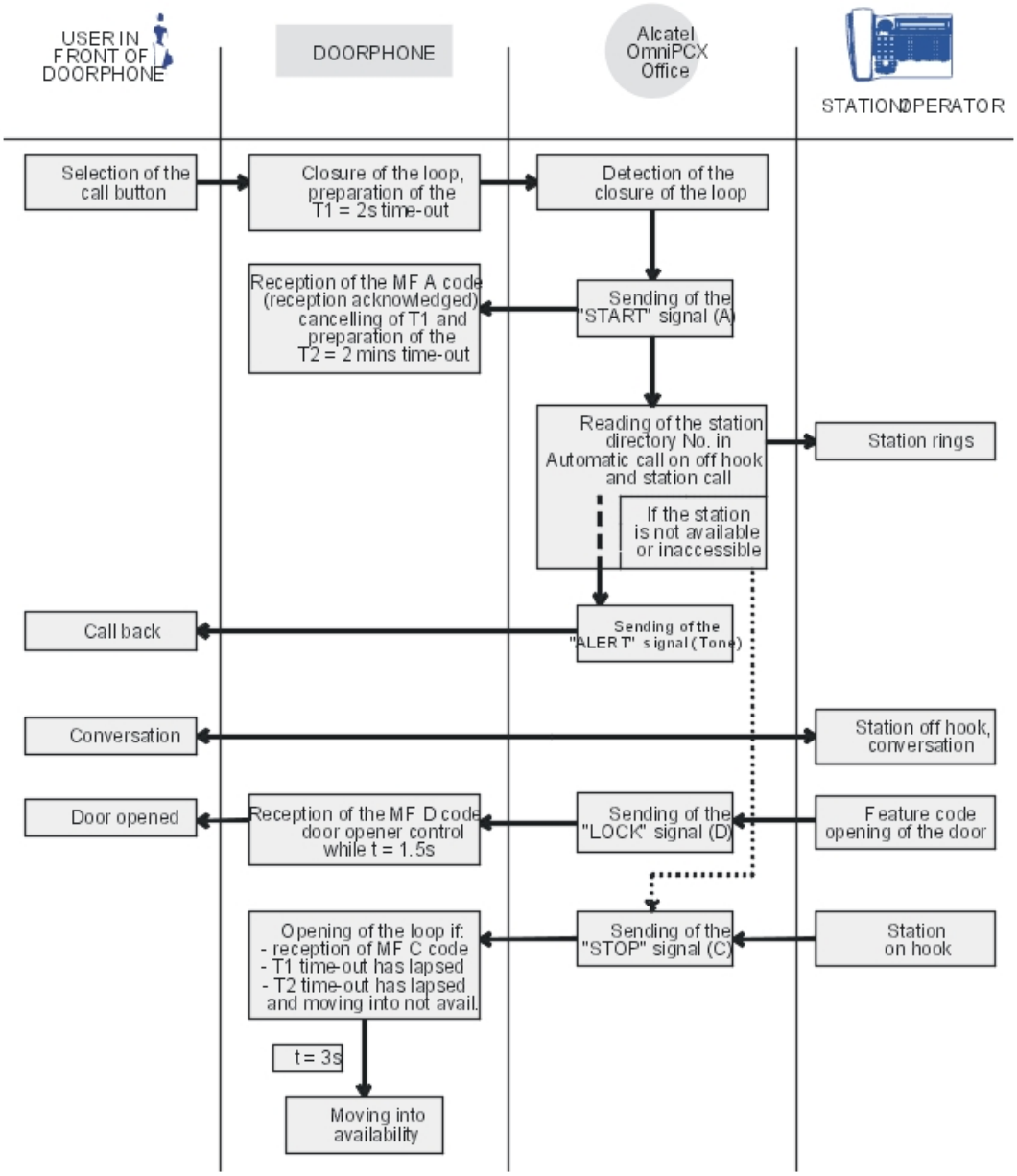
Note:

It is recommended that you consult the doorphone installation manual.

Functional analysis of the "UNIVERSAL DOORPHONE"



Functional analysis of the "TELEMINI" doorphone



8.7.3 Using a NPTT Doorphone

8.7.3.1 Operation

The doorphone interface comprises an intercom and an optional door strike that works in conjunction with an electrical supply provided through a suitable low voltage transformer, for example a SELV (Safety Extra Low Voltage) transformer.

A single doorphone with doorstrike may be connected to the system.

The system also allows for the connection of 2 doorphones without doorstrikes.

8.7.3.1.1 Operating principle

Pressing the doorphone call button triggers a loop on the associated Z terminal. The loop is maintained by relay 1 on the AFU board until the call is answered. The Z terminal is in immediate selection on the doorphone destination group or terminal.

There is a specific key for answering the call, while another controls the automatic doorstrike (latch) via relay 2 on the AFU board.

8.7.3.1.2 Hardware requirements

- An AFU board (a CPU daughter board)
- a free Z device on an SLI board
- 2 free keys on one or more dedicated sets
- An NPTT doorphone
- A doorstrike with transformer

8.7.3.1.3 Programming with OMC

- Set the flag "DPHMode" to 01.
  This flag, with a default value of 00, enables the Alcatel-Lucent OmniPCX Office Communication Server to manage the type of doorphone interface employed. Only the values 00 and 01 are currently used.

By PC- OMC (Expert View), select:
System Miscellaneous -> **Memory Read/Write** -> **Misc. Labels** -> **DPHMode** -> **Details** -> **01** -> **Modify** -> **Write**

- Defining the Z interface (for subscriber 111, for example).

By OMC (Expert View), select:
Users/Basestations List -> **Users/Basestations List** -> **111** -> **Details** -> **Misc.** -> **Special Function = Door Phone** -> **Hotline = Immediate** -> **destination n° = set or group Subscribers** -> **Subscriber** -> **111** -> **Details** -> **Features = protection against camp-on tone and intrusion (optional)**

- The feature access code for controlling the doorstrike

By OMC (Expert View), select:
Numbering -> **Features in Conversation** -> **XX = Doorphone Unlock**

- To create specific keys on the set(s) linked to the doorphone
  - Supervision keys

By OMC (Expert View), select:
Subscribers/Basestations List -> **Subscriber (select doorphone destination set)** -> **Details** -> **Keys** -> **select a key** -> **Type = Resource Key** -> **Function = RSL** -> **Number = 111**

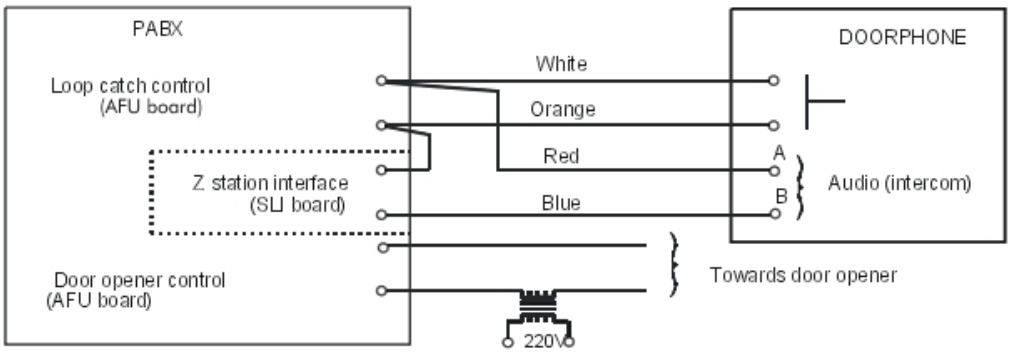
  - Doorstrike key

By OMC (Expert View), select:
Subscribers/Basestations List -> **Subscriber (select set)** -> **Details** -> **Keys** -> **select a key** -> **Type = Function Key** -> **Function = Doorphone Unlock**

- configuring the Auxiliaries board relays

By OMC (Expert View), select:
Hardware and Limits -> **Auxiliary Interfaces** -> **Doorphone 1**: **Hold Line = relay1 (maintain call)**, **Doorstrike = relay2 (open doorstrike)**, **N° = doorphone Z interface number (111)**

8.7.3.1.4 Connection diagram



8.8 Network Management Centre

8.8.1 Detailed description

The Alcatel-Lucent 4760 network Management Centre has been designed to enable telephone network managers to manage, administer and optimise one or several Alcatel-Lucent OmniPCX Office Communication Server communication systems remotely.

8.8.1.1 ENVIRONMENT

Connecting remote Alcatel-Lucent OmniPCX Office Communication Server systems (Management Centre subscribers)

All remote Alcatel-Lucent OmniPCX Office Communication Server subscribed systems managed by the same Management Centre are connected to the public network (PSTN or ISDN) through analog trunk lines or via T0 (2 B-channels), T2 or E1 accesses (30 B-channels).

Note:

ANALOG NMC:

The TL must be configured with Polarity Inversion (or Busy Tone Detection must be activated) to release the modem (the Management Centre being the master of the call).

Connecting the Management Centre

The Alcatel-Lucent 4760 station is connected to the Alcatel-Lucent OmniPCX Office Communication Server system by an Ethernet link (the client LAN, ISDN or V34 modem).

8.8.1.2 OMC CONFIGURATION AND IMPLEMENTATION

The **Network Management Control** option makes it possible to access the various configuration windows to set the network management parameters. To access the NMC home window from within the main menu:

Select the **Network Management Control** menu -> the following submenus are proposed:
- **Callback/Authorised Callers**
- **Centralised Management**
- **Select Urgent Alarms**
- **SNMP (Simple Network Management Protocol)**

Caution:

Programming the authorised callers also affects access to the system by NMC, as well as remote access by OMC.

CENTRALISED MANAGEMENT SUBMENU

Network Management Active

Check the box to activate the central management feature (this avoids starting up the management feature before the end of the system configuration). By default, the feature is inhibited.

General

Note 1:

All fields in the General section are automatically configured through 47xx.

Changing them does not make much sense. All values will be overwritten after the next 47xx synchronization.

- **NMC number for automatic alarms reporting (outside NMC session)**: contact number of the remote NMC to dial for automatic alarm reporting if no NMC session is in progress.
- **NMC Connectivity Mode:** this field defines the connectivity mode.
- **System Label:** this field, with a maximum of 30 characters, states the name of the remote system. The name is defined by the Management Centre; it cannot be modified by OMC (Expert View).

Note 2:

The fields which are not modifiable by OMC (Expert View) are defined either by the system or by the Management Centre; thus, as a minimum, an "online" connection to the remote system is required so that these fields can be used.

The Connection mode provides also an IP connection mode.

Call Accounting

- **Active call accounting for:** activation of the call accounting management according to the type of calls: The following choices are offered:
  - no call
  - incoming calls
  - outgoing calls
  - incoming and outgoing calls (default value)

- **Database threshold for alarm activation (%):** (by default: 80%) 100% = from 1,000 to 30,000 records, depending on the software licence and the hardware configuration. When the assigned threshold is reached, an alarm is sent to the Management Centre (on condition that automatic alarm reporting is activated and the "NMC_THRESHOLD_METERING_TBL" alarm is configured as urgent); the Management Centre reacts to the alarm and connects up to the remote system in order to collect and void the metering tickets.

Alarms Reporting(Only visible after clicking the **Part 2** button)

Alarms reporting enables the remote system to inform the Management Centre as soon as an abnormal event arises with the Alcatel-Lucent OmniPCX Office Communication Server.

- **Automatic alarms reporting:** check the box to activate automatic alarms reporting. By default, this feature is inhibited.
- **Reaction on erroneous call:** for example, the call number does not correspond to that of the Management Centre:
  - **Time before retry (min):** waiting time, in minutes, before trying again (value between 1 and 12 minutes inclusive, by default: 12 minutes)
  - **Max. number of call attempts:** maximum number of call backs (a single callback authorised)
- **Reaction on non-answered call:** for example, the Management Centre has not answered because all accesses are busy:
  - **Time before retry (min):** waiting time, in minutes, before trying again (value between 1 and 12 minutes inclusive, by default: 12 minutes)
  - **Max. number of retries:** maximum number of callbacks (value between 1 and 99, by default: 50)
- **Threshold for alarms reporting activation:** by default, when the threshold is reached, an alarm is sent to the Management Centre. This one is connected to the remote system automatically so as to deduct the alarm information:
  - **History table:** by default 80% (100% = 400 history messages)
  - **HW Anomalies table:** hardware messages, by default 80% (100% = 200 hardware messages)
  - **Urgent Alarms table:** by default 80% (100% = 200 urgent alarm messages)

SELECT URGENT ALARMS SUBMENU

This window makes it possible to define the urgent alarms for hardware anomalies as well as historic events.

Note 3:

The Urgent Alarm account and password are configured via 2 new fields: URGALARM account and URGALARM password.

Alarm password: Any alphanumeric character plus @ - _ + . /\ is allowed. (See default password)

Alarm user: If windows domain/user group must be defined, it must be under the form :"domain\\user". Any alphanumeric character plus @ - _ + . /\ is allowed.

Predefined urgent events in the Hardware Anomalies section

- PRINTING_ATTEMPT_FAULT: Message sent by the output device (printer) after every 5 failed print attempts.
- T2_NO_MULTIFRAME_FOUND: A signal shortage has been detected on a T2 access.

This alarm occurs after synchronisation is lost in multi-frame mode and after timer has expired. T2 automatically starts double-frame mode.

- T2_REMOTE_ALARM_INDICATION: A remote alarm indication has been received on a T2 access.

RECOMMENDATIONS FOR IMPLEMENTING THE NMC FEATURE (remote system)

The recommended procedure is the following:

- Activate network management (value deactivated by default or after a cold reset)
- Enter the remote system's complete configuration:
  - station number for alarm reporting
  - validation of the automatic alarm reporting feature
  - definition of the various thresholds
  - definition of the urgent alarms
  - etc.
- Activate the central management feature by checking the **Try to use active NMC session for alarms reporting** box in the **Centralised Management** window
- Perform a warm reset for table resizing
- Check that the call number has been programmed properly

Remark:

Transmissions of Internet alarms are integrated in the History messages window.

8.9 Point to Point/Point to Multipoint T0

8.9.1 Detailed description

8.9.1.1 DEFINITIONS

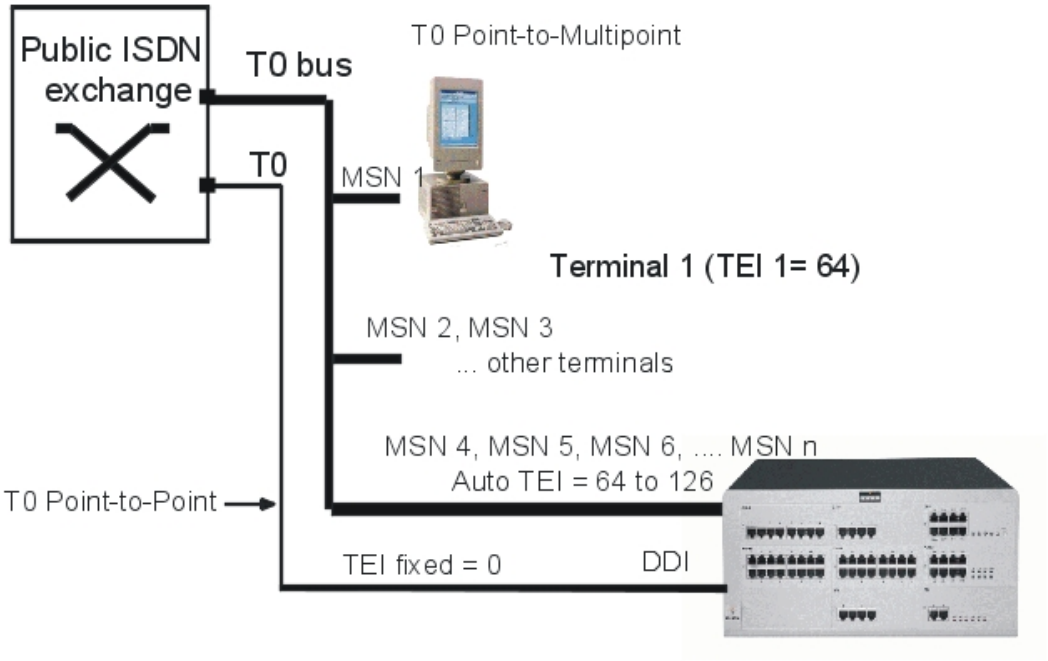
Point-to-Point link: a Point-to-Point link is a digital access to the public network used exclusively by Alcatel-Lucent OmniPCX Office Communication Server. The TEI settings are generally fixed, as there is only one terminal (Alcatel-Lucent OmniPCX Office Communication Server) for this access, but they can also be dynamic.

Point-to-Multipoint link: a Point-to-Multipoint link is a digital access to the public network shared by several terminals. In this type of configuration, each terminal is identified by its TEI and dedicated DID sequence. The TEI management mode can be fixed or dynamic, depending on the public carrier.

Both types of link can be supported simultaneously on the same system. The TEI management mode (fixed or automatic) is configured separately for each access.

8.9.1.1.1 Example of the environment

This example illustrates both connection types: Point-to-Point and Point-to-Multipoint.



8.9.1.2 DYNAMIC TEI

This feature assigns a TEI automatically to each T0 bus (mainly assured by the public network on multipoint accesses).

At each connection and at each reset, (cold or warm), each T0 "asks" the network to assign it a TEI; this procedure is performed by sending 2 level 2 messages: the "Identity Request" message sent by the system to the network, then the "Identity Assigned" message sent by the network. The value assigned is stored by the system until the next reset.

Possible TEI values (in accordance with ETS300 125)

- 0 to 63: fixed TEIs (values used on the system side)
- 64 to 126: automatic TEIs (values used on the network carrier side)
- 127: value reserved for management operations

When changing from a digital access with fixed TEI management to automatic TEI management, it is essential to perform a warm reset so that the Alcatel-Lucent OmniPCX Office Communication Server sends the TEI allocation request to the public exchange; if not, the TEI management on the system will be unstable.

8.9.1.3 CONFIGURATION

8.9.1.3.1 T0 configured in Point-to-Point

- To define the management mode:

By OMC (Expert View), select: **External Lines** -> **List of Accesses** -> **Details** -> check **? Fixed TEI** or **? Auto TEI**

- For fixed TEI, assign a value between 0 and 63 inclusive:

By OMC (Expert View), select: **External Lines** -> **List of Accesses** -> **Details** -> **Value**

- Configuring the installation number:

- by OMC (Expert View): **Numbering -> Installation Number**
- by MMC-Station: **Global -> Ins Num -> Public**

- Completing the substitution table (refer to the file concerning DID with more than 4 digits in the "System Features" section):

- by OMC (Expert View): **Dialling -> DID Number Modification Table**
- by MMC-Station: **Num Pln -> PubNMT**

- Fill in the public numbering plan:

- by OMC (Expert View): **Dialling -> Dialling Plans -> Public Dialling Plan**
- by MMC-Station: **NumPln -> PubNum**

8.9.1.3.2 T0 configured in Point-to-Multipoint

- To configure the T0 access in Point-to-Multipoint:

By OMC (Expert View), select: **External Lines** -> **List of Accesses** -> **Details** -> select **? Point to Multipoint**

- To define the management mode:

By OMC (Expert View), select: **External Lines** -> **List of Accesses** -> **Details** -> select **? Fixed TEI or ? Auto TEI**

- For fixed TEI, assign a value between 0 and 63 inclusive:

By OMC (Expert View), select: **External Lines** -> **List of Accesses** -> **Details** -> **Value**

- Configuring the installation number:

- by OMC (Expert View): **Numbering -> Installation Number**
- by MMC-Station: **Global -> Ins Num -> Public**

- Completing the substitution table (refer to the file concerning DID with more than 4 digits in the "System Features" section):

- by OMC (Expert View): **Dialling -> DID Number Modification Table**
- by MMC-Station: **Num Pln -> PubNMT**

- Fill in the public numbering plan:

- by OMC (Expert View): **Dialling -> Dialling Plans -> Public Dialling Plan**
- by MMC-Station: **NumPln -> PubNum**

8.9.1.4 ADDITIONAL INFORMATION

- By default, the T0 accesses are in Point- to-Point with automatic TEI management for all countries.
- Once the system has been configured for automatic TEI and reset, the automatic TEI request is sent to the network. If there is no reply before the T202 timeout, the system switches back to fixed TEI mode; otherwise, it stays in automatic TEI mode.

8.10 Permanent Logical Link

8.10.1 Detailed description

The Permanent Logical Link (PLL) service handles the simultaneous bi-directional transfer of data frames between a T interface (T0 or T2) and an S0 interface (ePLL) or between 2 S0 interfaces (iPLL), each interface being one extremity of a semi-PLL with:

- either a public network Packet Access Point (PAP) on the T interface side
- or an S0 terminal connected to the S0 bus on the S0 interface side.

The data packets are exchanged on this link in a transparent way through the D channels of these accesses.

The rate for this type of data transmission is limited to 9600 bps.

The link between the 2 Alcatel-Lucent OmniPCX Office Communication Server interfaces that connect the 2 semi-PLLs is established by configuring a routing table.

The S0 terminals are connected to 4084 or 4094 interfaces.

8.10.1.1 DEFINITIONS

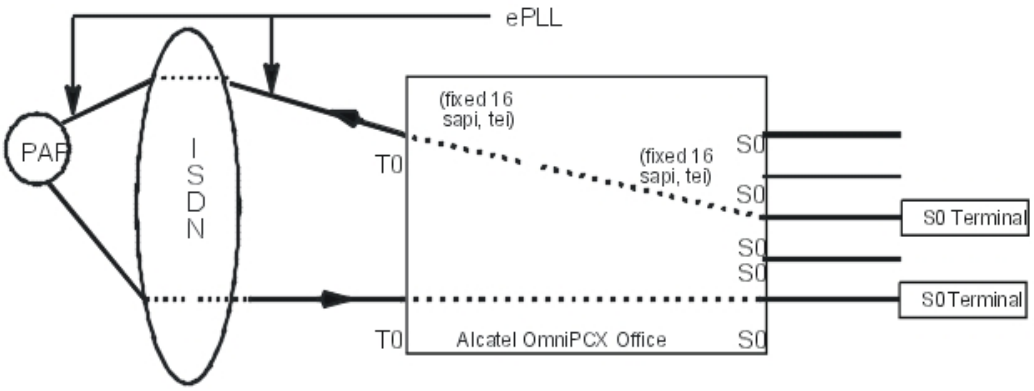
- SAPI: Service Access Point Identification; the value in the SAPI field identifies the type of information transported by the data link and, for this reason, identifies the targeted access point, source or frame destination. By default, a SAPI value of 16 is assigned to links carrying X25 type packets to the PAP.
- TEI: Terminal Extremity Identification

8.10.1.2 EXTERNAL PLLs

The system makes it possible to establish one or several external PLLs (ePLLs) between T accesses of the system and a data network access port and also to extend them to S0 accesses according to the following rules:

- each ePLL associates the trinome [Interface T, SAPI (16), TEI] with an [Interface S0, SAPI (16), TEI] trinome.
- a T or S0 interface can be used for several ePLLs (max. 4) by changing the TEI value.

General summary of an external PLL

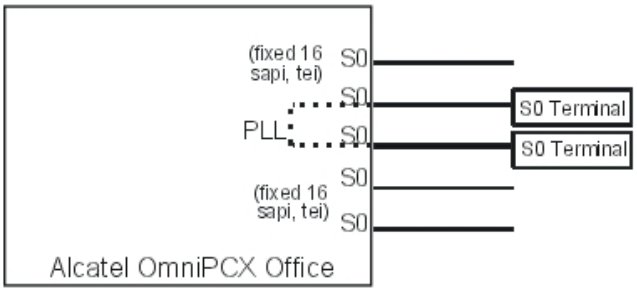


8.10.1.3 INTERNAL PLLs

The system makes it possible to establish one or several internal PLLs. The following rules apply to internal PLLs (iPLLs):

- each iPLL associates the trinome [Interface S0, SAPI (16), TEI] with an [Interface S0, SAPI (16), TEI] trinome.

General summary of an internal PLL



8.10.1.4 CONFIGURATION

Preliminary

Before configuring the PLL, the installer must:

- Define the S0 and T0 accesses.
- Check that the interfaces to be used are present in the "Subscribers/Basestations List" screen (for S0 interfaces) and the "External Lines" screens (for T interfaces).

Creating a PLL

- by OMC (Expert View), select: **Subscribers Misc.** -> **Permanent Logical Link**

To create a PLL, proceed as follows:

- Select the PLL caller from the list of declared accesses presented in the left-hand part of the window.

- Enter the TEI of the caller PLL (SAPI = 16 is displayed, this value is not modifiable):
  - For an external access, the TEI is provided on subscription by the public network carrier and is between 0 and 63 inclusive.
  - For an internal access, the TEI is between 1 and 63 inclusive (depending on the configuration of the terminals).
- Select the PLL destination from the list of declared accesses presented in the right-hand part of the window.
- Enter the TEI of the destination PLL (follow the same procedure as for the TEI of the caller PLL)
- Click **Add** to establish the connection. If all the checks are OK (see below), the connections are added to the list of existing PLLs.

Checks

- The system can contain a maximum of 32 PLLs.
- The system cannot contain PLLs between 2 external accesses.
- The caller and the destination of the same PLL cannot be one and the same (same physical address and same TEI).
- 4 TEIs per basic access (S0/T0), 16 per primary access (T2); 2 PLLs associated with different accesses can have the same TEI (there is no check at OMC level).

Overflow

It is possible to overflow onto a second destination if the initial destination is busy by configuring the same caller with 2 different called parties.

Note:

Once declared, an ePLL or iPLL is bi-directional, i.e. either interface can initiate a call.

8.11 Multiple Automated Attendant

8.11.1 Overview

8.11.1.1 Description

The Multiple Automated Attendant is a software module used to create sets of multiple, tree-structured voice guides. One such voice guide can give a caller a choice between 4 different languages for messages.

The Multiple Automated Attendant also provides the following features (from Alcatel-Lucent OmniPCX Office Communication Server R6.0):

- Multiple language menus proposing action choices to callers
- Identification (DDI/CLIR) of the call and subsequent routing to attendant groups
- Error management when a caller fails to respond to a voice prompt
- Programming of time ranges
- Upload (to the call server) of locally created tree-structures
- Configuration of media ports using OMC

- Management of audio files using OMC

Voice guides indicate how to access other selection options or final destinations, which can be:

- Hunting groups
- Voice mailboxes. All of the following options are available:
  - General voice box (VMU) of the group in consultation (if available on the set)
  - Transfer to a group/user voice mailbox with recording a message as an option (maximum length: 30 seconds)
  - Free dialling to any voice mailbox (only via menu action)
- Subscribers
- Attendants
- Active MeetMe/Join MeetMe
- Collective Speed Dialling

  Note 1:
  The Collective Speed Dialling numbers are not listed in the picklist but they can be configured manually.

Note 2:
When a call is transferred to ACD, Calling Line Identification information is included in the transfer.

8.11.1.2 Additional Information

Licence types

- The maximum number of voice guides that can be created depends on the licence type:
  - I tree
  - 5 trees

Media ports

- The maximum number of calls that the ACD/MLAA engine can manage at a time equals the number of media ports dedicated to each feature (MLAA and ACD).
- The maximum number of VTM available to MLAA and ACD at the same time is 16.

Voice messages

- The maximum number of available MLAA voice messages that can exist in the system at the same time depends on the number of checked languages. 100 audio files (in .wav format) per language gives a maximum of 400 messages, including the welcome or greeting message. Maximum duration of each message is 30 seconds.
- To increase the duration of a voice message, modify the "**MLAA_MSG**" noteworthy address value - OMC (Expert View) only:

System Miscellaneous > **Memory Read/Write** > **Other Labels** >**MLAA_MSG** > **Details**

Languages

- The maximum number of languages that can be used in one and a same tree structure MLAA is 4.

8.11.2 Activation/Use

Use OMC to:

- Configure MLAA dedicated media ports and DDI numbers to route to MLAA hunting groups (MLAA Setup window)
- Manage audio files (up/downloading, deletion) MLAA Voice messages window). Creating your own voice messages can be done on a system, external to the OMC, which can handle the wav format. It is also possible to record voice messages on telephone handsets of the type 4038 IP Touch, 4068 IP Touch, or 4035 (Advanced)
- Launch the Multiple Automated Attendant application GUI (MLAA Services window).

Use the MLAA GUI to

- Create voice guide tree-structures.

8.11.2.1 MLAA Setup Documentation

For information and details about MLAA setup and voice message management, refer to the OMC on-line help, chapter Multiple Automated Attendant.

8.11.2.2 MLAA GUI Documentation

For user information about the MLAA graphic user interface, refer to the MLAA on-line help. It is available from the MLAA application. Once the MLAA application is installed, select the Help menu/ press the "F1" key to open the MLAA on line help.

Chapter 9

Internet Services

9.1 General Presentation

9.1.1 Overview

Web-Based Tool is a monitoring tool that offers a means to observe the OmniPCX Office through Internet.

Web-Based Tool is located within OmniPCX Office and can be reached by simple remote Web browsers.

It does not require any installation or specific program on the Client side and is available on any OmniPCX Office model.

You can access Web-Based Tool at the following URLs: **https://IP_address/services/webapp/** or **https://host_name/services/webapp/** with the following Web browsers: Internet Explorer, Mozilla and Mozilla Firefox.

2 classes of clients may be connected to OmniPCX Office.

These clients get different services according to their roles.

- Users (login name: operator)
- Managers (login name: installer)

9.1.1.1 SERVICES PROVIDED

Service	Details	Operator	Installer
MOH upload	Load audio files for the Music On Hold feature	X	
System Start	Display System Start log file		X
Data Saving	Display Data Saving log file		X
Swap Serial	Select application connected to CPU config socket		X
General Information	Show CPU hardware equipment and state, memory use and software version		X
Cabinet Topology	Show hardware equipment of cabinets		X
Boot Information	Show the order in which boot devices are tried		X
Disk Smart Fs&disks	Display hard disk smart information Display mount table and partition table		X

Service	Details	Operator	Installer
System files	Give read access to log files in /current /boot and /current /debug directories, to current and alternate configrc files. Give read access to all file system including /proc		X
Net Configuration	Display net devices, routing table and cached routing table		X
Dump System	Display in a typewriter format a summary of system state Download debug and log files Display proc file system in a typewriter format		X
Memory Info	Display the contents of /proc/meminfo		X
Traces&Debug	Give read access to WLAN and NMC log files, allow trace activation and collection on T1		X

9.1.1.2 ARCHITECTURE

9.1.1.2.1 Type of configuration

Web-Based Tool is a client-server architecture that uses the HTTPS communication protocol. The client is a browser and the server is embedded in OmniPCX Office.

There are 3 types of configuration according to the access path:

- LAN
- Remote Access Server (management)
- WAN

LAN access

The computer running the client browser is connected to the same LAN as OmniPCX Office.

Remote Access Server (management)

The remote user is connected to the OmniPCX Office Remote Access Server (RAS) board through ISDN.

The RAS board routes the packets to WBT through the LAN.

WAN access

The remote user connects to the Internet and reaches OmniPCX Office on its WAN access (through VPN or not).

The HTTPS port must be open on the WAN. This is possible through the Internet Access Web-Based Management feature of OmniPCX Office.

9.1.1.3 DESCRIPTION

9.1.1.3.1 Function specifications

Web-Based Tool is only available in English.

Operator session

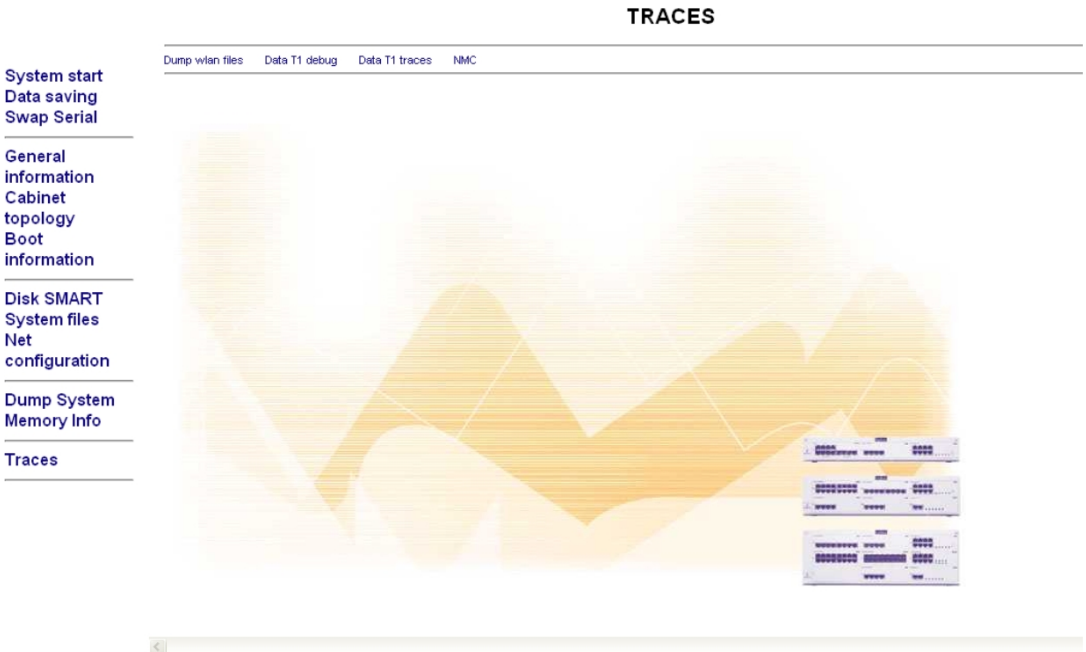
- Enter the audio file name in the **File** box or browse your system to find it.
- Click the **Submit** button.

Installer session

Click any of the items in the menu on the left to access the corresponding pages.

The pages that show up are self-explanatory.

Traces



The **Traces** page opens a submenu with the following items:

- **Dump wlan files**: To display the WLAN log files that store up to 4500 events that occurred on the Mobile IP Touch and WLAN access points.
- **Data T1 debug**
- **Data T1 traces**
- **NMC**: is the Alcatel-Lucent Network Management Centre which enables a telephone network manager to manage, administer and optimize one or several Alcatel-Lucent 4200 communication system from a remote site.
  The NMC submenu offers a means to activate/deactivate the monitoring of the OmniPCX Office embedded NMC server and to display the corresponding traces.

9.1.1.4 INTERACTIONS

Web-Based Tool is accessed through the Secure Application Server (SAS). SAS provides HTTPS access and centralized authentication.

9.1.1.5 MAINTENANCE PROCEDURES

9.1.1.5.1 Incident

The server may send error messages in HTTP packets; the Web browser displays these messages.

9.1.2 Services provided

The services available with Alcatel-Lucent OmniPCX Office Communication Server Internet access depend on the hardware and software keys purchased.

The following services are available:

- **Internet Access**: the system offers several possibilities for connecting to the Internet Service Provider (ISP):
  - **Connection on demand:** connection to the ISP is established on the basis of user demand (Internet access, sending e-mails, etc.) and cut off when there is no more traffic. The bitrate options are: static (64 Kbps, 128 Kbps) or dynamic (bandwidth on demand from 64 to 128 Kbps) in the case of ISDN. For ADSL, the bitrates are different and vary according to the IAP.
  - **Connection on demand with callback:** the IAP sends a signal to Alcatel-Lucent OmniPCX Office Communication Server that establishes the connection by return. This mechanism is validated using the ISDN caller ID: only authorized caller numbers can be called back. This type of connection must be used when implementing VPN services on an ISDN link (see the "VPN" section for more details).
  - **Always-on connection:** a permanent link to the ISP.

  The authentication protocols used are PAP/CHAP (ISDN and DSL Modem/Cable Modem). In the case of the External Router, if Alcatel-Lucent OmniPCX Office Communication Server does not communicate directly with the IAP.
- **Connection protocol**:
  - ISDN: MPPP, PPP
  - DSL modem: PPTP or PPPoE or IP over Ethernet

  - Cable Modem: PPTP or PPPoE or IP over Ethernet
  - External router: OmniPCX Office communicates with the IAP via the external router. The protocol used depends on the external router.
- **LAN Functions**: DNS server and DHCP integrated, as well as the routing table.
- **NAT**: address translation is used to internally store private IP addresses and to use only one public address.
- **Protection by integrated firewall**: the integrated packet filtering and IP address translation functions offer protection to the LAN against the Internet.
- **Antivirus**: the anti-virus software protects the electronic messaging as well as the HTTP and FTP flows. This software is hosted on a server connected to the same LAN as Alcatel-Lucent OmniPCX Office Communication Server.
- **Access control**: Alcatel-Lucent OmniPCX Office Communication Server offers control solutions for user access by integrated proxy. In addition to controlling web access, it generates the associated statistics (users, protocols, URLs, etc).
- **Integrated cache**: this function speeds up Internet requests, thereby reducing the cost of access to the telephone network.
- **E-mail server**: enables users to have a personal e-mail address within the company. You can create as many e-mail accounts as required, within the limits of the system itself, while optimizing the corresponding Internet traffic. Depending on the IAP, the e-mail reception protocols are as follows:
  - SMTP
  - POP3
- **VPN**: this solution authorizes secure connections to the LAN via the Internet infrastructure. This means distant users can benefit from all the resources on the LAN. Each VPN can manage accommodate several remote sites. The existing possibilities are:
  - Remote access to the LAN via Internet ("Client to LAN" configuration, PPTP protocol and IPsec)
  - Access between two LAN ("LAN to LAN" configuration, IPSec protocol)
- **Dynamic DNS**: it enables the automatic update of a domain name and a machine name when the IAP assigns a new IP Address. This service is in particular used in the event of a permanent connection (DSL Modem), to connect a remote worker to a machine with a dynamic IP Address. The update of the association table Domain Name/IP Address is handled by an ASP.
  Alcatel-Lucent does not provide the list of supported ASP's. The client must contact the installer to use this functionality.
- **Web Communication Assistant**: a Web application designed for Alcatel-Lucent OmniPCX Office Communication Server end users to help them manage in-house corporate communication (e-mails and voice messages).

All these services are configured via a secure Web interface; Web-based Management (WBM). For more information about WBM, refer to the "Web Based Management" section.

9.2 Web-Based Management

9.2.1 Overview

Web-Based Management (WBM) is an Alcatel-Lucent OmniPCX Office Communication Server Internet service administration tool.

The WBM operates with Internet Explorer (release 6 or later), Mozilla (release 1.7 or later), or Mozilla Firefox (release 1.1 or later). It uses a secure Web interface. The secure transfer protocol, HTTPS, ensures the identification of the transmitter and the receiver, the integrity and the privacy of the exchanged data.

WBM can be used directly via the LAN, or remotely from the WAN if this option is enabled.

WBM is an intuitive interface which simplifies navigation of the product functions. Depending on the selected software keys, one of the following two menus is available:

- a reduced menu. This menu is available when only the RAS software key has been chosen.
- a complete menu. This menu gives access to all the Alcatel-Lucent OmniPCX Office Communication Server Internet services.

This section deals successively with the administration levels, the presentation of the interface and connecting to WBM.

9.2.1.1 ADMINISTRATION LEVELS

The WBM has two administration levels:

1. **Administrator level**
   The administrator configures all the Alcatel-Lucent OmniPCX Office Communication Server Internet services.
   To use the WBM at administrator level, you must log on using:
   - either a user account belonging to a group that has administrator rights.
   - or the default "admin" account.
2. **Operator level**
   To facilitate Alcatel-Lucent OmniPCX Office Communication Server administration and enable administrators to delegate certain tasks, the WBM can be administrated by a local administrator called an operator.

   Remark 1:
   the operator administration level is not available for the reduced menu.
   To use the WBM at operator level, you must log on using:
   - either a user account belonging to a group that has operator rights.
   - or the default "operator" account.

   Remark 2:
   the operator has limited rights.

9.2.2 Operator Tasks

9.2.2.1 Overview

The main tasks are:

- User management.
- Supervision of system information and statistics.
- Configuration of time ranges and the voice mail, as well as backup management.

The following table lists all the Alcatel-Lucent OmniPCX Office Communication Server Internet services. For each service, it indicates whether or not the operator is authorized to configure the associated tasks via the WBM.

TASKS		OPERATOR
Access to the Welcome Page		Authorised
Users and users" groups		
Creating users		Authorised
Changing a user's properties,		Authorised
Deleting one or more users		Authorised
Transferring a user to a group without administrator rights		Authorised
Transferring a user to a group with administrator rights		Not allowed
Creating an operator		Authorised
Changing properties of other operators		Authorised
Deleting one or more other operators		Authorised
Changing the group of another operator		Authorised
Creating, changing and deleting an administrator		Not allowed
Changing an administrator's group		Not allowed
Creating and managing a group of users		Not allowed
Changing the properties of a group of users		Not allowed
Creating, modifying and deleting a group of users		Not allowed
Intranet		
Configuration of the intranet is not authorized		
Internet Access		
Configuration of Internet access is not authorized		
E-mail		
E-mail server configuration		Not allowed
Distribution list management		
	Adding a new mailing list	Authorised
	Deleting one or more mailing lists	Authorised
	Changing the properties of a mailing list	Authorised
E-mail server functioning test		Not allowed
Making Internet access secure		
Managing firewall rules		Not allowed
Controlling Internet use		
Configuring the proxy		Not allowed
URL filters management		Not allowed
Time ranges management		

	Changing the properties of the global time range	Authorised
	Changing the properties of existing time ranges	Authorised
	Adding a time range	Not allowed
	Deleting a time range	Not allowed
VPN		
VPN configuration is not authorized		
Anti-virus		
Anti-virus configuration is not authorized		
Security		
Changing the operator password		Authorised
Changing the administrator password		Not allowed
Administration		
Access to the dashboard		Authorised
Backup Management		
	Backup management (program or delete a back and perform a manual backup)	Authorised
	Configuration of the backup system.	Not allowed
	Restoring a backup	Not allowed
Test management		Not allowed
Access to general information (software key, hardware component, configuration file and drivers)		Not allowed

9.2.3 Interface

9.2.3.1 Basic description

The main characteristics of the interface are:

- The use of hyperlinks, tables, buttons and wizards,
- direct access to a contextual online help,
- verification of information prior to validation,
- the possibility of choosing the display language (French, English, German, Italian, Spanish, Portuguese or Dutch). The language is configured in the Web navigator.

9.2.3.1.1 The screens

The WBM interface contains three screen types:

1. **The wizard screens**
   They allow rapid simple configuration of the Internet services. The administrator can access the following wizards:
   - Connection
   - User
   - ACD

- E-mail
- VPN Tunnel
- VPN Customer
- Backup
- Anti-virus
- RAS

Remark:
the operator can only access the User wizard.

2. **the administration screens**
These screens are accessed by clicking on the corresponding hypertext link in the navigation bar. The administration screens give access to the lists of:
   - Users per group
   - Connection profiles
   - Time Ranges
   - URL filter
   - Mailing lists
   - Teleworker and VPN services
   - Certificates and revocation lists
   - Firewall rules
   - Backups performed
   - System information
   - Test tools
   - Software keys

   From the administration screens you can access the configuration screens.
3. **the configuration screens.**
The following screens are associated with the administration screens: Users, User Groups, Connection Profile, Time Range, URL Filter, Firewall Rule and Mailing List.
The following screens are used to directly configure the associated features:
   - Proxy
   - E-mail
   - RAS
   - Network
   - Firewall
   - Backup
   - Anti-virus

9.2.3.1.2 Description of the configuration and administration screens

The configuration and administration screens are divided into four areas:

1. **The general information banner**
It is made up of the current configuration title and the other configurations that can be accessed from this page.
2. **The navigation bar**
It is divided into sub-sections each representing a characteristic of Alcatel-Lucent OmniPCX Office Communication Server. Click on one of the menu options to get to the

appropriate configuration screen.

3. **The online help**
   Online help can be accessed directly on the right-hand side of each screen.
4. **The screen body**
   The screens may be a single area or offer several tabs. Click on a tab to display its content. If all the tabs cannot be displayed on the same screen, navigation arrows can be used to move from one tab to another. Various windows can be accessed by clicking on the hyperlinks on any given page.

9.2.3.1.3 Some common actions

The following actions are common to all the screens.

To delete or move several elements in a list, use the check boxes to the left of the elements and click on the **Delete selection** or **Move selection** button (in the middle of the screen).

To delete or add only the element corresponding to the line, click on the hypertext link **Add** or **Delete**.

9.2.4 Connection

9.2.4.1 Operation

For an administrator or operator, the procedure for connecting to the WBM is as follows:

1. Open the Web navigator.
2. Enter the following address in the **Address** field of the Web navigator:
   https://<Alcatel-Lucent OmniPCX Office Communication Server>/admin
   where *<Alcatel-Lucent OmniPCX Office Communication Server>*is the machine's IP address or name.
   You go to the **Web-Based Management - Authentication** page.
3. In the **Administrator/operator authentication** area, type in either:
   - A user name belonging to a group that has administrator rights or "admin", followed by the associated password.
   - A user name belonging to a group that had operator rights or "operator" followed by the associated password.
4. Click on **Connect**. Your service connection is established.
   Depending on your profile (administrator or operator), the **WBM Administrator Home Page** or the **WBM Operator Home Page** is displayed directly. It presents a summary of the system's activity.

9.2.4.1.1 How to disconnect

To disconnect, click on**Disconnect** in the navigation bar. Your connection has been deactivated.

Remark:

after 30 minutes of inactivity, disconnection is automatic.

9.2.5 Users and User Groups

9.2.5.1 Overview

9.2.5.1.1 WHAT IS A USER?

In Alcatel-Lucent OmniPCX Office Communication Server, a user is defined by a username and its associated password. The username and password are the user's ID card, which will be asked for in the following circumstances:

- By the e-mail server, in order to enable the user to collect mail from his local mailbox;
- By the proxy, if configured to require authentication (see Proxy chapter), in order to clear the user for Internet access;
- By the PPTP server, if the user wants to access the local network via the Internet (see VPN chapter);
- For the VPN IPsec clients PPTP and IPsec on L2TP access.
- For access to the file server.
- For Intranet publication (web server).
- To access the WBM configuration tool.
- To use the Web Communication Assistant.

9.2.5.1.2 WHAT IS A USER GROUP?

In Alcatel-Lucent OmniPCX Office Communication Server, each user is associated to a group. A profile is defined for each group. A profile is a set of privileges attributed to a group of users. The administrator may modify privileges at any time.

There is no limit to the number of groups that an administrator can create. However, in order to simplify the configuration and optimize the time, the following groups are predefined:

- administrators,
- operators,
- remote workers,
- unlimited accesses,
- professional accesses,
- free time accesses,
- without Web access.

9.2.6 Configuring Users and User Groups

9.2.6.1 Configuration procedure

The configuration of users and user groups involves two main tasks:

- Creating users.
- creating user groups

9.2.6.1.1 CREATING A USER

Click **Wizards** in the navigation bar. The wizards icons appear.

1. Click the **User's Assistant** icon. The **User Wizard** window displays.

2. The following field must be filled in:
   - **First name**: The user's first name (optional).
   - **Name**: The user's last name.
   - **User name**: this field is completed automatically. The user name takes the form *First Name.Surname*. The user uses this name to log on to the Web Communication Assistant. This name is also used to create the user's e-mail address.
   - **Password**: User password

     Remark 1:
     passwords must comply with the following rules:
     - comprise 6 to 8 characters
     - comprise at least one upper-case letter
     - comprise at least one non alphanumeric character
   - **Confirm password**
3. Click **Next**. A new window appears.
4. In the drop-down list, select the group where you want to associate the new user.
5. Click **Next**. The **License allocation** window appears.
6. Select **Yes** from the **Web Communication Assistant** drop-down menu to assign a license from the Web Communication Assistant to the user and give him/her the right to use all the applications.
7. Click **Next**. The **Summary** window appears, showing the user's various characteristics.
8. Click **Finish**.

Remark 2:

depending on your system's configuration (mainly the RAS and e-mail functions), other screens may appear in this assistant.

9.2.6.1.2 CREATING A USER GROUP

Click **Wizards** in the navigation bar. The wizards icons appear.

1. Click on the **Group Assistant** icon. The **Group Wizard** window is displayed.
2. In the **Group properties**field, input the name of the group you want to create.
3. Click **Next**. A new window appears.
4. In the **Group rights** field, check the box or boxes matching the rights you wish to attribute to the group. The available choices are:
   - **Web site access (HTTP)**: This field enables Internet access control if the authentication request function is active in the proxy (see Proxy/Cache chapter). If this box is checked, it means that the user has access to the Web sites authorized by the proxy filters (see Proxy/Cache chapter). Depending on the rights granted to the group to which he/she belongs, a user may or may not access the Web sites (for more details, please refer to the "Make Internet Access More Secure" sheet.
   - **File transfers (FTP)**: The user may transfer files. This service is available if you have a proxy software key and if you have chosen an access control policy based on groups.
   - **Local Mailbox**: The user has a local mailbox.
   - **Intranet Publishing**: The user may publish files on the Intranet.

- **Remote Access (VPN/RAS)**: Users can connect to Alcatel-Lucent OmniPCX Office Communication Server from a notebook computer and establish a VPN tunnel to the local network via the Internet.

5. Click **Next**. The **Résumé** window appears, showing the various characteristics of the user groups you have created.
6. Click **Finish**.

9.2.7 Managing Users and User Groups

9.2.7.1 Operation

The management of users and user groups involves the following tasks:

- Modifying a user's properties.
- modifying user group properties,
- adding one or several users or user groups,
- deleting one or several users or user groups,
- changing one or several user groups.

In order to access the **Users and Groups Management** window, click **Users** in the navigation bar. This window comprises two areas:

- The **Users List** area, which shows all the defined users, sorted by group.
- The **Pre-configured Groups** area shows all the empty and usable groups.

9.2.7.1.1 MODIFYING A USER'S PROPERTIES

1. Click the user's last name. The **User Settings** window displays. This page includes six tabs: **Settings**, **E-mails**, **Vacation**, **Forwards**, **Aliases**, **Voice messages, Licenses, Remote Access**.
2. Click the **Settings** tab. This tab allows verifying or modifying all the parameters input during a user's creation.

   Remark 1:
   if you change this user's group, he/she inherits all the rights of the new group.
3. Click the **E-mails** tab. This tab allows verification or modification of the user's e-mail parameters.
4. Click the **Vacation** tab. This tab allows you to enter an absence message.
   a. Check the **Send an e-mail for vacation** box to enable this service.
   b. In the field **E-mail subject**, enter the subject of your e-mail.
   c. In the field **E-mail content**, enter the content of your e-mail.
   d. Click **Apply** to accept the data, or click **Cancel** if you do not want to keep the changes.
5. Click the **Forward** tab. This tab allows you to enter the e-mail addresses where the user's mail is to be sent on; a copy can be stored at the user's base address.
   a. In the **E-mail forwarding** area, check the box:
      - **Forward all my e-mails** to activate this service.
      - **Keep a copy before forwarding** to keep a copy at the e-mail's initial recipient.
   b. In the **Forward address** area, fill in the **New address** field by entering your e-mails'

destination address.

c. Click **Apply** to accept the data, or click **Cancel** if you do not want to keep the changes.

6. Click on the **Aliases** tab. This tab allows you to configure an alias. An alias is another name for the same user (for more details, please review the E-mail sheet).
   a. In the **Aliases** area, fill in the following field:
   - **New Alias**: allows customization of the user with an alias.

   b. Click the **Add** button. The new alias appears in the **Existing aliases** list.
   c. Click **Apply** to accept the data, or click **Cancel** if you do not want to keep the changes.

   Remark 2:
   *Click **Delete** to delete an existing alias.*

7. Click on the **License** tab. This tab is used to assign a license from the Web Communication Assistant to the user. Select **Yes** from the **Web Communication Assistant** drop-down menu if you want to assign the license to the user.
8. Click on the **Remote Access** tab. This tab allows you to configure a remote access.
   a. In the **Callback** area, select your callback method. Three choices are available:
   - **No callback**
   - **Dynamic**
   - **Static**

   b. In the **IP Address Assignment** area, you have two choices:
   - **Dynamic**: The RAS server manages the IP address negotiation.
   - **Static**: Enter the IP address associated to the user in the**IP Address** field.

   c. Click **Apply** to accept the data, or click **Cancel** if you do not want to keep the changes.

9.2.7.1.2 MODIFYING A USER GROUP PROPERTIES

1. Click your choice of user group name. The **Group Settings** window displays. This page includes five tabs: **Settings**, **Rights**, **Control**, **Alert** and **Voice mess.**
2. Click the **Settings** tab. This tab allows verifying or modifying all the parameters input during user group creation.
3. Click the **Rights** tab. This tab is used to define the user group rights. Check the Box or boxes matching the rights you want to assign to the group. The available choices are:
   - **Access to web sites (HTTP)**
   - **File transfer (FTP)**
   - **Local mailboxes**
   - **Authorize e-mail sending for vacation**
   - **Authorize e-mail forwarding**
   - **Intranet Web authoring**
   - **Remote access (VPN / RAS)**
   - **Administrator privileges**
   - **Operator privilege**
4. Click the **Control** tab. This tab is used to define the control policy relating to the user group.
   a. In the **Time range selection** area, select the time range assigned to the group from the **Time range** drop-down menu.
   b. In the **Web site control** area, select the control type from the drop-down list, i.e.:

- **All sites except forbidden sites**
- **Authorized sites only**
- **No control**

Remark:
*when you select **All sites except forbidden sites** or **Authorized sites only**, you have access to the **Forbidden sites filters** and **Authorized sites filters** lists respectively. Check or uncheck the boxes to the left of the prohibited sites per your choices.*

5. Click the **Alert** tab. This tab allows you to define the receipt policy related to alert messages. An alert message is sent when the space on the disk containing the e-mail exceeds the threshold value. By default, this value is 100 MB.

9.2.7.1.3 ADDING A USER OR USER GROUP

Click **Add** in the user list to add a user.

Click on the **Group Assistant** icon to add a user group.

9.2.7.1.4 DELETING ONE OR MORE USERS

Deleting a user or a user group

Click the corresponding **Delete** hypertext link.

Deleting several users or user groups

1. Select the users or user groups by checking the box preceding the user's or the user group's name.
2. Click **Delete the selection**.

9.2.7.1.5 CHANGING GROUP FOR ONE OR MORE USERS

1. Select users by checking the box preceding the user's name.
2. Select the user group to which they will belong from now on.
3. Click the button **Move the selection**.

Remark:
when a user is moved from group A to B, s/he loses the rights of group A and gains the rights of group B.

9.2.8 Operator Tasks at Administration Level

9.2.8.1 Overview

Web-Based Management (WBM) is an Alcatel-Lucent OmniPCX Office Communication Server Internet service administration tool.

WBM can be used by a local administrator called an operator.

To use the WBM at operator level, you must log on using:

- either a user account belonging to a group that has operator rights.
- or the default "operator" account.

9.2.8.1.1 WHAT ARE THE OPERATOR'S FUNCTIONS?

An operator can only manage routine tasks. S/he cannot modify service configuration.

The operator's main tasks are:

1. **User management**
   The operator's most important responsibility is user management. Concerning the user groups, the operator only has access to a read-only summary of the existing groups" settings. Creation of user groups remains the administrator's privilege.

2. **Supervision of system information and statistics**
   Advanced statistics on system activity can be obtained over a period of time or at a given time, and on application aspects, thanks to the statistics tool integrated in Alcatel-Lucent OmniPCX Office Communication Server. These data can be accessed through the WBM interface. These statistics are shown in tables with the possibility of accessing graphics allowing the user to view the evolution over time.
   Two types of information are accessible via WBM:
   - Snapshot information
     These are measurements of the system's activity, recorded in real time.
     - System information,
     - management of the memory and swap, as well as the processor load,
     - hard disk utilisation (partition),
     - network traffic.
   - Statistics
     Information stored on the Alcatel-Lucent OmniPCX Office Communication Server's hard disk (system activity statistics and applications statistics). It is stored in the log files. Three types of statistical analysis are available:
     - Statistics on HTTP resources access: Proxy server (HTTP or FTP protocol) and Intranet Web server.
     - Statistics on e-mail service.
     - Statistics on the various connection types: Internet connections (DSL or ISDN modem), VPN and RAS connections.

   Snapshot information and statistics can be consulted in the form of either graphics or tables.

3. **Configuration of time ranges and mailing lists, as well as backup management.**
   - Configuration of the time ranges
     Here, a time range for Internet access is determined for each day of the week, either for the system itself, or for individual groups of users.
   - Mailing list configuration
     A mailing list contains one or more user's login and/or one or more email addresses. If an email is sent to this mailing list, the message will be broadcast to every member belonging to this list.
   - Backup Management
     To avoid losing data after a hard drive crash, Alcatel-Lucent OmniPCX Office Communication Server is equipped with a backup mechanism for all existing files. This mechanism also creates backup files for the configuration of telephony and Internet services. The backup is done on network equipment.
     In the event of a hard disk replacement, all data are restored on the new hard disk from the last backup operation.
     The backup can be manual or automatic. If it is automatic, the operator programs how often and at what time the backup is carried out. Data restoration is manual.

SUMMARY OF THE OPERATOR'S TASKS

The following table lists all the Alcatel-Lucent OmniPCX Office Communication Server Internet services that can be configured by an operator using WBM.

TASKS		INDIRECT
Access to the Welcome Page		Authorised
User management		
Creating users		Authorised
Changing a user's properties,		Authorised
Deleting one or more users		Authorised
Transferring a user to a group without administrator rights		Authorised
Transferring a user to a group with administrator rights		Not allowed
Creating an operator		Authorised
Changing properties of other operators		Authorised
Deleting one or more other operators		Authorised
Changing the group of another operator		Authorised
Creating, changing and deleting an administrator		Not allowed
Changing an administrator's group		Not allowed
Distribution list management		
Distribution list management		
	Adding a new mailing list,	Authorised
	Deleting one or more mailing lists	Authorised
	Changing the properties of a mailing list	Authorised
Controlling Internet use		
Time ranges management		
	Changing the properties of the global time range	Authorised
	Changing the properties of existing time ranges	Authorised
	Adding a time range	Not allowed
	Deleting a time range	Not allowed
Security		
Changing the operator password		authorized
Supervision of system information and statistics		
Access to the dashboard		Authorised
Backup Management		
	Backup management (programming or deleting a backup, performing a manual backup and managing the backup history)	Authorised
	Configuration of the backup system.	Not allowed
	Restoring a backup	Not allowed

Remark:

The operator cannot access context-sensitive help.

If an operator attempts to access screens to which he does not have access, the login page is displayed with an error message.

9.2.9 Interface Description

9.2.9.1 Basic description

The main characteristics of the interface are:

- the use of hyperlinks, tables, buttons and wizards,
- verification of information prior to validation,
- the possibility of choosing the display language (French, English, German, Italian, Spanish, Portuguese or Dutch). The language is configured in the Web navigator.

9.2.9.1.1 The screens

The WBM interface contains three screen types:

1. **A wizard screen**
   It allows rapid, easy user configuration (User Wizard)
2. **The administration screens**
   These screens are accessed by clicking on the corresponding hypertext link in the navigation bar. The administration screens give access to the lists of:
   - Users per group
   - Time Ranges
   - Mailing lists
   - Backups performed
   - System information

   From the administration screens you can access the configuration screens.
3. **The configuration screens**
   The following screens are associated with the administration screens:
   - user screens
   - time range
   - mailing lists

   The following screens are used to directly configure the associated features:
   - E-mail
   - Backup

9.2.9.1.2 Description of the configuration and administration screens

The configuration and administration screens are divided into four areas:

1. **The general information banner**
   It is made up of the current configuration title and the other configurations that can be accessed from this page.
2. **The navigation bar**
   It is divided into sub-sections each representing a characteristic of Alcatel-Lucent OmniPCX Office Communication Server. By clicking on one of the menus offered, you will go to the corresponding configuration screens.
3. **The screen body**

Several tabs are available, depending on the screen. By clicking on one of the tabs, you will go to other screens. Various windows can be accessed by clicking on the hyperlinks on any given page.

9.2.9.1.3 Some common actions

The following actions are common to all the screens.

To delete or move several elements in a list, use the check boxes to the left of the elements and click on the **Delete selection** or **Move selection** button (in the middle of the screen).

To delete or add only the element corresponding to the line, click on the hypertext link **Add** or **Delete**.

9.2.10 Connection to WBM

9.2.10.1 Operation

The procedure for connecting to the WBM is as follows:

1. Open the Web navigator.
2. Enter the following address in the **Address** field of the Web navigator:
   https://<Alcatel-Lucent OmniPCX Office Communication Server>/admin
   where <Alcatel-Lucent OmniPCX Office Communication Server> is the machine's IP address or name.
   You go to the **Web-Based Management - Authentication** page.
3. In the **Administrator / operator authentication** area, enter the user name belonging to a group that had operator rights or "operator" followed by the associated password.
4. Click on **Connect**. Your service connection is established.
   The **WBM Operator Home Page** is displayed directly. It presents a summary of the system's activity.

9.2.10.1.1 How to disconnect

To disconnect, click on**Disconnect** in the navigation bar. The connection has been deactivated.

Remark:

After 30 minutes of inactivity, disconnection is automatic.

9.2.11 Managing Users

9.2.11.1 Operation

User management comprises the following tasks:

- creating a user
- Modifying a user's properties.
- adding one or several users,
- deleting one or several users,
- changing one or several users" group.

9.2.11.1.1 CREATING A USER

Click **Wizards** in the navigation bar. The assistants" icons appear.

1. Click the **User's Assistant** icon. The **User Wizard** window displays.
2. The following field must be filled in:
   - **First name**: The user's first name (optional).
   - **Name**: The user's last name.
   - **User name**: this field is completed automatically. The user name takes the form *First Name.Surname*. The user uses this name to connect to the services offered by the system. This name is also used to create the user's e-mail address.
   - **Password**: User password

     Remark 1:
     The passwords must comply with the following rules:
     - comprise 6 to 8 characters,
     - comprise at least one upper-case letter,
     - comprise at least one non alphanumeric character.
   - **Confirm password**
3. Click **Next**. A new window appears.
4. In the drop-down list, select the group where you want to associate the new user.
5. Click **Next**. The **Summary** window appears, showing the user's various characteristics.
6. Click **Finish**.

Remark 2:
Depending on your system's configuration (mainly the RAS and e-mail features), other screens may appear in this assistant.

9.2.11.1.2 MODIFYING A USER'S PROPERTIES

1. Click on **Users** in the navigation bar. The **Users and Groups Management** window appears.
2. Click on the user name in the **User list** area. The **User Settings** window displays. This page includes six tabs: **Settings**, **E-mails**, **Vacation**, **Forwards**, **Aliases**.
3. Click the **Settings** tab. This tab is used to:
   - verify or modify all the parameters input during a user's creation.
   - attribute a Web Communication Assistant license to the user by selecting **Yes** in the **Web Communication Assistant License** drop-down menu.

   Remark 1:
   If you assign a user to another group, he/she inherits all the rights of the new group.
4. Click the **E-mails** tab. This tab allows verification or modification of the user's e-mail parameters.
5. Click the **Vacation** tab. This tab allows you to enter an absence message.
   a. Check the **Send an e-mail for vacation** box to enable this service.
   b. In the field **E-mail subject**, enter the subject of your e-mail.
   c. In the field **E-mail content**, enter the content of your e-mail.

d. Click **Apply** to accept the data, or click **Cancel** if you do not want to keep the changes.

6. Click the **Forward** tab. This tab allows you to enter the e-mail addresses where the user's mail is to be sent on; a copy can be stored at the user's base address.
   a. In the **E-mail forwarding** area, check the box:
      - **Forward all my e-mails** to activate this service.
      - **Keep a copy before forwarding** to keep a copy at the e-mail's initial recipient.
   b. In the **Forward address** area, fill in the **New address** field by inputting your e-mails" destination address.
   c. Click **Apply** to accept the data, or click **Cancel** if you do not want to keep the changes.
7. Click on the **Aliases** tab. This tab allows you to configure an alias. An alias is another name for the same user (for more details, please review the E-mail sheet).
   a. In the **Aliases** area, fill in the following field:
      - **New Alias**: allows customization of the user with an alias.
   b. Click the **Add** button. The new alias appears in the **Existing aliases** list.
   c. Click **Apply** to accept the data, or click **Cancel** if you do not want to keep the changes.

   Remark 2:
   *Click **Delete** to delete an existing alias.*

9.2.11.1.3 ADDING A USER

1. Click on **Users** in the navigation bar. The **Users and Groups Management** window appears.
2. Click **Add** in the users" list to add a user.

9.2.11.1.4 DELETING ONE OR MORE USERS

Delete a user

1. Click on**Users** in the navigation bar. The **Users and Groups Management** window appears.
2. Click the corresponding **Delete** hypertext link.

Delete several users

1. Click on**Users** in the navigation bar. The **Users and Groups Management** window appears.
2. Select users by checking the box preceding the user's name.
3. Click **Delete the selection**.

9.2.11.1.5 CHANGING GROUP FOR ONE OR MORE USERS

Remark 1:
It is not permitted to transfer a user to a group that has administrator rights.

1. Click on**Users** in the navigation bar. The **Users and Groups Management** window appears.
2. Select users by checking the box preceding the user's name.
3. Select the users" group to which they will belong from now on.

4. Click the button **Move the selection**.

   Remark 2:
   When a user is moved from group A to B, s/he loses the rights of group A and gains the rights of group B.

9.2.12 Managing Mailing Lists

9.2.12.1 Operation

Mailing lists management comprises the following tasks:

- adding a new mailing list,
- deleting one or several mailing lists,
- modifying mailing list properties,

Click on **E-mail** in the navigation bar. The **E-mail management** window appears, with the **Mailing list** area showing. This window has the following areas:

- the **E-mail server operating mode** area, which lists the characteristics of the mail server configured via the wizard.
- the **User list** area, which lists all the users created who have a local mailbox with their e-mail address. Click on the user name to access the **E-mail** tab of the **User Settings** window.
- the **Mailing lists** area shows all the mailing lists. When the users and the messaging accounts have been created, Alcatel-Lucent OmniPCX Office Communication Server is used to create and manage the mailing lists. A mailing list holds several electronic addresses under the same name, which allows users to fill in the name of the list as the recipient of a message (name of a service for instance), rather than having to fill in all the addresses of the individuals concerned.

9.2.12.1.1 ADDING A NEW MAILING LIST

1. Click **Add** The **Mailing List Wizard** window appears. It comprises the following tabs: **Settings**, **Members** and **E-mail**.
2. Click on the **Settings** tab. In the **Mailing List Name** area, enter the name of the mailing list.
3. Click on the **Members** tab. This tab is used to create the mailing list members.
   a. In the **New Members** area, there are two possible choices:
      - Select **Add a defined user** if the member you want to add to the list is a user defined in the system. Select the user(s) in the drop-down menu.
      - Select **Add an e-mail address** if the member you want to add to the list has an external e-mail address. Enter this e-mail address in the **E-mail Address** field.

   b. Click on the **Add** button to validate the new member's addition. The new members appear in the list located below the **New Members** area.
4. Click on the **E-mail** tab. This tab is used to configure the e-mail settings of the mailing list.
   a. The **E-mail Server Operating Mode** area lists the characteristics of the e-mail server configured via the wizard.
   b. The **Mailing List e-mail address** area gives the mailing list address which will be used to send e-mails to this list. This address cannot be modified.

c. In the **External POP3 mailbox** area, fill in the following fields:

- **POP3 mailbox name**
- **Password**
- **Confirm password**

Remark:
This area is only displayed in POP3 configuration or POP3 multidrop configuration with a mailbox dedicated to the mailing list.

5. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

DELETING ONE OR SEVERAL MAILING LISTS

To delete a mailing list, click on the corresponding **Delete** hypertext link.

To delete several mailing lists: select the mailing lists by checking the box located before the mailing list name and click on **Delete selection**.

MODIFY A MAILING LIST PROPERTIES

Click on the mailing list name of your choice. The **Mailing List Settings** window appears. It comprises three tabs: **Settings**, **Members** and **E-mail**. For more information on configuring this tab, see the Add a new mailing list section.

9.2.13 Managing Time Ranges

9.2.13.1 Operation

Time range management comprises the following tasks:

- Time range selection,
- changing the settings of a time range,

Remark:
The system's time range always takes precedence over a group's defined time range.

To access the **URL Filter Management** window, click on **URL Filters** in the navigation bar. This window comprises two areas:

- The **Time range selection** area.
- The**Time range list** area.

9.2.13.1.1 SELECT A GLOBAL TIME RANGE

1. In the **Select a time range** zone, choose a time range in the **Global time range** drop-down menu.
2. Click **Apply** to validate.

9.2.13.1.2 CHANGING THE SETTINGS OF A TIME RANGE

1. Click on the name of the time range you want to change. The **Time Range Settings** window is displayed.
2. Check and/or modify the characteristics of the time range.
3. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

9.2.14 Security

9.2.14.1 Operation

9.2.14.1.1 CHANGING THE OPERATOR PASSWORD

If the password is stolen or divulged, the operator password can be changed via WBM.

1. Click on **General** in the navigation bar. The **General** window displays.
2. Click on the **Password** tab.
3. In the **Operator password** area, fill in the following fields:
   - **Old password**
   - **New password**
   - **Confirm password**
4. Click **Change** to validate the changes.

Remark:
*If the old password is entered incorrectly, the **Web-Based Management - Error** window is displayed, giving the causes and the solutions to the problem.*

9.2.15 Access to the Dashboard

9.2.15.1 Operation

Click on **Dashboard** in the navigation bar. The **System Dashboard** window appears. This window has the following tabs:

- **Statistics**
- **Information**
- **System**
- **Partitions**
- **Network**

1. Click on the **Statistics** tab. This tab shows system application statistics. Three types of statistics are defined:
   - Connection statistics: to access those statistics, click on the hyperlinks in the **Internet connections**, **VPN Connections** or **RAS Connections** areas.
     - The **Available statistics** table lists connection indexes with the appropriate counters.
     - For each month, the hyperlink makes it possible to access the monthly connection details. In case of VPN or RAS connections, the hyperlink list may contain an additional link (User connections) for the analysis period. In those cases, the page contains an additional table listing all users who have established a connection along with their statistics. The **Summary** table contains a counter-based summary. The **Daily Connections** graphic represents all days of the month when connections have been established. The histograms correspond to the connection duration, and they are labelled in hours. The **Connection List** table lists all connections established in the course of the month. The "Status" column shows a

successful connection.

- E-mail statistics: to access those statistics, click on the **See e-mail statistics** hyperlink in the **Internet utilisation** area.
  - The **Mailbox sizes** table lists the local mailboxes with their sizes. The **Available statistics** table lists the months for which statistics are available.
  - For each month, the hyperlink makes it possible to access the monthly index details. The **Summary** table contains a counter-based summary. The **Daily Messages** graphic shows the times at which the mail server has been accessed the most. The first table lists machines with which the local server has processed the most messages: the transmitting machines first, then the external servers. The other two tables show the accounts which received most of the e-mail messages, and those which transmitted the most.
- Webalizer statistics: to access those statistics, click on the **Proxy statistics** and **Intranet web statistics** hyperlinks in the **Internet utilization** area.

2. Click on the **Information** tab. This tab shows system statistics. They are specific to the hardware configuration and the software version. Therefore, they remain unchanged as long as Alcatel-Lucent OmniPCX Office Communication Server is running. They are gathered as Alcatel-Lucent OmniPCX Office Communication Server boots up.
3. Click on the **System** tab. This tab shows system snapshot information. This information shows the system status at a given moment.
   - Click on the **CPU Loads**, **Memory used** or **Swap used** hyperlinks to open the **System Graph** window. Each graphic shows the evolution for the dynamic data period.
     - If necessary, use the **Automatic scaling** option.
     - The drop-down list allows the user to choose between an hourly synthesis and a daily synthesis.
   - Click on the **Process** hyperlink to open the **Process Tree** window. The process tree is mainly used to identify errors.
     - The **Close** button causes the window to close.
     - The **Refresh** button allows the data to be updated.
   - Click on the **Refresh** button to update the dynamic information.
   - Check the **Auto-refresh** box to automatically update the data every 7 seconds.
4. Click on the **Partitions** tab. This tab lists the partitions on the system, their mount points, capacities and occupancy rate.
   - Click on the partition-related hyperlinks to open the **System Graph** window. Each graphic shows the partition occupancy over time.
     - If necessary, use the **Automatic scaling** option.
     - The drop-down list allows the user to choose between an hourly synthesis and a daily synthesis.
   - Click on the **Refresh** button to update the partition rates.
5. Click on the **Network** tab. This tab displays detailed information on the network interface usage.
   - Click on the interface-related hyperlinks to open the **System Graph** window. Each graphic shows the network traffic over time.
     - If necessary, use the **Automatic scaling** option.
     - The drop-down list allows the user to choose between an hourly synthesis and a daily synthesis.
   - Click on the **Refresh** button to update the information.

a.

9.2.16 Managing Backup

9.2.16.1 Operation

To access the **Backup Management** window, click on **Backup** in the navigation bar.

1. In the **Manual backup** area, click on the **Backup** button to start the full system backup.
2. The **Backup list** area shows all the backups already carried out. To delete one or more list backups, click on the **Delete** button or on the **Delete Selection** button.
3. To access the **Backup Settings** window, click on the **Backup Settings** hyperlink. The **Behavior** tab displays the information needed to determine the backup behavior.
   a. In the **Periodicity** area, select the backup activation frequency and type in the backup activation time.
   b. In the **Backup History** area, type in the number of backups you want to save on the network hardware in the **Size of backup history**.
   c. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

9.3 Internet Access

9.3.1 Overview

Setting up shared Internet access on a client station involves a number of stages:

- Installation of Alcatel-Lucent OmniPCX Office Communication Server.
- Creating and configuring an Internet connection
- Configuring the client station

9.3.2 Subscription to an ISP

9.3.2.1 Detailed description

9.3.2.1.1 The essential information

A subscription with an ISP is necessary to access the Internet. After you have subscribed, the ISP sends you back **essential** information for installing you Internet access. This information must be entered when configuring Alcatel-Lucent OmniPCX Office Communication Server.

The information required to install the Internet access varies according to the type of connection to be established.

ISDN connection	Connection DSL modem/Cable modem	External Router Connection	LAN server
User name Password Telephone number Bandwidth Connection type IP address Primary and secondary name server	Authentication: - User name - Password IP parameters - IP address of router modem - Network mask - IP address of the WAN interface Protocols - IP over Ethernet - PPTP - PPPOE Name server - IP address of router modem - Primary DNS - Secondary DNS	Router's IP address System's IP address Network mask Primary and secondary name server	Router's IP address Primary and secondary DNS IP address or Router IP address

9.3.2.1.2 Description

All this information is described below.

- **Connection account**
  This account is used when identifying the connection to the ISP. This account is unique, and enable users to authenticate on connection to the access provider by entering the account name and associated password (except for External Router and LAN Server connections).
  - "User name": account issued by the access provider. This account is used in the PAP/CHAP authentication process on connection to the ISP. This account, a form of security used by the access provider, must be entered only once in Alcatel-Lucent OmniPCX Office Communication Server. It must not be confused with the user identifier and password: these are entered in the browser when requesting access to the Web, and enable verification of the number of users with access to Internet resources. There are two levels of authentication:
    - authentication (client station) managed by Alcatel-Lucent OmniPCX Office Communication Server for each Internet user in the company.
    - authentication (Alcatel-Lucent OmniPCX Office Communication Server) managed by the access provider. Internet access is shared by all the users; This process is unique and transparent for all users.
  - "Password": password associated with the connection's user name.
- **Access provider's telephone number**
  - "Telephone number": the telephone number dialed for connection to the ISP.
  - "Emergency phone number**"**: may or may not exist, depending on the chosen access provider. This number is used when the main number is unavailable.
- **Bandwidth**
  The allocated bandwidth corresponds to the throughput between Alcatel-Lucent OmniPCX Office Communication Server and the access provider for an ISDN type connection. The larger the bandwidth, the faster the data transmission (and the greater the connection

costs). Three choices are possible in the number of B channels used:

- "1 64 Kbps B channel": the connection uses a single B-channel (static mode).
- "2 128 Kbps B channels": uses two B-channels statically. This doubles the connection cost.
- "on demand (64-128 Kbits/s)": uses two B-channels dynamically. The charge rates are identical to those for the 128 Kbps mode, but the traffic is optimized as a function of bandwidth requirement. The bitrate at the ISP must correspond to 128 Kbps access. This option cannot therefore be chosen if the connection to the access provider is set at 64 Kbps.

- **Type de connection**
  The type of link between Alcatel-Lucent OmniPCX Office Communication Server and the access supplier can be established with:
  - "On demand call": the channel or channels are called up in response to user demand and automatically timed out when there is no more traffic. This type of connection avoids unnecessary charges when there is no traffic.
  - "Permanent": the connection between the IAP and Alcatel-Lucent OmniPCX Office Communication Server is permanent, it is like using a leased line from the telephone operator.
  - "Callback": this option is chosen when a client terminal outside the LAN wishes to access Alcatel-Lucent OmniPCX Office Communication Server via Internet (See Section VPN). It allows Alcatel-Lucent OmniPCX Office Communication Server to dial automatically the call number of the ISP in order to establish connection.
- **IP address allocation**
  The IP address is allocated to Alcatel-Lucent OmniPCX Office Communication Server by the access provider. This address is public. If the access provider manages the IP address negotiation, the "dynamic" option must be checked, otherwise enter the assigned IP address. A fixed IP address is needed for always-on connections and VPN use.
- **DNS servers**
  This information corresponds to the IP addresses of the DNS servers on the premises of the access provider. These servers are used to translate site names into IP addresses.
  - "Address of primary DNS server". ".
  - "Address of secondary DNS server".
- **Connection protocol**
  This information is provided by the ISP for a DSL modem/Cable Modem type connection. In this case, a point-to-point connection is established between OmniPCX Office and the DSL modem/Cable Modem. Two types of communication protocols are available to manage this connection.
  - PPPoE: this protocol is used to send PPP packets over Ethernet. This protocol allows "permanent" or "on-demand call" type connections.
  - PPTP: this protocol consists of establishing an IP tunnel between Alcatel-Lucent OmniPCX Office Communication Server and the modem. This protocol allows only "permanent" connections.
  - IP over Ethernet: this protocol is used to send IP packets over Ethernet. It allows only "permanent" connections.
- **Connection properties**
  To define the connection parameters, the ISP gives the following elements:
  - "WAN interface IP address": this is the IP address of the WAN interface. This parameter must be consistent with the IP address of the router, the DSL Modem or the

Cable Modem.

- "DSL modem/Cable modem address" or "Router address": this is the IP address of the Router, the DSL Modem or the Cable Modem
- "Network mask": parameter determining the range of the network.

9.3.3 Configuring Internet Connection

9.3.3.1 Configuration procedure

There are several ways to configure an Internet connection:

- creation of an ISDN type connection,
- creation of a DSL modem type connection,
- creation of a Cable Modem type connection,
- creation of an External Router connection,
- creation of LAN Server connection,

9.3.3.1.1 CREATION OF AN ISDN TYPE CONNECTION

Click on **Wizards** in the navigation bar. The assistants" icons appear.

1. Click on the **Connection Assistant** icon. The **Assistant connection** window displays.
2. In the **Profile identification** area, fill in the following field:
   - **Profile name**: this name identifies the new Internet connection managed by Alcatel-Lucent OmniPCX Office Communication Server. The profile groups together all the parameters associated with the connection. It is best to give it a name that represents the newly created connection - the name of the access provider, for example.
3. Check the **Configure this profile as the active profile** box if the profile you are creating is to be active (default value).
4. Click on **Next**. A new window appears.
5. In the **Connection type** area, click **ISDN**.
6. Click on **Next**. A new window appears.
7. In the **ISDN connection parameters** area, fill in the following fields:
   - **ISP phone number**: enter the telephone number dialled when connecting to the IAP. Must include any external line prefix for calling outside the company.
   - **ISDN bandwidth**: select the bandwidth type in the drop-down menu. Three choices are possible for the number of B channels used:
     - 64 kbps static (1 B channel)
     - Dynamic 64/128 Kbit/s (1-2 B channels): this option must not be chosen if the connection to the access provider is 64 Kbits/s.
     - 128 kbps static (2 B channels)
   - **Connection mode**: three choices are possible:
     - Dial on demand
     - Dial on demand - call-back allowed
     - Permanent connection

8. Click on **Next**. A new window appears.
9. In the **Authentication parameters** area, fill in the following fields:
   - **Account name**: enter the account name sent by the access provider.
   - **Password**: input the password associated to the connection's account name.
   - **Confirm the password**: enter the same password as was just entered. This confirmation filters out typing errors.
10. Click on **Next**. A new window appears.
11. In the **IP Address Allocation** area, you have two choices:
    - **Dynamic Allocation**: the ISP manages the IP address negotiation.
    - **Fixed IP address**: input the IP address provided by the ISP in the**Public IP Address** field.
12. In the **ISP's DNS** area, you have two choices:
    - **Dynamically find the ISP DNS**: the DNS resolution is automatic during connection.
    - **Set the ISP's DNS**: input the IP address for the ISP's primary DNS in the **ISP's primary DNS** field. We recommend keeping automatic DNS resolution.
13. Click on **Next**. The **Summary** window displays. This stage is used to verify the connection properties.
14. Click **Finish** to validate the parameters. Click **Previous** to return to the previous screens and modify the desired parameters.

9.3.3.1.2 CREATION OF A DSL MODEM/CABLE MODEM TYPE CONNECTION

Click on **Wizards** in the navigation bar. The assistants" icons appear.

1. Click on the **Connection Assistant** icon. The "Connection Assistant" window displays.
2. In the **Profile identification** area, fill in the following field:
   - **Profile name**: this name identifies the new Internet connection managed by Alcatel-Lucent OmniPCX Office Communication Server. The profile groups together all the parameters associated with the connection. It is advisable to enter a name that is representative of the created connection, such as the name of the access provider.
3. Check the **Configure this profile as the active profile** box if the profile you are creating is to be active.
4. Click on **Next**. A new window appears.
5. In the **Connection type** area, click **DSL Modem** (requires 2 Ethernet interfaces).
6. Click on **Next**. A new window appears.
7. In the **DSL Connection Parameters** area, chose the protocol used in the drop-down list **Connection's Protocol**:
   - **PPPoE (direct Ethernet connection)**

   a. In the **Connection Mode** field, select **On Demand** if your access is not permanent.

   b. Click on **Next**. A new window appears.

   c. In the **Authentication parameters** area, fill in the following fields:
   - **Account name**: enter the account name sent by the access provider.
   - **Password**: input the password associated to the connection's account name.
   - **Confirm the password**: enter the same password as was just entered. This

confirmation filters out typing errors.

d. Click on **Next**. A new window appears.

e. In the **IP Address Allocation** area, you have two choices:

- **Dynamic Allocation**: the ISP manages the IP address negotiation.
- **Fixed IP address**: enter the IP parameters supplied by the ISP.

f. In the **ISP's DNS** area, you have two choices:

- **Dynamically find the ISP DNS**: the DNS resolution is automatic during connection.
- **Set the ISP's DNS**: input the IP address for the ISP's primary DNS in the **ISP's primary DNS** field. We recommend keeping automatic DNS resolution.

g. Click on **Next**. The **Summary** window displays. This stage is used to verify the connection properties.

h. Click **Finish** to validate the parameters. Click **Previous** to return to the previous screens and modify the desired parameters.

- **PPTP (tunnelling)**

i. Click on **Next**. A new window appears.

j. In the DSL Modem Connection area, fill in the following fields:

a.
- **WAN interface IP address**: input the IP address of the WAN interface.
- **IP address of the DSL modem**: enter the IP address of the external modem.
- **Subnet mask**: enter the defined mask.

b. Click on **Next**. The **Summary** window displays. This stage is used to verify the connection properties.

c. Click **Finish** to validate the parameters. Click **Previous** to return to the previous screens and modify the desired parameters.

- **IP over Ethernet**

d. Click on **Next**. A new window appears.

e. In the **ISP's DNS** area, you have two choices:

- **Dynamically find the ISP DNS**: the DNS resolution is automatic during connection.
- **Set the ISP's DNS**: input the IP address for the ISP's primary DNS in the **ISP's primary DNS** field. We recommend keeping automatic DNS resolution.

f. Click on **Next**. The **Summary** window displays. This stage is used to verify the connection properties.

g. Click **Finish** to validate the parameters. Click **Previous** to return to the previous screens and modify the desired parameters.

9.3.3.1.3 CREATION OF AN EXTERNAL ROUTER TYPE CONNECTION

Click on **Wizards** in the navigation bar. The assistants" icons appear.

1. Click on the **Connection Assistant** icon. The "Connection Assistant" window displays.
2. In the **Profile identification** area, fill in the following field:
   - **Profile name**: this name identifies the new Internet connection managed by Alcatel-Lucent OmniPCX Office Communication Server. The profile groups together all the parameters associated with the connection. It is best to give it a name that represents the newly created connection - the name of the access provider, for example.

3. Check the **Configure this profile as the active profile** box if the profile you are creating is to be active.
4. Click on **Next**. A new window appears.
5. In the IP Address Allocation area, you have two choices:
   - **Dynamic Allocation**: the ISP manages the IP address negotiation.
   - **Fixed IP address**: enter the IP parameters supplied by the ISP.
6. Click on **Next**. A new window appears.
7. In the **ISP's DNS** area, you have two choices:
   - **Dynamically find the ISP DNS**: the DNS resolution is automatic during connection.
   - **Set the ISP's DNS**: input the IP address for the ISP's primary DNS in the **ISP's primary DNS** field. We recommend keeping automatic DNS resolution.
8. Click on **Next**. The **Summary** window displays. This stage is used to verify the connection properties.
9. Click **Finish** to validate the parameters. Click **Previous** to return to the previous screens and modify the desired parameters.

9.3.3.1.4 CREATION OF LAN SERVER CONNECTION

Click on **Wizards** in the navigation bar. The assistants" icons appear.

1. Click on the **Connection Assistant** icon. The "Connection Assistant" window displays.
2. In the **Profile identification** area, fill in the following field:
   - **Profile name**: this name identifies the new Internet connection managed by Alcatel-Lucent OmniPCX Office Communication Server. The profile groups together all the parameters associated with the connection. It is best to give it a name that represents the newly created connection - the name of the access provider, for example.
3. Check the **Configure this profile as the active profile** box if the profile you are creating is to be active.
4. Click on **Next**. A new window appears.
5. In the **Connection Type** area, click **No Direct WAN Connection (LAN Server)**.
6. Click on **Next**. A new window appears.
7. In the **Default Gateway** area, fill in the following field:
   - **Default gateway**: enter the IP address of your router.
8. Click on **Next**. A new window appears.
9. In the **ISP's DNS** area, fill in the following fields:
   - **ISP's primary DNS**: enter the IP address of the access provider's primary DNS or the router's IP address if the access provider's DNSs are configured in the router.
   - **ISP's secondary DNS**: enter the IP address of the access provider's secondary DNS or the router's IP address if the access provider's DNSs are configured in the router. The configuration of a secondary DNS server is optional.
10. Click on **Next**. The **Summary** window displays. This stage is used to verify the connection properties.
11. Click **Finish** to validate the parameters. Click **Previous** to return to the previous screens

and modify the desired parameters.

To configure access to other ISP's, repeat the above procedure starting from the **Assistants** menu. So it is possible to create several connections to various ISP with different types of connection.

9.3.4 Managing Internet Connections

9.3.4.1 Operation

The management of Internet connections involves five main tasks:

- selecting the active profile,
- adding an Internet connection profile,
- deleting one or several Internet connection profiles,
- refining the Internet connection profile,
- testing the connection.

In order to access the **Connections Management**window, click **Connection** in the navigation bar. This window comprises two areas:

- The **Selecting the Active Connection Profile** area, which shows the active profile.
- The **Connection Profiles List** area, which shows the list of profiles managed by the system, as well as the active Internet connection.

9.3.4.1.1 SELECTING THE ACTIVE PROFILE

1. In the **Selecting the Active Connection Profile** area, select the active profile in the **Active Profile** drop-down list.
2. To activate the selected profile, click **Apply**.
3. In order to test the connection corresponding to the active profile, click **Test**. You access the test screen described in the "Test the Connection" section.

9.3.4.1.2 ADDING A CONNECTION PROFILE

In the **Connection Profiles" List** area, click **Add**. You access the first **Connection** assistant screen.

9.3.4.1.3 DELETING ONE OR SEVERAL CONNECTION PROFILES

You can only delete an inactive connection profile.

Deleting a connection profile

In the **Connection Profiles" List** area, click on the **Delete** hypertext link corresponding to the the profile you wish to delete.

Deleting several connection profiles

1. In the **Connection Profiles" List** area, select the profiles by checking the box next to the profile name.
2. Click **Delete the selection**.

9.3.4.1.4 REFINING THE ACTIVE PROFILE PARAMETERS

1. In the **Connection Profiles" List** area, click the profile name you wish to modify. The **Connection Settings** window is displayed.

   Remark 1:
   Depending on the selected connection (ISDN, DSL Modem, External Router or LAN Server), the tabs may be different. However, you still have access to tabs relating to profile, connection type, connection authentication, DNS and service quality (QoS).

2. Click on the **Profile** tab. This tab allows verifying or modifying the profile's characteristics.
3. Depending on the selected connection type, click the **DSL** or **ISDN** or **External Router** or **LAN Server** tab. This tab allows modifying the connection's characteristics.

   Remark 2:
   *In the **DSL** or **ISDN** tab, you may check the **Allow VJ (Van Jacobson) compression** box. It corresponds to the compression of the IP headers. Check that box if the ISP supports this function.*

4. Click the **Authentication** tab. This tab allows verifying or modifying the authentication's characteristics.
5. Click the **IP/DNS** tab. This tab allows modifying the DNS and the IP addresses" allocation characteristics.
6. Click the **QoS** tab. This feature allows you to activate or deactivate the Quality of Service (QoS) feature. By enabling this feature, you give priority to voice traffic on IP. The mechanism used is based on the principles given in the Diffserv standard. The system is based on a particular value of the "Type de service" field of the IP header of VoIP packets, which must be different from the value of the "best effort" field so that the QoS takes it into account. For further information refer to the on-line help. There are three possibilities:
   - Click **No QoS** if you do not wish to enable this function.
   - Click **QoS with predefined bandwidth** and select the value of the bandwidth of the Internet access from the dropdown menu.
   - Click **QoS with configured bandwidth**, if none of the predefined values is suitable, and indicate the value of the bandwidth of the internet access in the field. Select the unit for the bandwidth from the dropdown menu.
7. Click on **Apply** to validate the data or on **Cancel** if you do not wish to keep the changes.

9.3.4.1.5 TESTING THE CONNECTION

Click **Connection Test** in the general information banner or the **Test** button in the **Selecting the Active Connection Profile** area. The connection test runs all the stages involved in connecting to an ISP, and gives the causes and related solutions to solve the problem if the connection fails. The following tests are run in sequence:

- Initial state test: the system checks that the active ISP is in "Enabled" mode and that the connection can be established in the set time ranges.
- Call to the ISP's telephone number, or ping to the DSL modem, the Cable Modem and the Router.
- Authentication check: the system tests the authentication of the login and password in accordance with the protocol supported by the ISP (PAP/CHAP). This verification is performed during a connection using ISDN or DSL modem.
- IP address negotiation: the system sends back the IP addresses of Alcatel-Lucent OmniPCX Office Communication Server, and of the router on the IAP's premises. This negotiation is tested during a connection using ISDN, DSL Modem and Cable Modem type connection.

- Testing the remote address by pinging the ISP's router. This checks that the router is working properly.
- DNS configuration check: this test is used to verify that the DNS configuration entered in the system is correct and, if not, it is used to dynamically locate the DNS servers present on the IAP's premises.
- Resolution of the IP address for the URL "www.ietf.org": checks that DNS resolution is working correctly.
- DNS ping: this test is carried out if DNS resolution isn't working. It ascertains whether the problem is due to an incorrect IP address or to the DNS service itself.
- Ping on www.ietf.org: tests the accessibility of a site present on the Internet.

9.3.5 Configuring the Client Station

9.3.5.1 Configuration procedure

To be able to use Alcatel-Lucent OmniPCX Office Communication Server's shared Internet access, the client station must be configured. Modifications have to be made to the network (TCP/IP) configuration and the browser settings.

9.3.5.1.1 TCP/IP configuration

Alcatel-Lucent OmniPCX Office Communication Server is a routing element between LAN and Internet. Alcatel-Lucent OmniPCX Office Communication Server needs to be configured as the default gateway on the client station to access the Internet.

Example:

Configuring a Windows 98 client station

- Right-click the **Network neighbourhood** icon, and choose the **Properties** option from the context menu.
- In the **Network** window, double-click the **TCP/IP** icon under the **Configuration** tab.
- Enter Alcatel-Lucent OmniPCX Office Communication Server's IP address in the **New gateway** area (**Gateway** tab of the **TCP/IP properties** window).
- Click **Add** and then click **OK** to close the windows.
- Re-boot the client station to validate the changes.

Note:

This configuration is valid only if Alcatel-Lucent OmniPCX Office Communication Server is the main router in relation to the client station. For other network configurations, contact the company's system administrator.

9.3.5.1.2 Configuring the web browser

The web browser has to be configured to recognize the existing LAN.

Example:

Configuring Internet Explorer 5.0

- Run an Internet Explorer session.
- Choose **Internet Options...** in the **Tools** menu.

- Click the **Connections** tab of the **Internet options** window.
- Click **LAN settings...**
- Change the options in the **Local network (LAN) settings** window.
- Click **OK** to validate the changes.

Note:
If the proxy server is active on Alcatel-Lucent OmniPCX Office Communication Server, enter the IP address of the main CPU, otherwise enter the IP address of the client's proxy server.

9.4 Intranet

9.4.1 Overview

An Intranet is a set of Internet services internal to a local network, i.e. accessible only from a local network's station and hidden from the outside.

Integration of Alcatel-Lucent OmniPCX Office Communication Server in the LAN requires the following functions :

- management of domain names (DNS server),
- dynamic management of IP addresses (DHCP server).

Alcatel-Lucent OmniPCX Office Communication Server provides two services to the LAN users :

- Make accessible and publish Web pages (Web server).
- Share files between users (file server).

What follows is a general description of how these services and functions work, before dealing with their configuration in Alcatel-Lucent OmniPCX Office Communication Server.

9.4.2 Integration

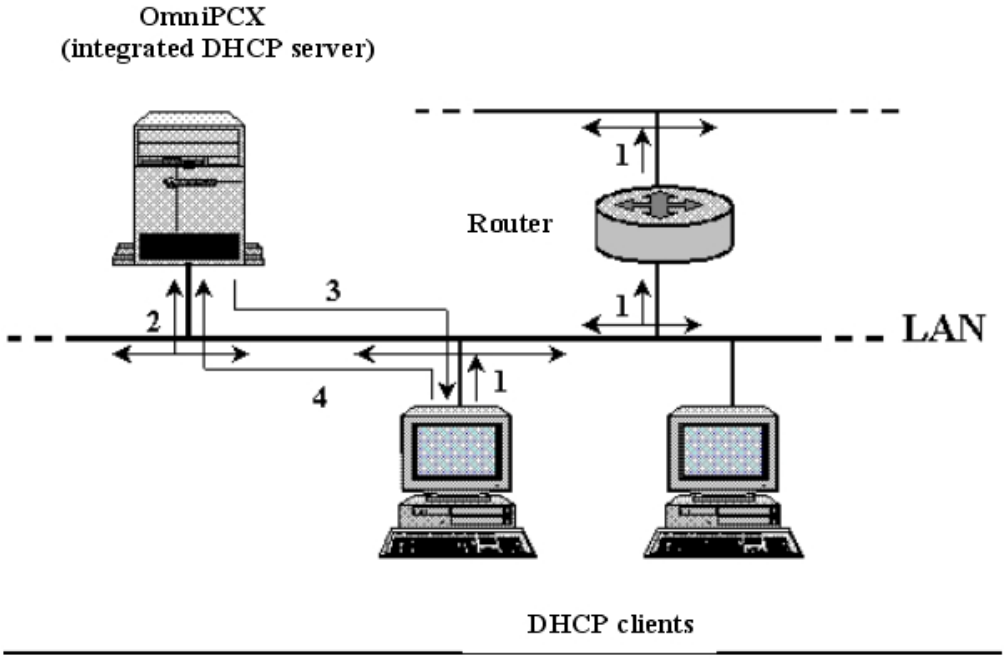
9.4.2.1 Detailed description

The internal network of a company, or LAN, comprises various elements such as servers, clients stations, routers, etc. To be effectively integrated into a LAN, these devices are subject to integration rules that govern the definition of an IP address plan, the adoption of domain names and naming conventions, etc.

Alcatel-Lucent OmniPCX Office Communication Server provides features that facilitate integration into a LAN, whatever topology it may present. These features correspond to name management (DNS) and dynamic management of IP addresses (DHCP server) services.

9.4.2.1.1 DHCP server

This server enables an IP address to be allocated dynamically on the LAN.



There are two types of IP address:

- public addresses: these addresses are unique on the Internet.
- private addresses: these addresses are assigned in a LAN, recognised in the LAN, but not routed on Internet.

Using private addresses in a LAN allows total freedom of choice in allocating addresses. A host name can have a fixed IP address, or it can be assigned one dynamically by a DHCP server each time it connects to the LAN. There are several stages in the LAN connection process (see diagram above):

1. the DHCP client connects up to the LAN, and requests an IP address allocation. This request is made by sending out ("broadcasting") a DHCP request over the LAN.
2. the DHCP server on the LAN receives the request and allocates an available IP address from the pre-defined range of addresses;
3. the allocated IP address is sent to the DHCP client;
4. the DHCP client accepts the IP address.

Alcatel-Lucent OmniPCX Office Communication Server provides DHCP server functionalities. The following parameters can be configured:

- The value range of IP addresses that the DHCP can allocate. These IP addresses are allocated for the network's computers and VoIP stations.
- The lifespan or "lease" of a dynamically allocated IP address.

When integrating into a LAN, two types of situation are encountered:

- **A DHCP server does not exist:** if a DHCP server is required, an address plan must be defined with a range of fixed addresses for the specific network elements (servers, printers, routers, etc.) and a range of DHCP-attributable addresses for the client stations.

- **A DHCP server already exists**. In this case Alcatel-Lucent OmniPCX Office Communication Server requires no particular DHCP configuration.

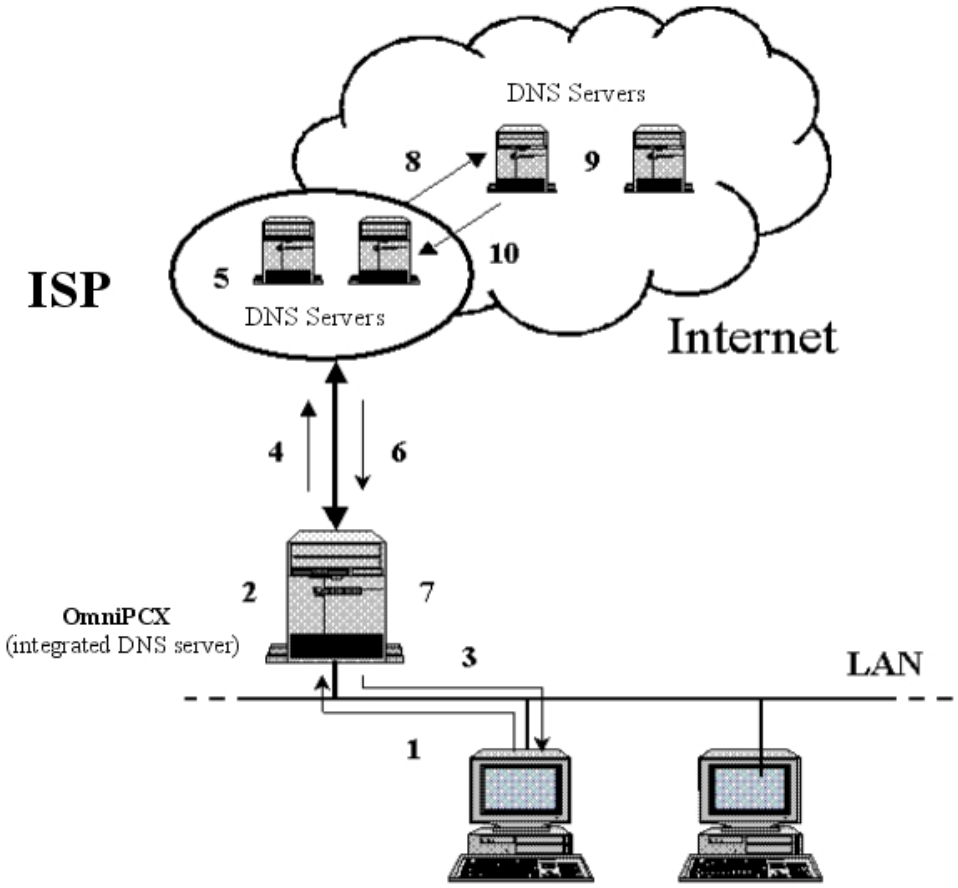
  Remark:
  LANs can accommodate more than one DHCP server, so long as their IP address ranges don't overlap.

9.4.2.1.2 DNS server

DNS servers handle the correspondence between an IP address and the host name of a machine. DNS servers perform two main functions:

- DNS caching for the resolution of names external to the LAN.
  The cache is updated whenever DNS servers other than Alcatel-Lucent OmniPCX Office Communication Server resolve a DNS request. This means that if an identical request is received, it can be resolved directly by Alcatel-Lucent OmniPCX Office Communication Server without calling on the DNS servers at the ISP. The request is thus resolved faster, with a corresponding reduction in communications costs. The Alcatel-Lucent OmniPCX Office Communication Server's DNS also has a negative cache for saving name resolution failures. The lifespan of the information in the cache is kept short so that the user can make a new attempt at resolving these names;
- Resolution of local host names with a fixed IP address on the LAN.
  These names are resolved provided the elements have been entered in Alcatel-Lucent OmniPCX Office Communication Server.

Resolving DNS requests from client stations involves several stages (see diagram):



- The client station emits a DNS request (Step 1).
- The host name - DNS server IP address correspondence table is consulted (Step 2). If the host name is found, the DNS server sends the corresponding IP address back to the client station (Step 3). If not, the request is relayed to the ISP's DNS servers (Step 4).
- The ISP's DNS servers are consulted. If the request is resolved, the servers send the corresponding IP address back to the DNS server on the LAN (Step 6). The LAN DNS server updates the DNS cache to take account of the request (Step 7), and proceeds from Step 3.
- If the request can't be resolved by the ISP's DNS servers, it is relayed to other DNSs on the Internet (Step 8). At this stage, the request is continuously relayed until a DNS server manages to resolve the host name (Step 9). The resolved IP address is then returned to the ISP's servers (Step 10), from whence it follows the same route as before.

9.4.3 LAN services

9.4.3.1 Overview

Alcatel-Lucent OmniPCX Office Communication Server provides two services to LAN users: a Web server and a file server.

9.4.3.1.1 Web Server

With its integrated Web server, Alcatel-Lucent OmniPCX Office Communication Server provides Intranet Web server functionality on the LAN. Only LAN elements have access to the Web server.

The two Intranet Web server functions are:

1. Allow access, for all LAN users, to the previously stored Web pages.
2. Publish, for the privileged users, static pages or pictures.

The Web pages comprise text files and picture files. To publish them, the Web pages text files must be transferred to the appropriate directories or files on the Web server. Three protocols are used:

- FTP (File Transfer Protocol): this protocol is used to transfer text files.
- CIFS (Common Internet File System): if you use the Windows systems" network neighbourhood.
- WebDAV (Web-Based Distributed Authoring and Versioning). This is an extension of the HTTP protocol that allows users to edit and manage collaborative files on Web sites. WebDAV is an IETF proposal for a standard (RFC 2518). Most Web sites" management tools are compatible with WebDAV. Under Windows, WebDAV is available through the "Web Folders". Contrary to FTP or CIFS, WebDAV manages file locks in order to avoid publishing conflicts between users.

The usual publishing tools such as Microsoft Office Frontpage, Adobe Golive or Macromedia Dreamweaver support these three protocols.

9.4.3.1.2 File server

A file server allows saving users" files on the local network and sharing them between users.

The main features of a file server include:

- centralized management of files,
- information sharing,
- private access to information from any LAN station.

The file server uses the CIFS protocol. With this protocol, a user is able to find one or several files on the network and to read or edit them. Editing is possible only if the file is not already open by another user.

9.4.4 Configuring Intranet

9.4.4.1 Configuration procedure

1. Connect the CPU card using an Ethernet cable:
   - Either to an available RJ45 socket on the company LAN;
   - Or to the internal switch in the Alcatel-Lucent OmniPCX Office Communication Server cabinet. This switch can then be connected to another switch if Alcatel-Lucent OmniPCX Office Communication Server has several switches.
2. If necessary, change the default IP addresses (192.168.92.246 for CPUe, 192.168.92.247 for CoCPU@) and the mask of the sub-network to IP addresses that are compatible with the existing LAN (for more information, contact the company's network and system

administrator). The IP addresses of the different cards can be accessed through the heading **OMC -> PCX Client -> Hardware and limits-> IP cards**.

3. Internet access configuration:
   - Either via the Internet navigator of a customer terminal connected to the LAN by entering the IP address of the CPU Main or CoCPU@ card in the address bar.
   - Or via the OMC software, from the **OMC -> PCX Client -> Internet access configuration** menu.

9.4.4.1.1 INTRANET CONFIGURATION

To configure the Intranet, click **Network** in the navigation bar. The **Network Parameters** window displays. This window consists of six tabs:

- **Intranet**
- **DNS**
- **DHCP**
- **Routing Table**
- **Dynamic DNS**

1. Click the **Intranet** tab. This tab displays the required information to publish on the Intranet site and to share files using Microsoft's network neighborhood.
   a. In the **Network Information** area, fill in the following fields:
      - **Host name of this system**: Give it a name to customize it. The default setting is *iaccess*.
      - **Workgroup or domain**: Allows you to integrate your server into a Microsoft network.
      - **WINS Server**: If your network is equipped with a WINS server, you can indicate its name. With this server, you can save domain names and therefore save the file server.

   b. In the **Intranet Publishing** area, choose the publishing protocol (with or without file locking) that you want to use to publish Web pages on your Intranet:
      - FTP and CIF (no locking)
      - WebDAV (locking)

   c. In the **Intranet Web site/file server** area, two hypertext links provide access to the Intranet server's Web pages or to the file server's files.

   d. Click **Apply** to accept the data, or click **Cancel** if you do not want to keep the changes.

2. Click the **DNS** tab. This tab displays the required information to configure your DNS server.
   a. In the **DNS** area, fill in the following field:
      - **DNS Domain Name**: Enter the internal domain name used on the LAN. The default setting is company.world.

   b. In the **New association name/IP address**area, you may add an entry in the associations" list. This list includes all the host names on the LAN with a corresponding fixed IP address. Each new item entered with its IP address and host name will be added to the Alcatel-Lucent OmniPCX Office Communication Server DNS table. To add an entry, fill in the following fields:
      - **IP Address**: fixed IP address of the host on the LAN.
      - **Name**: Name associated to this IP address.

   Then, click **Add**. The new configured item is added to the other associations already

defined. Repeat the operation as many times as there are associations to define. The new validated associations name / IP address can then be deleted by clicking **Delete**.

Important:
This list includes all the LAN hosts, except the DHCP clients.

c. Click **Apply** to accept the data, or click **Cancel** if you do not want to keep the changes.

3. Click the **DHCP** tab. This tab displays the required information to configure your DHCP server and define the ranges of IP addresses.
   a. In the **DHCP** area, fill in the following field:
   - **DHCP lease time**: The lapse of time after which an IP address assigned to a DHCP client that logs off is made available to another DHCP client. The shorter the lease time, the easier it will be to redistribute the IP address pool dynamically to the client stations.

   b. In the **New IP address range** area, you may add an entry to the list of IP address ranges assigned to the LAN items. These ranges are defined by a "begin" IP address and an "end" IP address. They are assigned to the computers, IP phone terminals and VPN clients. To add an entry, fill in the following fields as required:
   - **Begin IP range**: Enter the range's beginning IP address
   - **End IP range**: enter the range's ending IP address
   - **Type of range**: Select a range type from the drop-down list. Two choices are possible:
     - **Computer**: For attribution to PCs.
     - **VoIP Stations**: For IP telephone sets

   Click **Add** to accept. The newly configured range is added to those already defined; Repeat the operation as many times as there are ranges to define. After validation, ranges can be deleted by clicking **Delete**.

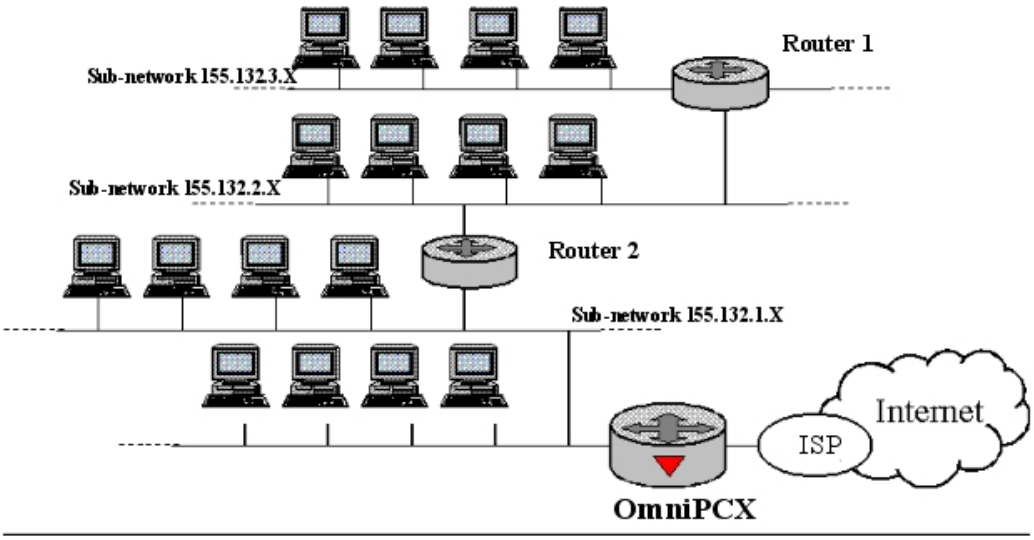
   c. Click **Apply** to accept the data, or click **Cancel** if you do not want to keep the changes.

4. Click the **Routing Table** tab. This tab displays the required information to configure Alcatel-Lucent OmniPCX Office Communication Server's routing table.
   a. In the **Routing Table** area, you may add an entry to the list of routes defined on your network. This routing table allows Alcatel-Lucent OmniPCX Office Communication Server to rout the various IP packets it receives towards their respective destinations (server or router in the LAN, PC, etc.). To add an entry, fill in the following fields:
   - **Destination**: Enter the destination's IP address after applying the subnet mask.
   - **Subnet mask**: Enter the subnet mask associated with the destination's address.
   - **Gateway**: enter the gateway's IP to be contacted in order to reach the destination's IP address.
   - **Type of access**: LAN only.
   - **Comment**: Comment for identifying the route entered.

   Click **Add** to accept. The newly configured route is added to those already defined. Repeat the operation as many times as there are ranges to define. After validation, ranges can be deleted by clicking **Delete**.

   b. Click **Apply** to accept the data, or click **Cancel** if you do not want to keep the changes.

   Example:
   Configuration of the routing table with three subnets present on the LAN.



In the architecture corresponding to the previous diagram, routers 1 and 2 must be entered into the Alcatel-Lucent OmniPCX Office Communication Server routing table in order to reroute the requests for destinations other than the Internet to the LAN. Two entries should be added to the "Additional Routes" table:

- One route for the 155.132.2.0 subnet with the following entries: 155.132.2.0 (Destination), router 2 IP address (Gateway), 255.255.255.0 (Mask).
- One route for the 155.132.3.0 subnet with the following entries: 155.132.3.0 (Destination), router 1 IP address (Gateway), 255.255.255.0 (Mask).

5. Click the **Dynamic DNS** tab. This tab displays the required information to configure your Dynamic DNS.
   a. In the **Choice of current ASP** area, select the ASP profile you want to use from the drop-down list. Three types of operation are possible:
   - If you select an ASP profile, the field **Current ASP Parameters** must be filled in.
   - If you select **Generic**, the field **Generic ASP Parameters** must be filled in.
   - If you select **None**, no field displays.

   b. In the **Current ASP Parameters** area, fill in the following fields:
   - **Domain Name**: Enter the domain name registered with the ASP.
   - **Account Name**: Enter the account name provided by the ASP.
   - **Password**: Enter the password provided by the ASP.
   - **Confirm the password**.

   c. In the **Generic ASP Parameters** area, fill in the following field:
   - **URL**: The generic ASP uses our standard method to update the host's IP address. The update requests are sent back to the entered URL.

   d. Click **Apply** to accept the data, or click **Cancel** if you do not want to keep the changes.

9.4.5 Configuring the Client Station

9.4.5.1 Configuration procedure

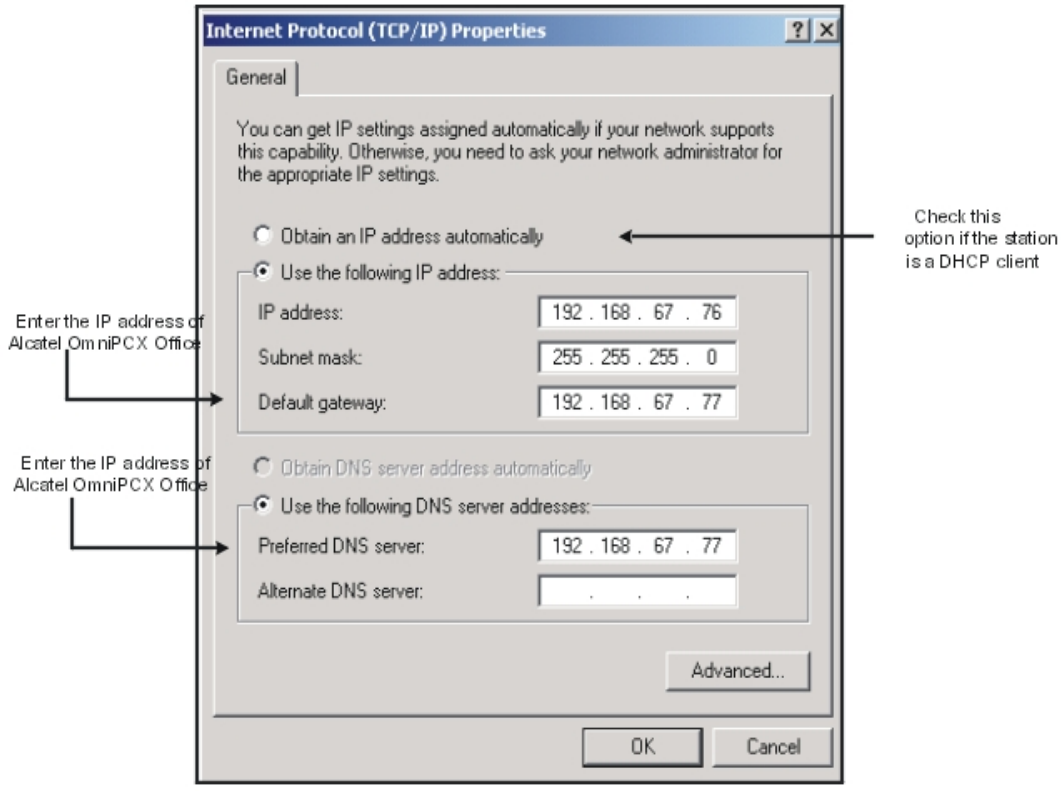
To bring in the Alcatel-Lucent OmniPCX Office Communication Server's LAN services, you have to change the TCP/IP configuration on the client stations. at two levels:

- reconfiguration as DHCP client.
  This is only necessary where there was no DHCP server on the LAN beforehand and Alcatel-Lucent OmniPCX Office Communication Server is configured as a DHCP server. If the client station keeps a fixed IP address, then the Alcatel-Lucent OmniPCX Office Communication Server's IP address must be entered as the default gateway.
- Insertion of the domain name and of the Alcatel-Lucent OmniPCX Office Communication Server's IP address as the DNS service.

Example:

Configuring a Windows XP client station

1. In the control panel, click on the **Network Connections** icon.
2. Right-click on **Local Network Connection** .
3. Choose **Properties** from the context-sensitive menu that pops up.
4. Double-click on **Internet Protocol (TCP/IP)**
5. Modify the settings as shown below.
6. Close the windows by clicking **OK** .
7. Reboot the computer to register the modifications.



9.5 VPN

9.5.1 Overview

A virtual private network extends to a private network incorporating one or more public network links such as the Internet. These links maintain the characteristics of a private point-to-point link by encapsulating data by means of tunneling protocols. Authentication methods are used to maintain the security of the private network. The confidentiality of the data carried by these links is guaranteed by ciphering methods. The idea behind is to offer companies exactly the same services as a private link at far less cost by utilizing a public infrastructure.

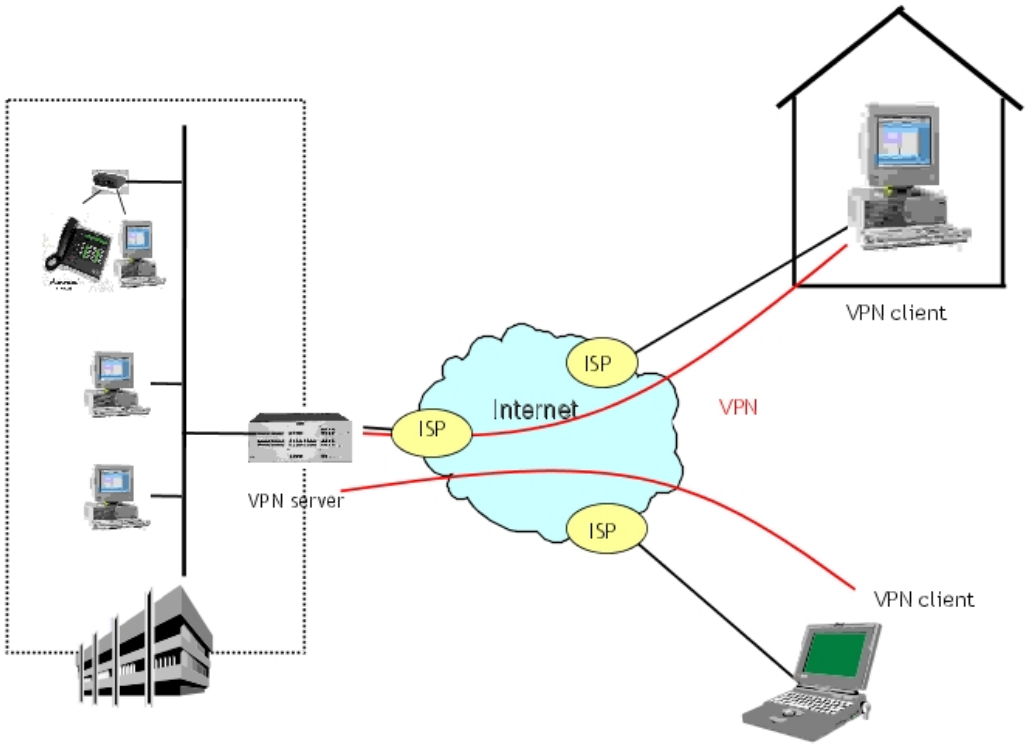
Alcatel-Lucent OmniPCX Office Communication Server offers two types of VPN:

- A remote-access VPN connection called "VPN Client to LAN"
- A router-to-router VPN connection called "VPN LAN to LAN"

9.5.1.1 VPN Client to LAN

9.5.1.1.1 Description

The remote user can connect up to the company LAN from fixed or mobile terminals. In this case, the user logs on to the Internet via the nearest point of presence and requests the creation of a VPN tunnel between his terminal and OmniPCX Office.



Security of exchanges is insured at several levels and by several features, such as data

encryption, authentication at both ends and monitoring of user access to resources.

For the creation and management of a tunnel both the client and the server must implement the same protocol. Three types of protocols are supported by Alcatel-Lucent OmniPCX Office Communication Server:

- the PPTP protocol (Point to Point Tunneling Protocol). It is a data link layer protocol on the OSI (Open Systems Interconnection) model.
- The L2TP protocol (Layer 2 Tunneling Protocol). It is also a data link layer protocol on the OSI.
- The IPSec protocol (IP Security Protocol). It is an OSI model network layer protocol. This protocol provides, between the clients and the server (IKE), key exchange, IP packets ciphering (ESP) and data authentication (AH and ESP) services.

When the VPN client issues a connection request, the authentication protocol, client IP address and data encryption method can all be negotiated with the VPN server (depending on the protocol used).

9.5.1.1.2 VPN clients

The remote user is termed the "VPN client" and OmniPCX Office the "VPN server". In all cases, the user must belong to the "Teleworkers" group or a group with "remote rights". Three types of clients are supported by Alcatel-Lucent OmniPCX Office Communication Server:

- the PPTP client,
- the client called other IPSec client, and
- the Microsoft IPSec client.

PPTP client

The PPTP client uses the PPTP protocol to protect connection tunnels created in order to establish a VPN. In this configuration, it seems that the client belongs to the LAN.

- Authentication
  The protocol proposed by Alcatel-Lucent OmniPCX Office Communication Server is MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) version 2. Unless the client can provide this type of authentication, connection will be refused.
- Client IP address
  The IPCP (Internet Protocol Control Protocol) negotiation process with the VPN server assigns an intranet IP address to the client. This address is configured beforehand in OmniPCX (see "Configuration for Alcatel-Lucent OmniPCX Office Communication Server").
- Data encryption
  The data ciphering method used by OmniPCX Office is MPPE (Microsoft Point to Point Encryption) with continuous RSA RC4 encoding and 40-bit or 128-bit ciphering keys. Connection attempts will be rejected if the client cannot use these methods.
- Data tunneling
  After the data have been encrypted, a PPP header is added to create the PPP frame. The latter is then encapsulated with a modified GRE header (Generic Routing Encapsulation RFC 1701 and 1702). The resulting frame is itself encapsulated with an IP header.

Microsoft IPSec client

The Microsoft IPSec client is integrated in Windows from the XP release. For the 98, NT and

Millennium releases, the client can be downloaded from the Microsoft site. This approach makes it possible to secure client/gateway remote access on the Internet by means of:

- the L2TP protocol for data tunneling,
- IPSec which guarantees confidentiality and data integrity by encrypting traffic.

The services provided by L2TP are user authentication and assignment of IP addresses to the client. Since this protocol is based on the PPP protocol, authentication (up to user level) is ensured by the MS-CHAP protocol version 2 (Microsoft Challenge Handshake Authentication Protocol version 2) and the client's IP addressing by IPCP (Internet Protocol Control Protocol).

IPSec provides data integrity, data origin authentication and confidentiality services as defined in the Other IPSec client section.

Other IPsec client

"Other IPSec client" refers to any client using IPSec for data tunneling and encryption. This gives the tunnel a very high level of security.

The security services are:

- data integrity,
- data origin authentication, and
- confidentiality.

The IPsec standard defines two extensions to the IP protocol to provide these services: AH (Authentication Header) for data integrity and authentication, and ESP (Encapsulating Security Payload) for data integrity and authentication and confidentiality.

Alcatel-Lucent OmniPCX Office Communication Server only supports ESP. Data confidentiality is provided by the ciphering algorithms DES, 3DES and AES. Data authentication and integrity use the algorithms HMAC-MD5 and HMAC-SHA-1.

When the IPsec connection is established, the machines authenticate each other thanks to:

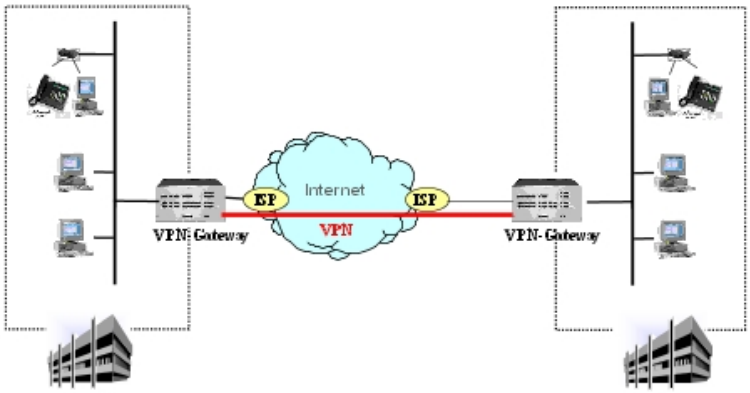
- The Pre-Shared secret key(PSK) method
- The public keys method. Using PKI (Public Key Infrastructure), public keys management system, makes the administrator's task easier (for more information, see the PKI section)

In certain cases, it is preferable to also perform an authentication of the user. To do this, Alcatel-Lucent OmniPCX Office Communication Server supports the extended authentication method (Xauth). The user must then enter his/her user name and password.

9.5.1.2 VPN LAN to LAN

9.5.1.2.1 Description

The idea behind a LAN VPN-to-LAN is to provide a secure connection between two remote sites while using a shared or public infrastructure. It utilizes a router-to-router connection on which all packets are encrypted and secured using negotiated methods.



The tunneling protocol used by Alcatel-Lucent OmniPCX Office Communication Server is IPSec (Internet Protocol Security, RFC 2401 2402 2406). This is a network layer protocol based on the OSI model (Open Systems Interconnection), whose principle consists in encrypting the IP packets and then encapsulating them in an additional IP header before sending them to an IP network.

In the case of a VPN LAN to LAN, security services offered by IPSec are the same as those presented in the "VPN Client to LAN" section. It is important to note that Alcatel-Lucent OmniPCX Office Communication Server allows:

- to secure either the whole LAN or part of the LAN,
- to manually configure security profiles according to the remote entity to insure a better interoperability.

9.5.2 Security Profiles

9.5.2.1 Overview

For all VPN connections using IPsec, the IKE protocol (Internet Key Exchange) is used to negotiate security settings, authenticate the systems and compute the data integrity and authentication keys.

The IKE protocol involves two negotiation phases that establish two Security Associations (SA). One SA groups all the security parameters (algorithms, keys, IP addresses) protecting a given connection (for more information, see the "Interoperability with other IPSec gateways" section). For each SA, the IKE protocol allows a system to send several propositions to the remote entity. These proposals are combinations of the ciphering, hashing and key computation algorithms.

There are then two possible cases:

- the remote entity selects the first proposition that meets its criteria and the connection is established,
- no proposition is selected and the negotiation fails.

The list of propositions for both SA (ISAKMP and IPSEC SA) is stored in the user-configured security profiles.

When configuring a VPN LAN to LAN, the administrator selects the security profile to use.

The Microsoft L2TP/IPsec clients and other IPsec clients must use the predefined profile, called "IPsec client".

Remark:
Alcatel-Lucent OmniPCX Office Communication Server implements the "traversal NAT" function, which makes it possible to establish IPsec VPN's via devices that modify the systems' IP addresses. This function does not require any configuration. Detection of the NAT and negotiation of use of this mechanism are performed automatically during establishment of the connection.

9.5.3 PKI Management System

9.5.3.1 Detailed description

PKIs (Public Key Infrastructure) are a public key management system used to manage important lists of public keys and to ensure their reliability. A PKI infrastructure provides the following services:

- manufacturing of public keys,
- certification of public keys and publication of digital certificates,
- revocation of certificates,
- management of the certification function.

9.5.3.1.1 CERTIFICATE

On administrator demand, the certification authority issues a digital certificate associating a public key with the identity of a user or a system. The public key on the certificate corresponds to a confidential private key, known only to the holder of the certificate. The data encrypted with the private key can only be decrypted by the corresponding public key, and vice-versa. This makes it possible to provide the electronic signature service used for VPN authentication.

Certificates must be obtained during system configuration. The VPN client and the VPN server request certification from the same certification authority. The certificates are exchanged during the IKE negotiation to allow the systems to verify the remote electronic signature. If this verification is successful, establishment of the connection is authorized.

Alcatel-Lucent OmniPCX Office Communication Server supports two methods for obtaining a certificate:

- **The "off-line" or manual method**: the certificate request is stored in a PKCS#10 format file. The administrator must submit this file to the certification authority. The certification string containing the CA's certificate and the system's certificate must then be imported manually into Alcatel-Lucent OmniPCX Office Communication Server.
- **The "on-line" or automatic method**: the SCEP protocol (Simple Certificate Enrolment Protocol) is used to submit the certificate request to the certification authority, and the certification string is recovered and automatically installed.

Regardless of the method used, the key pair is automatically generated on the system before the certificate request is sent.

Since certificates are not renewed automatically, the administrator must request a certificate again before the current certificate's period of validity ends.

Remark:
The whole of the certification string must be imported into the system. It will not be possible to verify a

certificate if the certificate of an intermediate authority or the certificate of the root CA are not found.

The certificates and keys are stored on protected files and are therefore linked to a CPU. If the board is changed, the certificate must be requested again.

Alcatel-Lucent OmniPCX Office Communication Server supports certificate revocation lists (CRL). They are regularly updated by the certification authorities and contain the list of certificates that must not be accepted (e.g. because the holder has left the company). These lists can be imported into the system manually or automatically, and will be scanned when a VPN is established to verify the validity of the remote system's certificate.

9.5.3.1.2 PKI ACCESS CONTROL LISTS (ACL)

VPN access control lists (ACL) are used for certificate-based authentification. They allow the administrator to manage authorization of access to the VPN service. This is particularly necessary in cases of a PKI where the certification authority is used to issue certificates for several different uses (for example, VPN or protection of e-mail), or for several enterprises (PKI managed by a services supplier). This control is not however necessary when the certification authority issues certificates only within the scope of the enterprise and for the VPN service. In this case, verifying the validity of the certificate is sufficient.

Access control is based on filters which are applied to the **Identity** field of the certificate presented by the remote access. These filters can specify all or part of a distinctive name X.500, and can be used, for example, to authorize access only for the personnel in the Marketing Department of enterprise ABC located in France (ou=Marketing, o=ABC, c=fr).

ACL MANAGEMENT

ACL DEFINITION

1. In order to access the **ACL management**window, click **VPN/RAS** in the navigation bar. The **VPN/RAS management** window opens, click on the **ACL management** link to display the ACL lists.
   This window shows the ACLs defined and the type of action which can be performed.

   Remark 1:
   *click **Delete** to delete an ACL.*

2. Click **Add** to set the parameters of a new ACL. A new window appears with the tabs **Identification** and **Description**.
   - **Identification**: used to give the ACL a name. This name is used by the administrator to identify the ACL. It is taken into account by the IPSec client, or by the Tunnel configuration if authentification is certificate-based. Enter the name of the ACL.
   - **Description** : used to define one or more filters. A filter is made up of a list of one or more attribute/value pairs, for example "o=EnterpriseName, c=fr". Access will be authorized if the **Identity** field of the certificate of the remote system contains all the attribute/value pairs specified in one of the ACL filters.

     Remark 2:
     *missing attributes can be added by listing them, and then clicking **Add** to confirm them.*
     A complete identity does not have to be specified.

     Example:
     the filter "o=EnterpriseName, c=fr" will authorize access to all the certificates issued for EnterpriseName in France, for example, certificates of which the identity is "cn=Jean Dupont, ou=Marketing, o=EnterpriseName, c=fr" or "cn=John Smith, ou=Research, o=EnterpriseName, c=fr".

ACL SELECTION

ACLs can be used for site-to-site tunnels and IPSec VPN clients.

Selecting an ACL for site-to-site VPN configuration

1. Click on**VPN/RAS** in the navigation bar.
2. In the **Site-to-site IPSec tunnel**, click on the name of the tunnel to be configured.

   Remark 1:
   the tunnel must be created first.
3. In the **Authentification** tab, click on **Certificate**, then select an ACL from the suggested list.

Selecting an ACL for an IPSec client VPN

1. Click on**VPN/RAS** in the navigation bar.
2. In the **Remote access services** area, click **IPSec**. The **IPSec client parameters** window appears.

   Remark 2:
   the support of IPSec VPN clients must be configured first before the parameters can be accessed.
3. In the **Authentification** tab, click on **Certificate**, then select an ACL from the suggested list.

   Remark 3:
   all IPSec clients will share the same ACL.

9.5.4 Configuring

9.5.4.1 Configuration procedure

Click on **Wizards** in the navigation bar. The assistants' icons appear.

1. Click on the **VPN Wizard** icon. The **VPN Tunnel Wizard** window appears.
2. Enter the name of the tunnel you are creating.
3. Click on **Next**. A new window appears.
4. In the **Remote Settings** area, fill in the following field:
   - **Public IP Address**: IP address provided by the remote entity.
   - **Remote Subnet**: enter an IP address or an IP address and a subnet mask.
5. In the **Security Profile** area, select the required security profile in the drop-down menu.
6. Click on **Next**. A new window appears.
7. The **Authentication Mode** is used to define the authentication mode used during the data tunneling. There are two possibilities:
   - **Pre-Shared Key (PSK)**. In this case, the following fields must be filled in:
     - **Secret key value**
     - **Key confirmation**
   - **Certificate**
8. Click on **Next**. The **Summary** window appears, showing the various characteristics of the tunnel you have created.

9. Click on **Finish**.

9.5.4.1.1 CONFIGURATION OF VPN CLIENT SUPPORT

Click on **Wizards** in the navigation bar. The assistants' icons appear.

1. Click on the **VPN Client Wizard** icon. The **VPN Client Wizard** window appears.
2. Select the type of client you want to create, by clicking on:
   - **PPTP protocols** to configure support for PPTP clients.
   - **IPSec protocols** to configure support for Microsoft IPSec clients or other IPSec clients.

- **Configuration of PPTP client support**

1. In the **New IP address range** area, if no IP range is defined for the PPTP client, fill in the following fields:
   - **Start of IP range**: start of the IP range allocated to VPN clients.
   - **End of IP range**: end of the IP range allocated to VPN clients.

   Remark 1:
   If a range is already created, the following window is accessed directly.
2. Click on **Next**. A new window appears.
3. In the **Microsoft LAN integration** area, if your LAN is equipped with a WINS server, enter its IP address.

   Remark 2:
   If a WINS server address has already been configured in the system, the following window appears directly.
4. Click on **Next**. The **Summary** window appears, showing the various characteristics of the PPTP client you have created.
5. Click on **Finish**.

- **Configuration of IPSec client support**

In this case, you can configure:

- another single IPSec client.
- a single Microsoft IPSec client.
- a Microsoft IPsec client and another IPSec client.

1. Configuration of "other IPSec client" support
   a. In the **Supported IPSec client protocols** area, check the **Other IPSec clients** box only.
   b. Click on **Next**. A new window appears.
   c. The **Authentication Mode** is used to define the authentication mode used during the data tunneling:
      - **Certificate**
      - **Pre-Shared Key (PSK)**. In this case, fill in the **Secret Key Value** and **Confirm Secret Key Value** fields.

        Remark 3:
        The choice is not exclusive. You can choose one of the authentication modes or both of them.

d. Click on **Next**. The **Summary** window appears, showing the various characteristics of the other IPSec client you have created.

e. Click on **Finish**.

2. Configuration of Microsoft IPSec client support

a. In the **Supported IPSec client protocols** area, check the **Microsoft IPSec client (L2TP over IPSec)** box only.

b. In the **New IP address range** area, if no IP range is defined for the other Microsoft IPSec client client, fill in the following fields:

- **Start of IP range**: start of the IP range allocated to VPN clients.
- **End of IP range**: end of the IP range allocated to VPN clients.

Remark 4:
If a range is already created, the following window is accessed directly.

c. Click on **Next**. A new window appears.

d. In the **Microsoft LAN integration** area, if your LAN is equipped with a WINS server, enter its IP address.

Remark 5:
If a WINS server address has already been configured in the system, the following window appears directly.

e. Click on **Next**. A new window appears.

f. The **Authentication Mode** is used to define the authentication mode used during the data tunneling:

- **Certificate**
- **Pre-Shared Key (PSK)**. In this case, fill in the **Secret Key Value** and **Confirm Secret Key Value** fields.

Remark 6:
The choice is not exclusive. You can choose one of the authentication modes or both of them.

g. Click on **Next**. A new window appears.

h. Click on **Next**. The **Summary** window appears, showing the various characteristics of the IPSec client you have created.

i. Click on **Finish**.

3. Configuration of support for Microsoft IPSec clients and "other IPSec Client" clients at the same time

a. In the **Supported IPSec client protocols** area, check the **Microsoft IPSec client (L2TP over IPSec)** and **Other IPSec clients** boxes.

b. In the **New IP address range** area, if no IP range is defined for the other Microsoft IPSec client client, fill in the following fields:

- **Start of IP range**: start of the IP range allocated to VPN clients.
- **End of IP range**: end of the IP range allocated to VPN clients.

Remark 7:
If a range is already created, the following window is accessed directly.

c. Click on **Next**. A new window appears.

d. In the **Microsoft LAN integration** area, if your LAN is equipped with a WINS server, enter its IP address.

Remark 8:
If a WINS server address has already been configured in the system, the following window appears directly.

e. Click on **Next**. A new window appears.

f. The **Authentication Mode** is used to define the authentication mode used during the data tunneling:

- **Certificate**
- **Pre-Shared Key (PSK)**. In this case, fill in the **Secret Key Value** and **Confirm Secret Key Value** fields.

Remark 9:
The choice is not exclusive. You can choose one of the authentication modes or both of them.

g. Click on **Next**. A new window appears.

h. In the **IPSec** area, check the **Use extended authentication** if you want to use a reinforced authentication.

i. Click on **Next**. The **Summary** window appears, showing the various characteristics of the Microsoft IPSec client clients and of the other IPSec client you have created.

j. Click on **Finish**.

9.5.5 Managing a VPN

9.5.5.1 Operation

VPN management comprises two main tasks:

- VPN clients administration, comprising:
  - management of the PPTP client service,
  - management of IPSec clients,
  - remote access configuration.
- Tunnel administration, comprising:
  - modifying a tunnel's properties,
  - adding one or several tunnels,
  - deleting one or several tunnels,
  - testing a tunnel.

Caution:
If the tunnel-initiating gateway is deemed to be the VPN client and the remote gateway the VPN server, then the Internet connection (if used) on the server side must be a "Callback" or "Permanent" connection with a fixed IP address. No such restrictions apply on the client side. However, if both sides happen to initiate the VPN tunnel, then the restriction applies to them both.

In order to access the **VPN/RAS Management**window, click **VPN/RAS** in the navigation bar. This window comprises two areas:

- The **Remote Worker Services** area, with three hypertext links giving access to the **VPN Client** wizard for creation of PPTP or IPSec clients.
- The **Site to site IPSec tunnels** area, which lists already created tunnels.

9.5.5.1.1 MANAGING THE PPTP CLIENT SERVICE

1. In the **Remote Worker Services** area, select **PPTP**. The **PPTP Client Settings** window appears. This page comprises two tabs: **Activation** and **IP Range**.
2. Click on the **Activation** tab. In the **Service activation/deactivation** area, check the **PPTP Client** box in order to activate the service.
3. Click on the **IP Range** tab. This tab is used to define a new IP address range.
   a. In the **New IP address range** area, fill in the following fields:
   - **Start of IP range**: start of the IP range allocated to VPN clients.
   - **End of IP range**: end of the IP range allocated to VPN clients.

   b. Click **Add**. The range thus created appears in the table located under the **New IP address range** area.
   c. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

9.5.5.1.2 MANAGING IPSec CLIENTS

1. In the **Remote Worker Services** area, select **IPSec**. The **IPSec Client Settings** window appears. This page comprises several tabs: **Activation**, **Authentication**and **IP Range** and **IPSec**.

   Remark 1:
   *The **IPSec** tab is only accessible if support for the other IPSec clients is activated.*
2. Click on the **Activation** tab. This tab is used to activate or deactivate support for the proposed client protocols.
3. Click the **Authentication** tab. This tab is used to define the authentication mode to use for data tunneling:
   - **Certificate**
   - **Pre-Shared Key (PSK)**. In this case, fill in the **Secret Key Value** and **Confirm Secret Key Value** fields.

     Remark 2:
     The choice is not exclusive. You can choose one of the authentication modes or both of them.
4. Click on the **IP Range** tab. This tab is used to define a new IP address range.
   a. In the **New IP address range** area:
   Complete the following fields:
   - **Start of IP range**: start of the IP range allocated to VPN clients.
   - **End of IP range**: end of the IP range allocated to VPN clients.

   Select **Range type**, **IPSec client** or **L2TP client** in the drop-down menu.
   b. Click **Add**. The new range is added to the others in the table. Restart the operation for each range to define.
5. Click on the **IPSec** tab. This tab is used to activate the following options:
   - **Local Settings**
   - **Remote Settings**
   - **Extended Authentication**

   a. The **Local Settings** are is used to modify the part of the LAN the client will have access to, or else to force the client to send all its traffic in the VPN. This option prevents access to the public network when the client is connected to its company. The security of the local network is reinforced. Select:
   - **Restrict traffic to a sub-network** to restrict traffic to a specific sub-network. Fill in

the **Local Subnet** field

- **Use this system as the client's default gateway** to force all traffic through Alcatel-Lucent OmniPCX Office Communication Server for security reasons.

b. In the **Remote Settings** area, check the **Assign a private address to the client** box so that Alcatel-Lucent OmniPCX Office Communication Server automatically assigns an IP address from the company's LAN for the duration of the connection. It is then necessary to configure a range of "IPsec client" IP addresses.

Remark 3:
The client must support the "ISAKMP Configuration Method" extension

c. In the **Extended Authentication** area, check the **Use extended authentication** box to activate the option. The client must enter his/her name and password to establish the connection.

Remark 4:
The client must support the extended authentication method (Xauth).

9.5.5.1.3 REMOTE ACCESS CONFIGURATION

In the **Remote Worker Services** area, select **RAS**. The **RAS Wizard** appears. For more information, consult the "RAS" section.

9.5.5.1.4 MODIFYING A TUNNEL'S PROPERTIES

1. Click on the tunnel name. The **VPN Tunnel Settings** window appears. This page comprises several tabs: **Identification**, **Security** and **Authentication**.
2. Click on the **Identification** tab. This tab is used to verify or modify the tunnel's name.
3. Click on the **Security** tab. This tab is used to verify or modify the tunnel's security parameters.
   a. In the **Local Settings** area, fill in the **local Subnet** field by entering an IP address or an IP address and a subnet mask or * to authorize all sources.
   b. In the **Remote Settings** area, fill in the following field:
   - **Public IP Address**: IP address provided by the remote entity.
   - **Remote Subnet**: enter either an IP address or an IP address and a subnet mask.

   c. In the **Security Profile** area, select the required security profile in the drop-down menu.
4. Click the **Authentication** tab. This tab is used to verify or modify the tunnel's authentication parameters.
   a. In the **Authentication Mode** area, check the box:
   - **Certificate**
   - **Pre-Shared Key (PSK)**. In this case, fill in the **Secret Key Value** and **Confirm Secret Key Value** fields.
5. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

9.5.5.1.5 ADDING A TUNNEL

Click on **Add** in the list of tunnels or click on the **VPN Client Wizard** icon.

9.5.5.1.6 DELETING ONE OR SEVERAL TUNNELS

Deleting a tunnel

Click the corresponding **Delete** hypertext link.

Deleting several tunnels

1. Select the tunnels by checking the box preceding the tunnel's name.
2. Click **Delete the selection**.

9.5.5.1.7 TESTING A TUNNEL

Click the corresponding **Test** hypertext link.

9.5.6 Managing Security Profiles

9.5.6.1 Operation

- modifying a profile,
- adding one or several profiles,
- deleting one or several profiles,

To access the **Security Profile Management** window:

1. Click on**VPN/RAS** in the navigation bar. The **VPN/RAS Management** window appears.
2. Click on the **Security Profile Management** hypertext link in the **VPN/RAS Management** window. The **Security Profile Management** window appears. This windows consists of a table listing all the existing profiles.

Remark:
By default, three profiles (IPSec client, Standard Security and High Security) are pre-configured. The IPSec client profile is non erasable and the Standard Security and High Security clients are only erasable if they are not used by a tunnel or a client.

9.5.6.1.1 MODIFYING A PROFILE'S PROPERTIES

1. Click on the profile name. The **Security Profile Settings** window appears. This page comprises several tabs: **Identification**, **ISAKMP SA** and **IPSec SA**.
2. Click on the **Identification** tab. This tab is used to verify or modify the security profile's name.
3. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.
4. Click on the **ISAKMP SA** tab. This tab is used to configure the ISAKMP SA (Security Association), which is used to secure the connection between the two gateways. This parameter is used during phase 1 of the IKE protocol. For each SA, one must define the type of ciphering, the integrity algorithm, the Diffie Helmann group and the SA lifetime. In the **Phase 1: ISAKMP** area, you can:
   - Create a new proposition by clicking on **Add** and selecting the protocols used from the drop-down menus. Then, click on **Apply** to validate the data. The new ISAKMP SA thus created is added to the list.
   - Delete an existing proposition by clicking on the **Delete** hypertext link corresponding to the ISAKMP SA you want to delete. This ISAKMP SA is automatically deleted from the list.
   - Change the propositions order of submission for approval by clicking on the up or

down arrows.

5. Click on the **IPSec SA** tab. This tab is used to configure the IPSEC SA security association, which is established during phase 2 of the IKE protocol. This security association is used to convey information in a secure way between both LANs. This tab consists of two areas:
   - the **Pfs** area which is used to activate "Perfect forward secrecy".
   - the **Phase 2: IPSec SA** which is used to define the type of ciphering, the integrity algorithm, the Diffie Helmann group and the SA lifetime.
6. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

9.5.6.1.2 ADDING A PROFILE

Click on **Add** in the list of security profiles. The **Security Profile Management** window is accessed directly. To define the new security profile, fill in the **Identification**, **ISAKMP SA** and **IPSec SA** tabs, as explained above.

9.5.6.1.3 DELETING ONE OR SEVERAL PROFILES

Important:

The IPSec client client cannot be erased and the Standard Security and High Security clients are only erasable if they are not used by a tunnel or a client.

Deleting a profile

Click the corresponding **Delete** hypertext link.

Deleting several profiles

1. Select the profiles by checking the box preceding the profile's name.
2. Click **Delete the selection**.

9.5.7 Managing PKI Lists

9.5.7.1 Operation

PKI list management comprises several main tasks:

- modifying PKI parameters;
- adding a new certificate,
- managing revocation and certificate lists.

In order to access the **PKI Management**window, click **PKI** in the navigation bar. This window comprises three areas:

- The **Certificates** area displays a list of all the certificates in existence or awaiting authorization.
- The **Certificate Revocation Lists** area displays the list of revoked certificates, regularly updated by the certification authorities.
- The **Import a new PKI file** area which is used to import a new file.

9.5.7.1.1 ADDING A NEW CERTIFICATE

1. In the **Certificates** area, click on **Enrol**. The **Enrolment** window appears.
2. In the **Distinguished name** area, fill in the following fields to obtain a certificate name:
   - **Common name**: enter, for example, the product name.
   - **Unit**: enter, for example, the name of your service.
   - **Organization**: enter, for example, the name of your organization.
   - **Country**: enter your country's initials (as defined in the ISO 3166 standard).
3. In the **Enrolment method** area, two methods are available to import a new certificate:
   - **Offline Enrolment**: a file, containing the information required for obtaining a certificate, is saved an a floppy disk or on the hard disk. This file is then sent on the site of a certification authority. When the certificate is obtained, it is imported in Alcatel-Lucent OmniPCX Office Communication Server.
   - **Online Enrolment**: the new certificate is directly requested from the certification authority via the Internet.

     Remark 1:
     *In this case you have access to the additional tabs **Protocol** and **Certificate**.*

   a. Complete the following fields:
   - **CA's URL**: enter the certification authority's URL.
   - **CAMD5 Print**: this field is optional. The CAMD5 print enables the system to verify the authenticity of the CA's certificate.
   - **Password**: this field is optional. If you have obtained a password, the certificate delivery will be quicker.

   b. Click on the **Protocol** tab. This tab is used to change the advanced parameters of the certification authority's server, if there is an interoperability problem with the CA.

   Remark 2:
   For any change, consult your CA's administrator.

   c. Click on the **Certificate** tab. This tab is used to add SubjectAltName and Key use extensions to the certificate request, if required by the certification authority.

   Remark 3:
   For any addition, consult your CA's administrator.
4. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

9.5.7.1.2 MANAGING CERTIFICATE REVOCATION LISTS

1. Click on the **PKI** hypertext link, the **PKI CRL Settings** window appears. This window has several tabs: **CRL Settings**, **Notifications**.
2. Click on the **CRL Settings** tab. This tab is used to configure the settings of certificate revocation lists.

   a. In the **CRL Usage** area, there are three possible choices:
   - **Use valid CRL only**
   - **Use CRL even if expired**
   - **Do not use CRL**

   Important:
   It is however recommended to check the Use valid CRL only box in order not to reduce security.

   b. In the **CRL update mode** area, there are three possible choices:

- **Manual update**: manual importation of the list from a file obtained from the certification authority.
- **Automatic update using URL**: by entering the URL of the certification authority's site, the list is automatically updated.
- **Automatic update using certificate**: the certificate presented by the remote entity indicates where to find the relevant revocation list. If the certificate does not contain a URL, you can fill in the **Backup URL** field.

c. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

3. Click on the **Notifications** tab. This tab is used to configure an e-mail address to receive notifications of expiry of the current certificate. In the **PKI Certificate Notifications** area, select the type of notification required. Three choices are available:
   - **Do not use notifications for PKI certificates**: no notification is given when the current certificate expires.
   - **Use a specific e-mail address**: an e-mail address is configured to receive notifications of the current certificate's expiry. In the **E-mail Address** field, type in the notification reception address.
   - **Use the general e-mail address for notification**: notifications of certificate expiry are sent to the general e-mail address configured by the administrator. For more information, consult the "Administration tools" section.

9.5.8 Interoperability with IPSEC Gateways

9.5.8.1 Interactions

9.5.8.1.1 INTEROPERABILITY WITH OTHER IPSEC GATEWAYS

IPsec Tunnel establishment phases

The IKE (Internet Key Exchange) protocol is used to establish secure IPsec connections. There are two phases in the protocol.

IKE phase 1

Phase 1 purpose is to establish a bi-directional secure connection between the two IPsec gateways, which is associated to an **ISAKMP SA** (Security Association). During this phase, the peers negotiate a set of parameters to use for:

- making this connection secure (ciphering and hashing algorithms),
- creating keys,
- mutual authentication.

The standards define two modes for Phase 1, namely Main Mode and Aggressive Mode. In the case of a VPN LAN to LAN, **Alcatel-Lucent OmniPCX Office Communication Server only handles the principal mode** sometimes called ID PROTECT.

IKE phase 2

The Phase 1 secure channel is then used to negotiate security settings for a particular mechanism, e.g. IPsec ESP in our case. This is the Phase 2 of IKE, and it allows establishing IPSEC SA, which will further be used to convey data securely between the two LANs.

The mode used for IKE Phase 2 is always **Quick Mode**.

Interoperability troubleshooting

This section describes the points in the IKE negotiation where interoperability problems are likely to arise. Information about the Alcatel-Lucent OmniPCX Office Communication Server features should help tuning the peer device's IPsec configuration and make the secure connection happen.

Foreword

The configuration of the IPsec VPN feature has been voluntary simplified on Alcatel-Lucent OmniPCX Office Communication Server to feet the "Plug-and-Play" aspect and ease of configuration of product. Integration of pre-configured security profiles usually avoids having to modify the negotiated parameters for SA establishing. Thus, for a LAN to LAN connection between two Alcatel-Lucent OmniPCX Office Communication Server, it is enough to select the same security profile to ensure inter-working. Equally, the pre-configured security profile for IPsec clients can be used "as is" for interoperability with Microsoft IPsec clients.

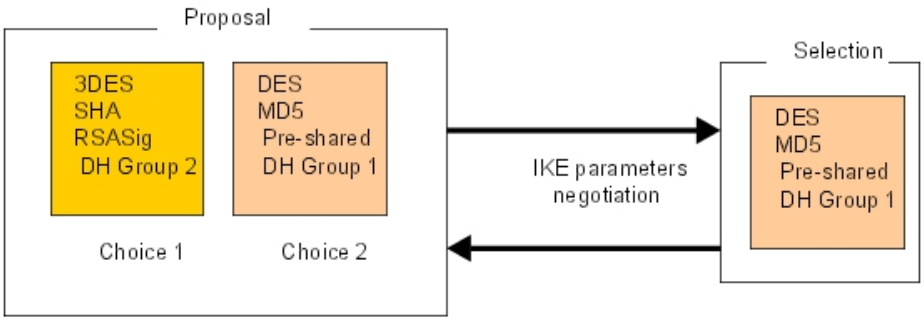
Interoperability with other products must also be ensured, since Alcatel-Lucent OmniPCX Office Communication Server supports all the IPSec functionalities defined as mandatory by IETF standards. When the default security profiles are not suitable, configuration of one of the two systems to be interconnected will have to be modified. In the case of the Alcatel-Lucent system:

- in the case of a VPN LAN to LAN, it is always possible to create or to modify the security profiles in order to adapt to a specific configuration of the remote gateway.
- In the case of IPSec clients other than Microsoft clients, the "Ipsec client" security profile must be edited in order to add the parameters required by the client.

SA settings negotiation

A security association gathers the settings that are used to secure a connection. They contain algorithms, keys, peers addresses, etc ... As explained in the previous section, a SA negotiation is performed in each of the two IKE phases. They both follow the same negotiation scheme, explained hereafter.

During negotiation, the initiator of the connection sends a list of proposals, i.e. a combination of SA settings it can accept. The responder then selects an acceptable proposal, and tells the initiator about this choice.



- Phase 1 SA settings

The table below depicts the settings being negotiated during phase 1, and the possibilities offered by Alcatel-Lucent OmniPCX Office Communication Server.

Settings	Purpose	Supported in Alcatel-Lucent OmniPCX Office Communication Server
Ciphering algorithm	Data confidentiality	DES 3-DES AES
Hash function	Data authentication + integrity	SHA-1 MD5
Diffie-Helman Group	Key computation	Group 1 (Oakley MODP768) Group 2 (Oakley MODP1024) Group 5 (Oakley MODP1536)
Authentication method	IPsec peers authentication	Pre-Shared secret key(PSK) Certificates
SA lifetime	Time before re-negotiation of this SA	Maximum 24 hours

- Phase 2 SA settings

The same settings as in Phase 1 are negotiated, except the authentication method. **The mechanism used to protect traffic for the VPN is always ESP. Encapsulation is performed by tunnel mode**, except for the Microsoft IPSec client where the transport mode is used.

Important:

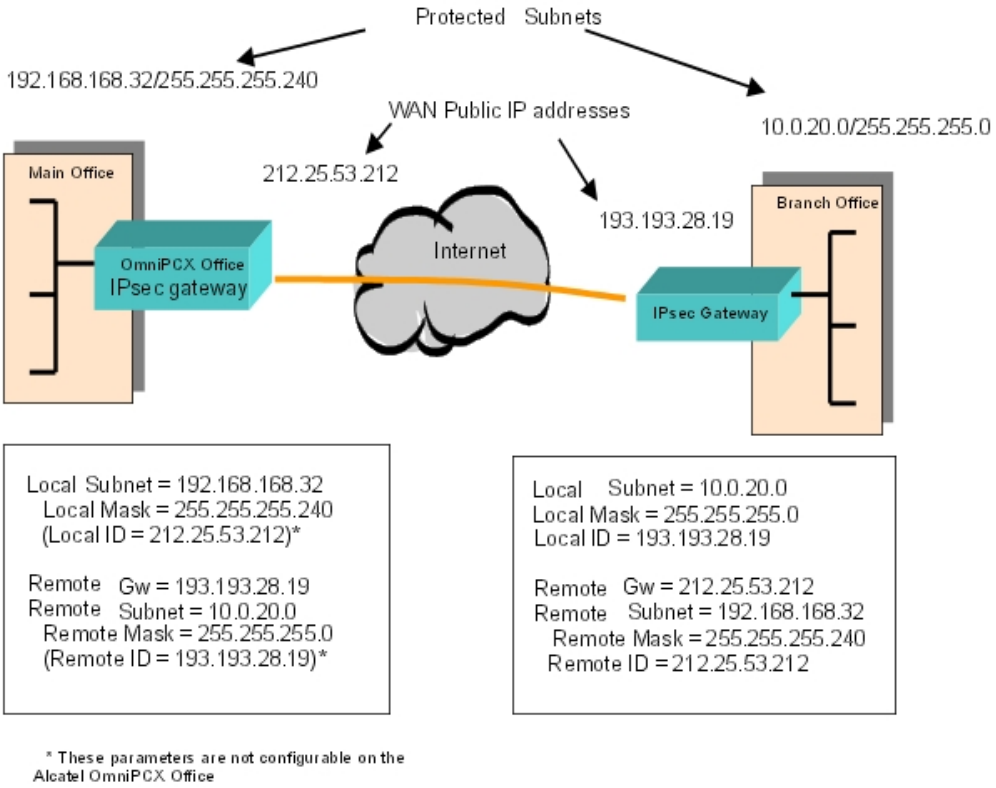
AH is not used on Alcatel-Lucent OmniPCX Office Communication Server. It is possible to configure separate Diffie Helman groups for Phase 1 and Phase 2, but it is highly recommended to set the same group for both phases.

Peers identity checking

Before Phase 2 can begin, the peer devices must authenticate each other. For this purpose, they use the method defined during the Phase 1 SA negotiation to compute some data that can be derived only thanks to a secret (shared secret or digital signature if the certificates are used). This data is sent with an identity payload that identifies the IPsec gateway.

Alcatel-Lucent OmniPCX Office Communication Server does not allow configuration of peer's identities, hence identities are always the WAN IP addresses of the system in the case of an authentication by shared key (PSK), or the "distinguished name" in the case of an authentication by certificates.

When using the PSK method, it must be ensured that the remote system is configured to send its IP address to identify itself (often referred as "local id" settings), and also uses an IP address to identify the remote Alcatel-Lucent OmniPCX Office Communication Server system. Such a configuration is shown in the next figure.



Phase 2 identities

There is also an identity payload exchange during Phase 2, but this one only refers to the subnets being protected. Both parties send the IP settings of the subnets (both local and remote) that are going to be protected by this tunnel. These settings must match on the two sides for the exchange to be valid.

Debugging tools

A VPN test tool for VPN LAN to LAN is available from the Alcatel-Lucent OmniPCX Office Communication Server web-based management tool (WBM): **VPN/RAS -> Site to Site VPN**. This tool is used to detect the most common problems, by giving an indication on the possible origin of the failure and the associated solutions.

If the tunnel is established, the test gives information on the negotiated parameters, which are used to protect the data. For example, ESP-3DES[168]-HMAC-MD5 for a tunnel using the ESP protocol, 3DES ciphering with a 168-bits key, and the MD5 hash algorithm.

9.6 E-mail

9.6.1 Overview

Alcatel-Lucent OmniPCX Office Communication Server is used to offer an electronic

messaging solution for all users in a company. To do this, it supports various configurations:

- It can be the company's messaging server,
- It can be integrated into the company network if it already has a messaging server,
- It can facilitate access to an external messaging server.

These various possible configurations are described below:

9.6.1.1 PRINCIPLES OF OPERATION

9.6.1.1.1 Scenario 1: Alcatel-Lucent OmniPCX Office Communication Server IS THE MESSAGING SERVER

- **For the description of the available e-mail addresses (Stand alone, PO3, IMAP4 or SMPTP subscription), see the APPENDIX 2 at the end of this file.**

Alcatel-Lucent OmniPCX Office Communication Server makes available to each user a local mailbox, and manages the flow of messages between users of the local network and those to and from the Internet. The protocols used by this server are SMTP, to send messages, and POP3 or IMAP4, to manage mailboxes.

Remark:

The IMAP4 protocol (Internet Mail Access Protocol) is an alternative to the protocol POP3. It offers many more possibilities, including:

- Check e-mail directly on the server, without having to download the messages.
- Retrieve all, or part of, the attributes of a message.
- Know the contents of a message before downloading it.
- Organize the mail on the server.

Two possibilities must be considered:

- POP3 subscription: the IAP stores the mail messages (POP3 accounts),
- SMTP subscription: the IAP does not store the mailbox.

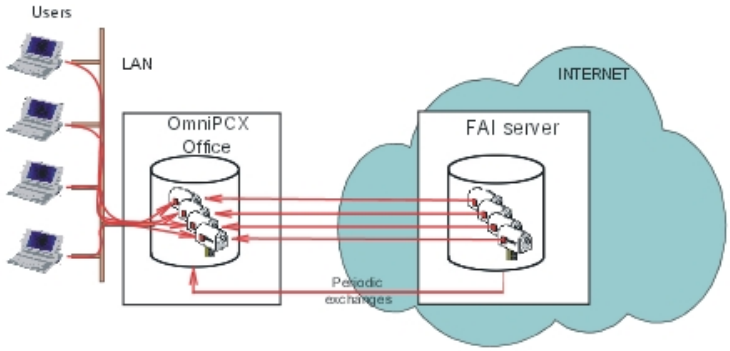
1 - POP3 SUBSCRIPTION: THE IAP STORES THE MAIL MESSAGES (POP3 ACCOUNTS)

Each user has available:

- a private mailbox with the IAP,
- a mailbox on Alcatel-Lucent OmniPCX Office Communication Server (internal).

It is the Alcatel-Lucent OmniPCX Office Communication Server messaging server that downloads the mail to the internal mailboxes for each IAP connection or at pre-defined time intervals.

This principle, known as **POP3 caching**, makes it possible to optimize the FAI connections: a user is not authorized to access his mailbox directly with the FAI (since this would automatically create a connection), he has access only to his local mailbox.



In addition to private mailboxes for each user, the IAP can also store a default mailbox. This box, which is optional, receives all the e-mails for an addressee who does not have a private mail box. Alcatel-Lucent OmniPCX Office Communication Server retrieves the contents of this mail box and distributes it to different local mail boxes depending on the addressee. This function is called **Multidrop**.

Note:

Refer to example 1 - B in the Using the E-mail Assistant section

The mode of operation is as follows:

- **Outgoing mail**
  The mail sent by a user is "entrusted" to an Alcatel-Lucent OmniPCX Office Communication Server that sorts it according to the following criteria:
  - If the recipient's e-mail address corresponds to an address associated with a local user, the message is deposited in the addressee's local mailbox.
  - In all other cases, the message is stored temporarily in Alcatel-Lucent OmniPCX Office Communication Server, then sent during the next connection or by default, at time intervals pre-defined in the Configuration ->E-mail [Main tab] menu, the Activity field of the mail.
- **Incoming mail**
  The mail deposited in the mailboxes with the IAP (user mailboxes or default mailboxes) is retrieved by Alcatel-Lucent OmniPCX Office Communication Server during the first connection following the depositing operation, or at pre-defined time intervals (as described above), and routed to local mailboxes. Each user will then be able to retrieve his mail in Alcatel-Lucent OmniPCX Office Communication Server.

Important:

The type of connection can be "on demand", "on demand with callback" or "permanent". Alcatel-Lucent OmniPCX Office Communication Server's IP address can be static or dynamic.

2 - SMTP SUBSCRIPTION: THE IAP DOES NOT STORE MAILBOXES

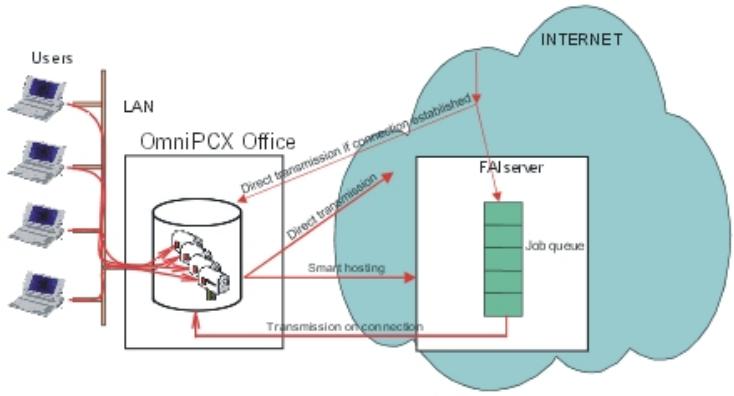
Mailboxes exist exclusively in Alcatel-Lucent OmniPCX Office Communication Server, and mail intended for users must be deposited directly in these boxes.

In the case of a non-permanent connection, this procedure is not possible for mail coming from the Internet without an additional service to store messages temporarily. This service, provided by many ISPs, is known as "SMTP relay".

There are two possibilities, depending on whether or not the ISP provides an SMTP relay service:

- **SMTP relay service provided by the ISP**

  Note 1:
  Refer to example 1 - A - a in the section on Using the E-mail Assistant



  The mode of operation is as follows:

  - **Incoming mail**
    The SMTP relay service consists of temporarily stored messages intended for Alcatel-Lucent OmniPCX Office Communication Server users in a queue, then transferring them to local mailboxes as soon as the connection is established, or on explicit request from Alcatel-Lucent OmniPCX Office Communication Server by virtue of the ETRN (Extended Turn) command.

    Note 2:
    If the ETRN box has been checked, this command will be sent to the IAP's SMTP server whenever a connection is made (on expiration of the "mail activity" time or voluntary connections). The command will be ignored by the IAP if the latter does not provide this service.

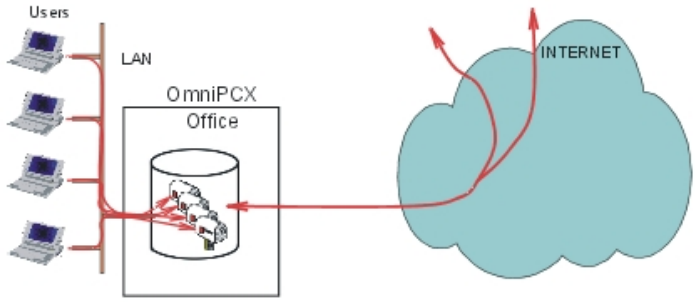
  - **Outgoing mail**
    Outgoing company mail and mail intended for the Internet can also be relayed by the IAP SMTP server, and this service is called “smart hosting”.

Important 1:

The type of connection can be "on demand", "on demand with callback" or "permanent". Alcatel-Lucent OmniPCX Office Communication Server's IP address must be static. The company must have its own domain name.

- **No SMTP relay service provided by the IAP (direct SMTP connection)**

  Note 3:
  Refer to example1 - A - b in the section on Using the E-mail Assistant



Alcatel-Lucent OmniPCX Office Communication Server is the main messaging server, the mail from the Internet is deposited directly into the users" local mail boxes.

Important 2:

The connection type must be "permanent". Alcatel-Lucent OmniPCX Office Communication Server's IP address must be static. The company must have its own domain name.

9.6.1.1.2 Scenario 2: A MESSAGING SERVER EXISTS ALREADY ON THE LAN

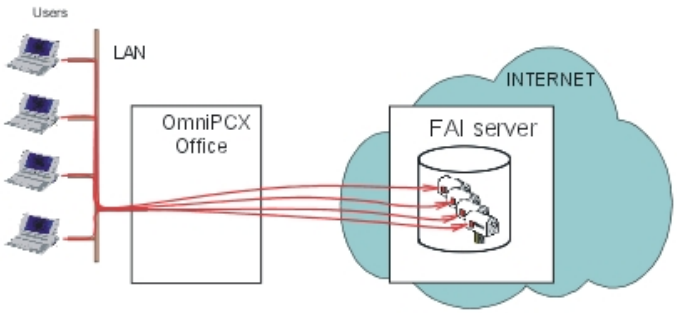
If the company is connected to the Internet via Alcatel-Lucent OmniPCX Office Communication Server, it is used as the gateway between the LAN and the Internet for the exchange of messages. In such cases, the user must specify:

- The e-mail server's IP address on the LAN
- The protocol used for e-mail messages coming from the IAP: SMTP or POP3/IMAP4 depending on the IAP's operating mode.

9.6.1.1.3 Scenario 3: THE MESSAGING SERVER IS HOSTED ON THE IAP

There is no messaging server in the company (Alcatel-Lucent OmniPCX Office Communication Server or LAN).

Alcatel-Lucent OmniPCX Office Communication Server is used as the gateway between LAN and Internet. To enable the exchange of e-mails between the client PCs on the LAN and the Internet, the firewall rule “e-mail” must be opened (see chapter on securing Internet access).



9.6.2 Services provided

When Alcatel-Lucent OmniPCX Office Communication Server is the messaging server, the following services are available:

- alias management,
- multi-domain management,
- routing to external users,
- Proxy POP3 server,
- Anti-virus
- Alert messages

9.6.2.1 Alias management

This service is used to provide several recipient names per user.

When Alcatel-Lucent OmniPCX Office Communication Server receives messages, a recipient name / mail box correspondence table allows the messaging server to distribute the messages to suitable local mail boxes. For each local mail box this correspondence table contains the various recipient names that can be used to reach it.

This service is available:

- as an SMTP subscription, either with or without the SMTP relay service,
- as a POP3 subscription, only if the IAP hosts a default mail box and if Alcatel-Lucent OmniPCX Office Communication Server has multidrop management enabled.

9.6.2.2 Multi-domain management

This service is used to manage several domain names for the same company. A main domain name and one or more secondary domain names are defined in the IAP and in Alcatel-Lucent OmniPCX Office Communication Server.

This service is available irrespective of the chosen subscription (POP3 or SMTP).

- as a POP3 subscription: the messages are sorted in the IAP and directed to the user mail boxes hosted on the IAP. This means the messages are already sorted when Alcatel-Lucent OmniPCX Office Communication Server retrieves them and forwards them to the local mail boxes.
- as an SMTP subscriber: Alcatel-Lucent OmniPCX Office Communication Server sorts the messages when received; all messages whose address includes a pre-defined domain name (main or secondary) are accepted, and routed to users" local mail boxes.

9.6.2.3 Routing to external users

When Alcatel-Lucent OmniPCX Office Communication Server is the messaging server, it is possible to define uses as “remote workers”. These users have a personal mail box stored with the IAP, but they do not have a local mail box on Alcatel-Lucent OmniPCX Office Communication Server.

The mail intended for them is routed as follows:

- **mail from the company**
  Alcatel-Lucent OmniPCX Office Communication Server recognises the address and routes

the message to the IAP. The mail is stored in the remote user's personal mail box in the IAP, and is retrieved by the remote worker when he logs onto the IAP server.

- **Mail from the Internet**
  The mail is stored in the remote user's personal mail box in the IAP, and is retrieved by the remote worker when he logs onto the IAP. This mail is not retrieved by Alcatel-Lucent OmniPCX Office Communication Server.

This service is available only in the case of a POP3 subscription:

9.6.2.4 Proxy POP3 server

The Proxy POP3 server (bypass server) allows a remote worker connecting to the company's LAN to check his mail box hosted on the IAP without being configured as an Alcatel-Lucent OmniPCX Office Communication Server user. To do this, simply create an e-mail account on the e-mail client, including the following characteristics:

- POP3 account with the IAP = POP3server:account
- Password for POP3 account with the IAP = password

9.6.2.5 Anti-virus

The anti-virus is only active when Alcatel-Lucent OmniPCX Office Communication Server is the e-mail server. For more information about how the anti-virus functions, consult the "Anti-virus" section.

9.6.2.6 Alert messages

There are two types of alert messages:

- alert messages on total disk space,
- alert messages on user disk space,

An alert message can be sent to the administrator when the disk space reserved for e-mails exceeds a specific rate. This rate and the administrator's address are configured in the e-mail settings.

9.6.3 Messaging Servers

9.6.3.1 Configuration procedure

The messaging server can be:

- Internal to the system.
- External on the LAN.
- Neither internal to the system not external on the LAN. In this case, it suffices to start the **E-mail** wizard.

9.6.3.1.1 INTERNAL E-MAIL SERVER CONFIGURATION

To configure an internal messaging server, click on **Wizards** in the navigation bar. The assistants" icons appear.

1. Click on the **E-mail wizard** icon.
2. In the **Location of the E-mail Server** area, check the box:
   - **Internal e-mail server on the system**

3. Click on **Next**. A new window appears.
4. In the **Internal e-mail server operating mode** area, there are three possible choices:
   - If **your ISP stores your personal mailboxes**

   a. Check the **With ISP mailboxes (POP3)** box

   b. Click on **Next**. A new window appears.

   c. In the **POP3 Settings** area, fill in the **POP3 server name** field.

   d. Click on **Next**. A new window appears.

   e. In the **Domain name for e-mails** area, there are two possible choices:
   - check **I have my own domain name** if you have your own domain name
   - check **I have to use the ISP domain name** if you must use the ISP's.

   In either case, enter the relevant domain name.

   f. Click on **Next**. A new window appears.

   g. In the **Anti-virus Settings** area,
   - check **No anti-virus e-mail scanning**, if you do not wish to have you e-mails checked for viruses
   - check **External anti-virus e-mail scanning** if you do. In **Anti-virus location**, enter the IP address of the equipment on which the anti-virus software is installed.

   h. Click on **Next**. The **Summary** area lists all the options you have chosen.

   - If **your ISP stores your mailboxes and manages a default mailbox**

   a. Check the **With ISP mailboxes and use of a default mailbox (Multidrop)** box

   b. Click on **Next**. A new window appears.

   c. In the **POP3 Settings** area, fill in the **POP3 server name** field.

   d. In the **Default mailbox settings (Multidrop)** area, fill in the following fields:
   - **Default POP3 account**: name of the mailbox (POP3 account) created in the ISP in order to receive any e-mail not addressed to personal mailboxes.
   - **Password**: each mail box (POP3 account) created in the ISP is password protected. Alcatel-Lucent OmniPCX Office Communication Server uses this password to download the mail before distributing it to users.
   - **Confirm password**

   e. Click on **Next**. A new window appears.

   f. In the **Domain name for e-mails** area, fill in the following field:
   - **My domain name**: this domain name is necessarily public (registered and declared with the authorities that manage Internet domain names).

   g. Click on **Next**. The **Summary** area lists all the options you have chosen.

   - If **your ISP does not store your personal mailboxes**

   a. Check the **Without ISP mailboxes (POP3)** box

   b. Click on **Next**. A new window appears.

   c. In the **Domain name for e-mails** area, fill in the **My domain name** field:

   d. Click on **Next**. The **Summary** area lists all the options you have chosen.

9.6.3.1.2 EXTERNAL E-MAIL SERVER CONFIGURATION

To configure an external messaging server, click on **Wizards** in the navigation bar. The assistants" icons appear.

1. Click on the **E-mail wizard** icon. The **E-mail Wizard** window displays.

2. In the **Location of the E-mail Server** area, check the box:
   - **External e-mail server on the LAN**
3. Click on **Next**. A new window appears.
4. In the **External e-mail server on the LAN** area, fill in the **E-Mail server IP address** field
5. In the **External e-mail server operating mode** area, there are two possible choices:
   - **POP3/IMAP4 accounts**
   - **SMTP relay**
6. Click on **Next**. The **Summary** area lists all the options you have chosen.
7. Click on **Finish**. The **E-mail Settings** window appears.

9.6.4 E-mail

9.6.4.1 Configuration procedure

To configure the e-mail, click on **E-mail** in the navigation bar. The **E-mail Management** window displays. This window comprises three areas:

- the **E-mail server operating mode** area, which lists the characteristics of the mail server configured via the wizard. Click on the **Test** button or the **E-mail test** hypertext link to launch the operating test. When the test is complete, the **E-mail** window appears and shows the test results.
- the **User list** area, which lists all the users created who have a local mailbox with their e-mail address. Click on the user name to access the **E-mail** tab of the **User Settings** window. For more information about these settings, see the User and User groups section.
- the **Mailing lists** area, which shows all the mailing lists. When the users and the messaging accounts have been created, Alcatel-Lucent OmniPCX Office Communication Server is used to create and manage the mailing lists. A distribution list holds several electronic addresses under the same name, which allows users to fill in the name of the list as the recipient of a message (name of a service for instance), rather than having to fill in all the addresses of the individuals concerned.

9.6.4.1.1 MAILING LIST

Mailing lists management comprises the following tasks:

- adding a new mailing list,
- deleting one or several mailing lists,
- modifying mailing list properties,

Click on **E-mail** in the navigation bar. The **E-mail management** window appears, with the **Mailing list** area showing.

ADDING A NEW MAILING LIST

1. Click **Add** The **Mailing List Wizard** window appears. It comprises the following tabs: **Settings**, **Members** and **E-mail**.
2. Click on the **Settings** tab. In the **Mailing List Name** area, enter the name of the mailing list.
3. Click on the **Members** tab. This tab is used to create the mailing list members.

a. In the **New Members** area, there are two possible choices:
- Select **Add a defined user** if the member you want to add to the list is a user defined in the system. Select the user(s) in the drop-down menu.
- Select **Add an e-mail address** if the member you want to add to the list has an external e-mail address. Enter this e-mail address in the **E-mail Address** field.

b. Click on the **Add** button to validate the new member's addition. The new members appear in the list located below the **New Members** area.

4. Click on the **E-mail** tab. This tab is used to configure the e-mail settings of the mailing list.
   a. The **E-mail Server Operating Mode** area lists the characteristics of the e-mail server configured via the wizard.
   b. The **Mailing List e-mail address** area gives the mailing list address which will be used to send e-mails to this list. This address cannot be modified.
   c. In the **External POP3 mailbox** area, fill in the following fields:
   - **POP3 mailbox name**
   - **Password**
   - **Confirm password**

   Remark:
   This area is only displayed in POP3 configuration or POP3 multidrop configuration with a mailbox dedicated to the mailing list.

5. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

DELETING ONE OR SEVERAL MAILING LISTS

To delete a mailing list, click on the corresponding **Delete** hypertext link.

To delete several mailing lists: select the mailing lists by checking the box located before the mailing list name and click on **Delete selection**.

MODIFY A MAILING LIST PROPERTIES

Click on the mailing list name of your choice. The **Mailing List Settings** window appears. This page comprises three tabs: **Settings**, **Members** and **E-mail**. For more information on configuring this tab, see the Add a new mailing list section.

9.6.4.1.2 E-MAIL SETTINGS

To configure the e-mail, click on **E-mail** in the navigation bar. The **E-mail Management** window displays. Click on the **E-mail Settings** hypertext link, the **E-mail Settings** window appears. This window comprises several tabs:

- **Location**
- **Mode**
- **Domains**
- **Greeting**
- **Alerts**

1. Click on the **Location** tab. This tab displays the information required to locate the e-mail server and to define the reception and distribution period for external e-mails.
   a. The **Location of the E-mail Server** area indicates the location (internal or external) of the e-mail server configured via the wizard.

b. In the **E-mail Exchange** area, fill in the following field:

- **Exchange every (min)**: used to define the reception and distribution period for external e-mails.

c. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

2. Click on the **Mode** tab. This tab displays the information necessary to define the e-mail server's operating mode.

a. In the **Internal E-mail Server Operating Mode** area, select one of the three following modes according to the contract agreed with your ISP.

- If you select the **With ISP mailboxes (POP3)** mode, fill in the following areas:
- **Incoming E-mail** by specifying the name of the POP3 server.
- **Outgoing E-mail** by specifying whether you choose the direct sending mode or the use of your IAP's SMTP server to relay outgoing mail. (This service is also called Smart Hosting)
- If you select the **With ISP mailboxes and use of a default mailbox (Multidrop)** mode, fill in the following areas:
- **Incoming E-mail** by specifying the name of the POP3 server.
- **Outgoing E-mail** by specifying whether you choose the direct sending mode or the use of your IAP's SMTP server to relay outgoing mail. (This service is also called Smart Hosting)

Click on **Switch to the default account** to access a new window comprising two areas:

- **Default mailbox settings (Multidrop)**: used to configure the default mailbox used.
- **Multidrop Envelope Field**: In the case of a POP3 subscription with Multidrop option, Alcatel-Lucent OmniPCX Office Communication Server needs to know which enveloped field is being used. Alcatel-Lucent OmniPCX Office Communication Server uses the default parameter X-Envelope-To. If a different parameter is used, select the **User-defined** option and enter the parameter in the adjacent text entry area.

Note:
The IAP must provide the parameter used. If this should happen, you can send a message to a mailbox using the default account, and consult the message header to find the parameter used.

- If you select the **Without ISP mailboxes (SMTP)** mode, fill in the following area:
- **Server** by specifying the name of the SMTP server, as well as the use of ETRN and smart hosting

b. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

3. Click on the **Domains** tab. This tab displays the information required to define several domain names for e-mail accounts managed by Alcatel-Lucent OmniPCX Office Communication Server.

a. The **Domain name for e-mails** area is used to define your main domain name. Two choices are possible:

- Select **I have to use the ISP domain name** if you do not have your own domain name and enter the domain name provided by your ISP.
- If you do, select **I have my own domain name** and enter the public domain name (registered and declared with the authorities that manage Internet domain names). In this case, it is possible to add a secondary domain name by typing the new name in the **New Secondary Domain Name** area and clicking on the **Add** button.

To delete a domain name, select the name to be deleted from the **Domain Name** field and click on the **Delete** button of the **Secondary Domain Names** area.

b. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

4. Click on the **Greeting** tab. This tab is used to define the message sent to a user during the creation of his or her mailbox.
   a. In the **Greeting message** area, fill in the following fields:
      - **E-mail subject**
      - **E-mail content**

   b. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.
5. Click on the **Alerts** tab. This tab is used to configure an e-mail address to receive alert notification and to define the type of alerts that trigger notifications. When the conditions are fulfilled, these alerts are sent every day at 4 a.m. and 4 p.m., until the situation returns to normal.
   a. In the **E-mail address for alert notification** area, select the required type of notification. Three choices are available:
      - **Do not use alerts on the E-mail Disk Space**: notification of the alert is not given.
      - **Use a specific e-mail address**: an e-mail address is configured to receive notifications of alerts when the hard disk filling threshold is reached. In the **E-mail Address** field, type in the notification reception address.
      - **Use the general e-mail address for notification**: notifications of alerts are sent to the general e-mail address configured by the administrator. For more information, consult the "Administration tools" section.

   b. In the **Notification Alert** area, select the types of alerts by checking the:
      - **Global Disk Space Alert** box to send a message when the e-mail disk space exceeds the level defined in the **Disk Space Used(%)** field.
      - **User Disk Space Alert** to send a message when the user threshold is reached. For more information, consult the "User and User Groups" file in the "Modifying a Users" Group Properties".

9.6.5 Appendix

9.6.5.1 APPENDIX 1: SUMMARY OF THE DIFFERENT CONFIGURATIONS SUPPORTED

9.6.5.1.1 Scenario 1: Alcatel-Lucent OmniPCX Office Communication Server is the messaging server

The IAP stores the mail messages (POP3 accounts)

Is an e-mail server software key required?	Type of Internet connection that can be used	IP address required	E-mail services required from the IAP	Remarks
YES	- Demand Dial - Callback - Permanent connection	- Dynamic - Static	Hosting of electronic messaging with POP3 accounts customised for users, and possibly a default account (multidrop). With a POP3 subscription, the company can have its own domain name (company.com) or can use the IAP's (IAP.com). With a POP3 multidrop subscription, the company must have its own domain name (company.com)	If the company does not have its own domain name (company.com) and uses the IAP name (IAP.com), you must fill in the IAP's **Main Domain Name** field.

- Protocol supported in this configuration:

The IAP does not store mailboxes

The company uses an SMTP messaging relay service (SMTP subscription).

Is an e-mail server software key required?	Type of Internet connection that can be used	IP address required	E-mail services required from the IAP	Remarks
YES	- Demand Dial - Callback - Permanent connection	- Static	SMTP electronic messaging relay service. The company must have its own domain name.	If the company uses an SMTP messaging relay service from its IAP, you must select **Without ISP mailboxes (SMPT)**

- Protocol supported in this configuration:

The company does not use an SMTP messaging relay service (without SMTP subscription).

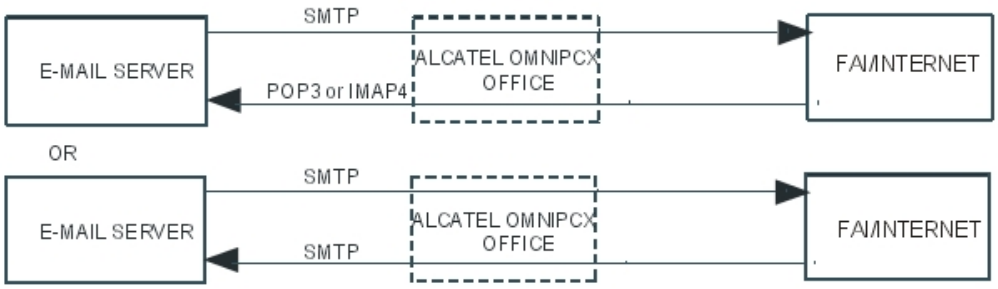
Is an e-mail server software key required?	**Type of Internet connection that can be used**	**IP address required**	**E-mail services required by the IAP**	**Remarks**
YES	- Permanent connection	- Static	The company must have its own domain name.	There is no help for incoming traffic if the line or the system are temporarily out of order.

- Protocol supported in this configuration:

9.6.5.1.2 Scenario 2: A messaging server already exists on the LAN

Is an e-mail server software key required?	**Type of Internet connection that can be used**	**IP address required**	**E-mail services required from the IAP**	**Remarks**
NO	- Demand Dial - Callback - Permanent connection	- Dynamic - Static	Depends on the e-mail server used in the company. The IAP services supported by Alcatel-Lucent OmniPCX Office Communication Server in this configuration are as follows: - hosting of POP3 accounts - SMTP messaging with/without relay service	If the company uses an SMTP messaging relay in its own IAP, the **smtp relay** field must be checked,.

- Protocol supported in this configuration:



9.6.5.1.3 Scenario 3: The messaging server is hosted on the IAP

Is an e-mail server software key required?	Type of Internet connection that can be used	IP address required	E-mail services required from the IAP	Remarks
NO	- Demand Dial - Callback - Permanent connection	- Dynamic - Static	Hosting of electronic messaging with as many POP3 accounts as users.	

- Protocol supported in this configuration:

9.6.5.2 APPENDIX 2: SUMMARY OF THE AVAILABLE E-MAIL ADDRESSES

This annex presents a summary of available E-mail addresses when Alcatel-Lucent OmniPCX Office Communication Server is the messaging server (scenario 1).

9.6.5.2.1 WHAT IS AN E-MAIL ADDRESS?

An e-mail address must have the format **user_part@domain_part**. It has two parts:

1. User_Part:
2. Domain_Part:

User_Part:

The user part is usually a person's name. It may also be the name of a department, team, office, etc. The user part can be more than a simple string.

Example:
"john.smith" or "research.team"

Domain_Part:

The domain part indicates the company's Internet address. For a company, "company.com" corresponds to the domain part of the address, and ".com" corresponds to the domain. The domain part can be more than a simple string.

Example 1:

"research.company.com"

".com", the last part of the address, tells more about what kind of institution the address belongs to, or what part of the world it's from.

Example 2:

- ".com' is usually a company or commercial institution
- ".gov' means a government site.
- ".net' means gateways and other administrative hosts for a network.
- ".org' groups private organizations that don't easily fit into other categories.

9.6.5.2.2 USER PART MANAGED BY OmniPCX Office

1. **Login**
   The login of an Alcatel-Lucent OmniPCX Office Communication Server account comprises the user's first name and last name. The login has the following form: **name.surname**.

   Example 1:
   the Alcatel-Lucent OmniPCX Office Communication Server account login for JOHN SMITH is "john.smith".

2. **User part of a POP3 e-mail address**:
   - **User managed on Alcatel-Lucent OmniPCX Office Communication Server** : The user has a POP3 account on the ISP e-mail server. An e-mail address in the format **user_part@domain_part** is associated with this account with this specific format. Most often, the IAP administrator has been able to configure the user part and uses the convention **First Name.Surname**.
   - **External User**: External users are only available if the Alcatel-Lucent OmniPCX Office Communication Server e-mail server mode is configured in POP3. An external user has his private POP3 mailbox by the ISP/ASP.

     Remark:
     Alcatel-Lucent OmniPCX Office Communication Server does not manage this mailbox. It is not polled by the Alcatel-Lucent OmniPCX Office Communication Server e-mail server.
     The user part of the external user's e-mail address should be in accordance with the address defined by the ISP/ASP's administrator.

3. **User Alias**
   Alcatel-Lucent OmniPCX Office Communication Server administrator can define for each user, one or more aliases. An alias is an alternative name for a user.

   Example 2:
   user aliases for "john.smith" could be "jsm", "johns", "bigboss", etc.

4. **Mailing List Name**
   A mailing list contains one or more user's login and/or one or more e-mail addresses. If an e-mail is sent to this mailing list, the message will be broadcast to every member belonging to this list.

Example 3:
Members of the "team_rd" mailing list: "john.smith", "nicole.kidman","mariane.seegelbrecht@alcatel.com".

9.6.5.2.3 DOMAIN PART MANAGED BY Alcatel-Lucent OmniPCX Office Communication Server

1. **Name of the company's Local Area Network (LAN)**
   This may be the company's name (company.com). This name can be configured using WBM.
   In the table below this name is identified by **Internal_domain_part**.
2. **Company's Public Domain Name**
   There are two possible cases:
   - The company has bought a domain name part from an IAP. This is the name of the company's public domain, or domains.
     In the table below this name is identified by **External_domain_part**.
   - The company hasn't bought a domain name part. The ISP defines the domain part. Very often, the domain name part corresponds to the name of the ISP.

     Example:
     Wanadoo uses "wanadoo.fr" in France and the user John SMITH will have for email address "john.smith@wanadoo.fr".
     In the table below, this name is identified by **ISP_domain_part**.

9.6.5.2.4 AVAILABLE E-MAIL ADDRESSES

The table below lists all the available e-mail addresses.

User part	E-mail from LAN	E-mail from ISP
STAND ALONE (System without Internet Access)		
user	login@internal_domain_part	not possible
user alias	useralias@internal_domain_part	not possible
mailing list	mailinglist@internal_domain_part	not possible
External user	not relevant	not relevant
SMTP SUBSCRIPTION		
user	login@internal_domain_part login@external_domain_part	login@external_domain_part
user alias	useralias@internal_domain_part useralias@external_domain_part	useralias@external_domain_part
mailing list	mailinglist@internal_domain_part mailinglist@external_domain_part	mailinglist@external_domain_part
External user	not relevant	not relevant
POP3 SUBSCRIPTION WITH BOUGHT PUBLIC DOMAIN NAME PART		
user with POP3 account	login@internal_domain_part login@external_domain_part user_part@external_domain_part	user_part@external_domain_part
user without POP3 account	login@internal_domain_part login@external_domain_part	not possible

User part	E-mail from LAN	E-mail from ISP
user alias	useralias@internal_domain_part useralias@external_domain_part	not possible
mailing list with POP3 account	mailinglist@internal_domain_part mailinglist@external_domain_part	mailinglist@external_domain_part
mailing list without POP3 account	mailinglist@internal_domain_part mailinglist@external_domain_part	not possible
External user	receives an e-mail via ISP: user_part@external_domain_part	user_part@external_domain_part
POP3 SUBSCRIPTION WITH ISP DOMAIN NAME PART		
user with POP3 account	login@internal_domain_part user_part@isp_domain_part	user_part@isp_domain_part
user without POP3 account	login@internal_domain_part	not possible
user alias	useralias@internal_domain_part	not possible
mailing list with POP3 account	mailinglist@internal_domain_part mailinglist@isp_domain_part	mailinglist@isp_domain_part
mailing list without POP3 account	mailinglist@internal_domain_part	not possible
External user	receives an e-mail via ISP: user_part@isp_domain_part	user_part@isp_domain_part
POP3 SUBSCRIPTION WITH MULTIDROP CAPABILITIES		
user with POP3 account	login@internal_domain_part login@external_domain_part user_part@external_domain_part	user_part@external_domain_part
user without POP3 account	login@internal_domain_part login@external_domain_part	login@external_domain_part
user alias	useralias@internal_domain_part useralias@external_domain_part	useralias@external_domain_part
mailing list with POP3 account	mailinglist@internal_domain_part mailinglist@external_domain_part	mailinglist@external_domain_part
mailing list without POP3 account	mailinglist@internal_domain_part mailinglist@external_domain_part	mailinglist@external_domain_part
External user	receives an e-mail via ISP: user_part@external_domain_part	user_part@external_domain_part

9.7 Web Communication Assistant

9.7.1 Overview

The Web Communication Assistant is a Web application designed for Alcatel-Lucent

OmniPCX Office Communication Server end users to help them manage in-house corporate communication (e-mails and voice messages).

The Web Communication Assistant provides the following services:

1. E-mail management via the Webmail.
2. Voice mail management.
3. Using the "call" application.
4. Configuration of user parameters andNomadic mode.

The main advantage of the Web Communication Assistant is that it gives teleworkers access to all these services, from any workstation on the company's LAN or via the Internet.

The Web Communication Assistant uses a secure Web interface enabling it to function with Internet Explorer (release 6 or later), Netscape Navigator (release 7 or later) and Mozilla (release 1.1 or later). The HTTPS secure transfer protocol ensures the identification of the transmitter and the receiver, the integrity and the privacy of the exchanged data.

This section deals in succession with the licence, the services provided, the association between the user account and the phone set, connection to the Web Communication Assistant and the relevant configurations.

9.7.1.1 THE LICENCE

By granting a user a Web Communication Assistant licence, you give him or her the right to use all of its associated applications, i.e.:

- e-mail via the "**e-mails"** application.
- the **"voice mail"** application

Remarks:

if a user tries to access these services without a licence, access will be refused.

It is not necessary to have a licence to access the user's configuration settings.

The final customer buys as many licences as there are users of Web Communication Assistant. The administrator or operator manages the number of licences attributed via WBM.

9.7.2 Services provided

The Web Communication Assistant gives access to the applications described below.

9.7.2.1 The "e-mails" application

This application is used to manage e-mails on a PC, by accessing the mail server. The mail server must be Alcatel-Lucent OmniPCX Office Communication Server. The user must have access to a local E-mailbox, and must have a Web Communication Assistant licence.

You can use this application to:

- send, receive, consult and organize your e-mails.
- Personalize this application's settings.

9.7.2.2 The "voice mail" application

This application is used to manage your phone set's mailbox using a multimedia PC, i.e.:

- Consult and listen to voice mail.

- Call back the person who left the message.
- Delete voice mail.
- Personalize this application's settings.

The user must first configure his internal mailbox, i.e. record his name and configure his password on his phone set.

9.7.2.3 The "call" application

This application uses the Web interface to make calls.

9.7.2.4 The "preferences" application

This application is used to modify the user settings, i.e.:

- Personalize the Web Communication Assistant.
- Change the password giving access to the Web Communication Assistant.
- Manage the user account settings.
- Specify the number of the user's phone set.
- Managing the parameters ofNomadic mode.

9.7.3 Associating a User Account to a Phone Set

9.7.3.1 Basic description

To have access to the **"voice mail"** application from any PC, it is necessary to create an association between the user account and the user's phone set.

If the user has not already configured the number of the phone set associated with his account, a window is displayed telling him his phone has not been identified and asking him to identify himself using his phone number and the password associated with the voice mailbox.

To activate the notification of voice messages by e-mail:

1. In OMC, click **Central Services Global Info**.
2. On the **E-mail notification** tab, select the **Activated** checkbox.

To configure the notification of voice messages by e-mail for each user, use OMC or the Web Communication Assistant Settings application.

9.7.4 Setting the Nomadic Mode

9.7.4.1 Overview

The Nomadic mode can be activated from the Web Communication Assistant.

When connected to the Web Communication Assistant, start the Nomadic set configuration wizard and enter the name and number of the Nomadic set. For more information, see: module Nomadic Mode - Configuration procedure .

9.7.5 Connection

9.7.5.1 Operation

To connect to the Web Communication Assistant, proceed as follows:

1. Open the Web navigator.
2. Enter the following address in the **Address** field of the Web navigator:
   https://<Alcatel-Lucent OmniPCX Office Communication Server>
   where *<Alcatel-Lucent OmniPCX Office Communication Server>* is the machine's IP address or name.
   The Web Communication Assistant's welcome page is displayed.
3. Type in your user name and password in the appropriate fields.
4. Click on **Connect**. Your service connection is established. You access the Welcome Page
   By default the welcome page displays the **"preferences"** application, i.e. the user settings. You can access the other application by clicking on the **e-mails** and **voice mail** icons in the tool bar.

Remark:

the session remains active for 24 hours after the last activity.

9.7.5.1.1 How to disconnect

To disconnect, click on the **quit** icon in the tool bar.

9.7.6 Managing

9.7.6.1 Configuration procedure

To make the Web Communication Assistant accessible to users, the administrator must configure the following items:

1. Via the WBM
   - Configuration of Alcatel-Lucent OmniPCX Office Communication Server as the mail server.
   - Creation of an Internet user account.
   - Allocation of a license to a user.
2. Via OMC
   - Access to an active internal voice mailbox

9.7.6.1.1 Configuration via the WBM

Configuration via the WBM makes it possible to:

1. Configure Alcatel-Lucent OmniPCX Office Communication Server as the mail server
   To configure Alcatel-Lucent OmniPCX Office Communication Server as the mail server, consult the "Electronic Messaging" file
2. Create a user account via the **User wizard**. When creating the account, you can assign a Web Communication Assistant license and the right to use nomad mode to the user.
   To read the detailed procedure, consult the "Users and User Group" file.
3. Change a user's settings via the **Settings** tab in the **User Settings** window.
   To read the detailed procedure, consult the "Users and User Group" file.

9.7.6.1.2 Configuration via OMC

Access to an active internal voice mailbox is configured via OMC. To read the detailed procedure, consult the "Diversion to voice mailbox", section "Call server: Telephone features".

9.8 Internet Utilization Control

9.8.1 Proxy Server

9.8.1.1 Overview

A proxy server is an application that gathers requests from client stations and transmits them to a remote server. The remote server's response is then relayed back to the local PCs. The server, which manages communications, can provide the following services:

- Record everything it does, with a view to compiling statistics on the access of user groups.
- Filter access according to the requested URLs.
- Filter previously connected users.

Proxy servers can also handle caching: i.e. storing the most recently downloaded or used files on a local disk for easier availability. This means a file need only be downloaded once from a web site, and will then be transferred locally at much greater speed in response to identical requests. The main advantage lies in reducing traffic to and from the Internet, and in reducing the connection costs incurred by Alcatel-Lucent OmniPCX Office Communication Server.

Remark:
Where the proxy license is available, the web access (HTTP, HTTPS and Gopher protocols) and file transfer (FTP protocols) services must go through the proxy, unless a rule is added to the firewall rule editor.

9.8.1.2 Services provided

Alcatel-Lucent OmniPCX Office Communication Server includes a HTTP and FTP proxy server with all of the control features listed below.

9.8.1.2.1 Web browsing

In the case of the mode with authentication, the user will be asked for a user name and a password each time s/he starts a navigation session on the Internet. In the case of the mode without authentication, access to the Web is immediate. If user control is active, then accounts without the necessary rights will be rejected.

An Internet navigation session is defined by the launch of a browser (Internet Explorer, Netscape Navigator), access to one or more web sites, and the closure of the browser.

9.8.1.2.2 URL filter

The URL filters are used to control the Internet access of certain user groups to certain web sites. The principle is to block specific URLs according to a list generated by the administrator. This control is applied to individual groups of users.

If the control is active, three alternatives are available:

1. Offer free access to all web sites.

2. Prohibit specific URLs (Forbidden sites filters).
3. Give restricted access (Authorized sites filters).

Nine URL filters are defined by default, but the administrator can create additional filters. In order to simplify filter management, they can be downloaded either manually or automatically (every week or month) to Alcatel-Lucent OmniPCX Office Communication Server.

9.8.1.2.3 Time range

Here, a time range for Internet access is determined for each day of the week, either for the system itself, or for individual groups of users.

9.8.1.2.4 File transfer

This control makes it possible to restrict the ability of one or two user groups to download files from the Internet by blocking the FTP protocol. Downloading is only permitted via HTTP.

9.8.1.2.5 Statistics

Alcatel-Lucent OmniPCX Office Communication Server provides a tool enabling the Administrator to get an overview of Internet activity, and compile statistics using log file data based on several criteria, namely user groups, services and destinations. These statistics describe web access in terms of:

- User groups: statistics on Internet use.
- services used: statistics on the traffic for each service (HTTP or FTP).
- Web sites: the list of web sites visited.

Remark:

Access Control is only possible when the proxy option is selected.

9.8.1.3 Configuration procedure

Click on**Proxy** in the navigation bar. The **Proxy/Cache Settings** window appears. This window consists of two tabs:

- **Parameters**
- **Controls**

1. Click on the **Settings** tab. This tab displays the information needed to configure the proxy.
   a. In the area **Control Policy**, you can define your proxy's operating mode. Two choices are possible:
   With authentication:
   - Click on **Group rights and controls: (authentication required)** .
   - In the drop-down list **with the exception of**, select the sites to be accessible without authentication. This option allows you to steer clear of the authentication and access certain sites, such as sites for updating anti-virus software.

   Without authentication:
   - Click on **Proxy global rights and controls: (no authentication)**.
   - In the area **Proxy Global Rights**, tick the boxes **Access to web sites (HTTP) or File transfer (FTP)**, depending on which rights you wish to attribute.

   b. In the area **Advanced Settings**, include the following field:
   - **Proxy port** :the port number to which the HTTP and FTP requests from the client

stations are sent. The default number is 8000.

c. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

2. Click on the **Control** tab. This tab displays the information needed to set the control policy. The control policy will be saved, but not active, in the mode without authentication.

a. The policy control is set in the area **Web site control**. In the drop-down list **Control policy**, three alternatives are available:

- If you select **All sites except the forbidden sites**, you can access the **Forbidden sites filters** list. You can select one or several sites by ticking the box(es) in front of the site name.
- If you select **Authorised sites only**, you can access the **Authorized sites filters** list. You can select one or several sites by ticking the box(es) in front of the site name.
- If you select **No control**, all sites will be accessible.

b. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

9.8.2 URL Filters

9.8.2.1 Operation

The management of URL filters consists of four main tasks:

- Adding a URL filter,
- deleting one or several URL filters,
- changing the settings of a URL filter,
- updating a URL filter.

To access the window **URL Filter Management**, click on **URL Filters** in the navigation bar. This window comprises two areas:

- The **Forbidden sites filters** area, which shows all of the filters for the forbidden sites.
- The **Authorized sites filters** area, which shows all of the filters for the authorized sites.

For these two lists, the following operations are configured in the same way.

9.8.2.1.1 ADDING A URL FILTER

1. Click **Add** The **URL filter settings** window appears.
2. In the **URL filter name** area, fill in the following field:
   - **URL filter name**: type the name you want to assign to the filter.
3. In the **URL filter type** area, choose the type of URL filter. Three choices are available:
   - If you select **Manually edited URL filter**, you can access the **Manual URL filter updating** area. This service allows you to manually edit a URL filter. Complete the following field:
     - **URL filter content**: type the URL filtering objects. Refer to online help to determine specific syntaxes.
   - If you select **Local download**, you can access the **Manually uploaded URL filter** area. This service allows you to manually upload a new edition of the URL filter. Complete the following field:

- **URL filter file**: Type the access path to the file which contains the URL filtering objects or click **Browse...** to search your workstation and select the file containing the URL lists.

- If you select **Automatically uploaded URL filter**, you can access the **Automatic URL filter upload** area. This service, which allows you to automatically upload a new edition of the URL filter, requires a subscription with an ASP. Complete the following fields:
  - **URL**: Type the URL to upload.
  - **Account name**
  - **Password**
  - **Periodicity**: choose how often you want the new version to be downloaded: every week or month.

4. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

9.8.2.1.2 DELETING ONE OR SEVERAL URL FILTERS

Only URL filters that are not activated can be deleted.

Deleting a URL filter.

Click the corresponding **Delete** hypertext link.

Deleting several URL filters.

1. Select the URL filters by ticking the box in front of the filter name.
2. Click **Delete the selection**.

9.8.2.1.3 CHANGING THE SETTINGS OF A URL FILTER

1. Click on the filter name you want to change. The **URL filter settings** window is displayed.
2. In the **URL filter name** area, check or modify the characteristics of the filter.

9.8.2.1.4 FORCING THE UPDATE OF A URL FILTER

You can force the update of automatically updated URL filters by clicking on **Update**.

9.8.3 Time Ranges

9.8.3.1 Operation

The management of time ranges consists of four main tasks:

- Time range selection,
- adding a time range,
- deleting one or several time ranges,
- changing the settings of a time range,

Remark:

The system's time range always takes precedence over a group's defined time range.

To access the **URL Filter Management** window, click on **URL Filters** in the navigation bar. This window comprises two areas:

- The **Time range selection** area.
- The**Time range list** area.

9.8.3.1.1 SELECT A GLOBAL TIME RANGE

1. In the **Select a time range** zone, choose a time range in the **Global time range** drop-down menu.
2. Click **Apply** to validate.

9.8.3.1.2 ADD A GLOBAL TIME RANGE

1. Click **Add** in the **Time range list** area. The **Time range settings** window displays.
2. In the **Time range name** area, fill in the following field:
   - **Time range name** : type the name you want to assign to the time range.
3. In the **Ranges** area, for each day enter:
   - in the left-hand field: the morning time range
   - in the right-hand field: the afternoon time range

   Type the time range in the left field if the time range is continuous. The format is hh:mm-hh:mm.
4. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

9.8.3.1.3 DELETING A TIME RANGE

Only time ranges that are not activated can be deleted.

Deleting a time range

Click the corresponding **Delete** hypertext link.

Deleting several time ranges

1. Select the time ranges by ticking the box in front of the time range.
2. Click **Delete the selection**.

9.8.3.1.4 CHANGING THE SETTINGS OF A TIME RANGE

1. Click on the name of the time range you want to change. The **Ranges** window displays.
2. Check and/or modify the characteristics of the time range.
3. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

9.8.4 Client Station

9.8.4.1 Configuration procedure

To use the Alcatel-Lucent OmniPCX Office Communication Server proxy it is necessary to configure the Internet navigator on the client workstations.

The browser needs to be instructed that HTTP and FTP requests are to be sent to the proxy: to this end, it is given the IP address of the proxy server (the OmniPCX Office IP address, on the LAN side) and the destination port number, which must correspond to the one entered in OmniPCX Office (**Settings -> Proxy/Cache -> Main -> Proxy Port Number**).

Internet Explorer configuration example

After launching Internet Explorer, the proxy settings can be reached by opening the **Tools -> Internet Options** menu and clicking on **LAN Settings** in the **Connections** tab. Check the **Use Automatic Configuration Script** box and enter the following address in the **Address** field:

- http://<@CPU_IA>/proxy.pac
  <@CPU_IA> represents the IP address or the name of the Internet Access CPU.

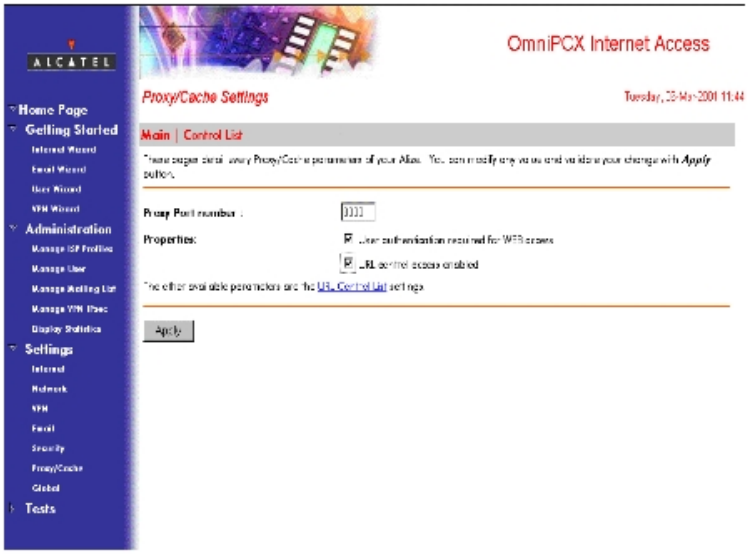
Example:

http://192.168.92.247/proxy.pac

or

http://iaccess.company.world/proxy.pac

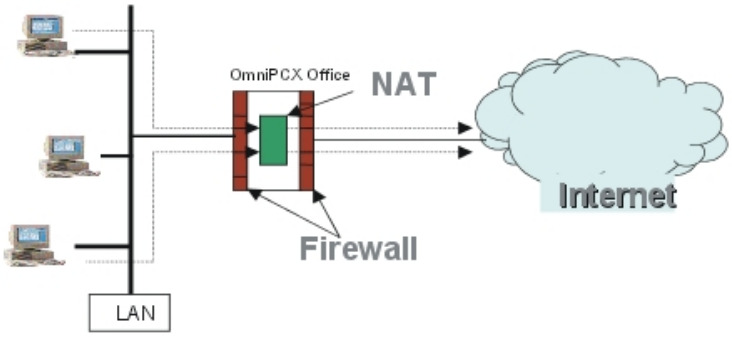
The default name for the IA CPU is iaccess.<domaine_name>.



9.9 Secure Internet Access

9.9.1 Overview

As Alcatel-Lucent OmniPCX Office Communication Server is the gateway between the company LAN and the Internet, it has to guarantee Internet access for LAN users while protecting all machines on the LAN from external intrusions. It is for this purpose that it incorporates the firewall and NAT (Network Address Translation) features.



9.9.2 Firewall

9.9.2.1 Overview

In order to secure the Internet access, Alcatel-Lucent OmniPCX Office Communication Server has a certified firewall, which allows to:

- Protect the LAN against external intrusions.
- Protect Alcatel-Lucent OmniPCX Office Communication Server against external intrusions and intrusions coming from the LAN.
- Limit the availability of Internet Access.

9.9.2.1.1 Description

The firewall integrated into Alcatel-Lucent OmniPCX Office Communication Server uses a connection memory system (Connection Tracking), based on the packets filtering method. In addition to filtering the data packets according to their origins, destination, protocol and port, Connection Tracking examines the context of the data flow. This firewall in particular saves the previous connection states and therefore controls continuously that the circulating data are part of a previously open and authorised session.

The firewall is enabled as soon as the system starts and stays enabled as long as it runs; the system is therefore permanently protected. The firewall configuration adapts itself, in a transparent manner for the administrator, whenever the configuration of the product and its services is modified. The main parameters affecting the firewall's configuration include:

- The software key's content.
  For example, if the Proxy software key is present, it is impossible to access the Internet or to download a file without going through the proxy, unless you explicitly authorize bypass of the Proxy by activating the "Web access" and "File transfer" rules in the rules editor.
- Certain Internet access configuration options:
  - Option to use the Alcatel-Lucent OmniPCX Office Communication Server e-mail server or another e-mail server.
  - The availability of Internet services from the WAN.
  - The VPN availability.

9.9.2.1.2 Filtering rules" editor

The rules" editor allows you to define, modify, enable, disable and delete rules. Each rule

describes a traffic (source, destination, ports and protocols) and its associated action (accept or reject). Upon request, an alarm message concerning the state of the system (accepted or rejected) is issued. The rules editor also makes it possible to change the ordering of the rules, determining the order in which the rules are examined when a packet is received. This order is therefore particularly important when a packet can be processed by two distinct rules. The online help provides all the details about the exact possibilities for configuring the rules and their syntax.

Caution:

The administrator takes responsibility for using the filtering rules" editor, as they may be compromising the network's safety. In this case, the firewall certification is no longer guaranteed.

This tool enables the administrator to define his or her own security rules for the data flow between the LAN and Internet, i.e.:

- the **outgoing** flow: traffic initiated by the LAN and flowing to the WAN.
- the **incoming** flow: traffic initiated by the WAN and flowing to the LAN.

Flows destined for the system are managed transparently by the firewall according to the availability and configuration of the system's services.

The outgoing flow

An outgoing flow rule filters the packets according to their origin and destination addresses, their protocol and their destination port. Unlike incoming flow rules, an outgoing flow rule behaves in the same way whether or not the NAT is activated.

The incoming flow

The incoming flow rules make the services hosted by the LAN servers accessible from Internet. The incoming flow rules are considered differently depending on whether or not the NAT is activated.

- When the NAT is deactivated, an incoming flow rule is considered as an outgoing flow rule, i.e. a packet filter applying to its origin, destination and type.
- When the NAT is activated, the rule only filters the packet's origin address and type. If the packet is accepted, the rule redirects it to the machine on the LAN whose address is indicated in the destination field. The packet is redirected using the "port forwarding" mechanism (see the NAT section).

Predefined rules

The predefined rules in the firewall configuration may be deleted or modified and new rules may be added. Predefined rules are proposed by default to facilitate configuration. In this case certain protocols are incompatible with NAT, when they transmit the stations" IP addresses or original port number in a devious way (generally through the OSI application layer) and thus generate incoherent ports or addresses.

The table below lists the preconfigured rules available, which group certain protocols according to theme. All these protocols are compatible with the NAT.

Pre-configured rules	Application/Protocol	Functionality
Web browsing rule	HTTP/HTTPS	Web search
	Gopher	Web search in text mode
	Wais	Database search

File transfer rule	Ftp (active and passive)	Download file
News Groups rule	Nntp/Nntps	News group
Remote Connection rule	Telnet/ssh	Remote connection
E-mail rule	SMTP	Send/Receive mail
	POP3/IMAP4	Receive mail
Multimedia rule	Quicktime	Multimedia (audio/vidéo)
	CUSEEME	Video-conferencing
	Windows Media	Multimedia (audio/vidéo)
	Real G2 Audio	Multimedia (audio)
Instant messaging rule	MSN Messenger Service	Instant messaging
	ICQ & AIM	Instant messaging
Connectivity test rule	Ping / Traceroute	Network tests
Netbios Protocol Rule	Netbios	Disk mounting (SMB), name resolution

The "Web browsing" and "File transfer" rules are automatically declared on the first start-up if the Proxy software key is not available.

The predefined rules of the Firewall rules editor group the above-mentioned protocols by theme (messaging, multimedia, instant messaging...). When a preconfigured rule is activated, all the machines on the LAN can exploit the protocols associated with this rule on the Internet. By editing these pre-configured rules, you can restrict:

- The LAN machines able to access the service, by limiting the source addresses and/or,
- the servers accessible on the Internet, by limiting the destination addresses.

9.9.2.1.3 Firewall events log

The firewall events are saved separate from other events linked to the system (for example in case of dysfunction). The packets saved include:

- Packets coming from the WAN and rejected by the firewall.
- Packets starting a new connection and stopped by an entry into the rules" editor, whose role is to trace the packets.

9.9.2.1.4 Firewall Rule Settings

The various firewall rule settings include:

- Protection of the WAN interface. By deactivating this setting it is possible to delete filtering of the flows from the WAN to the LAN. This adjustment setting is useful when instead of being directly connected to the Internet, the WAN is connected to a company network protected by another firewall.
- Disabling the NAT, in case of an external router connection, for example.
- Accessibility of the services giving Internet access from the WAN, i.e. the DNS server, the mail server (SMTP, POP3, IMAP4), the Web proxy, the Intranet Web server and the FTP server. This adjustment setting is useful for example in the case of an External Router connection.
- Access to a Web configuration from the WAN, in case of external router connection or

remote maintenance, for example.

Remark:
When the configuration, service or LAN are opened up to Internet, the system is exposed to external attack.

9.9.3 NAT

9.9.3.1 Overview

9.9.3.1.1 Presentation

NAT is a mechanism devised to palliate the shortage of web addresses. It enables a group of computers in a local network to access the Internet using a single IP address, in this case that of Alcatel-Lucent OmniPCX Office Communication Server, which makes it appear as the only system using the Internet connection.

Remark:
Alcatel-Lucent OmniPCX Office Communication Server only has the IP address officially provided by the active ISP at any given time. The correlation of addresses in the NAT process is always of the type: n local addresses to 1 public address.

9.9.3.1.2 Operation

Computer X, located on the LAN, is instructed that Alcatel-Lucent OmniPCX Office Communication Server is its default gateway.

When a packet arrives in Alcatel-Lucent OmniPCX Office Communication Server from computer X, it is assigned a new available source port number, and the OmniPCX Office IP address is declared in the packet header, without overwriting the original header. It then sends the changed packet to Internet.

When a packet arrives in Alcatel-Lucent OmniPCX Office Communication Server from the Internet, if the destination port number is one of the source ports assigned in the preceding stage, then the header is again modified to restore the original port numbers and IP addresses, and the packet is passed on to machine X.

9.9.3.1.3 Advantages

These advantages are:

- flexibility in the private address plan of the LAN;
- the shared use of a single public IP address for any number of private addresses in the LAN;
- Increase in security via concealment of the company network from Internet.

9.9.3.1.4 Restrictions

There are two types of restriction:

1. An Alcatel-Lucent OmniPCX Office Communication Server user (see the "Users and User Groups" file) is the client of an Internet service. The predefined rules comprise all the protocols compatible with the NAT.
   The table gives a non-exhaustive list of the applications or protocols that are incompatible with the NAT and are not supported.

Application/Protocol	Functionality
Applications H.323	Internet telephony
IRC	Instant messaging
Archie	FTP search

2. A computer on the local network hosts a service for clients on the Internet (i.e. acts as a web server).
   The functioning principle of the NAT prohibits this type of topology. However, thanks to Alcatel-Lucent OmniPCX Office Communication Server's port forwarding feature, a server located on the LAN is made accessible from Internet, if the protocols concerned remain compatible with the NAT. This forwarding is configured using the firewall rules for incoming flows (see the "Filtering rules" editor" section). When messaging is configured in "server hosted on the LAN" mode, the appropriate rules are automatically added to the firewall rules" editor.

9.9.4 Managing Firewall Rules

9.9.4.1 Operation

The firewall rules are defined for the outgoing and incoming flows. We refer to outgoing rules and incoming rules. Incoming and outgoing rules are configured in the same way.

Management of the firewall rules, whether incoming and outgoing, comprises the following tasks:

- Adding a rule,
- Modifying a rule's properties,
- Deleting one or more rules,
- Enabling one or more rules,
- Disabling one or more rules.

The procedures below are described in the case of outgoing rules. They are identical for incoming rules, except when the NAT is activated.

Important:

It is recommended to read the online help available before starting to configure the firewall rules.

9.9.4.1.1 Accessing the Firewall Rules" Editor window (incoming or outgoing)

Click on **Firewall** in the navigation bar. The **Firewall Rules" Editor - Outgoing Rules** window is displayed. This window comprises two areas:

- The **Enabled Rules** area, which lists all the enabled firewall rules.
- The **Disabled Rules** area, which lists all the disabled, but already created, firewall rules.

Remark:

*To access the incoming rules, click on the hypertext link **Incoming Rules**. You access the **Firewall Rules" Editor - Incoming Rules** window, identical to the **Firewall Rules" Editor - Outgoing Rules** window.*

9.9.4.1.2 ADDING A RULE TO THE FIREWALL

1. Click **Add**:
   - either in the **Enabled Rules** area so that the new rule is enabled,
   - or in the **Disabled Rules** area so that the new rule is created but not enabled.

   The **Firewall Outgoing Rules" Settings** window is displayed.
2. In the **Rule identification** area, fill in the following field:
   - **Rule Number**: defines the order of the rules (see online help).
   - **Rule name**: allows customizing of the rule by giving it a name.
   - **Source**: see online help.
   - **Destination**: see online help.
   - **Destination protocol and port**: see online help.
     In the **Firewall action** drop-down list, select the action associated with the defined traffic. Four choices are available:
     - Accept
     - Accept and log
     - Reject
     - Reject and log
3. In the **Comment** area, enter the comment describing the rule's objective.
4. Click **Apply** to accept the data, or click **Cancel** if you do not want to keep the changes.

Remark:

*Depending on your choice during step 1, the new firewall rule appears in the **Enabled Rules** or **Disabled Rules** area.*

9.9.4.1.3 MODIFYING A FIREWALL'S RULE PROPERTIES

A firewall rule can be edited, whether it is enabled or disabled.

1. Click the name of the rule you want to edit. The **Firewall Outgoing Rules" Settings** window is displayed. You have access to all the selected rule's settings.
2. You can modify the following areas" fields:
   - **Rule definition** area
   - **Comment** area

   as defined in the "Adding a firewall rule" section.
3. Click **Apply** to accept the data, or click **Cancel** if you do not want to keep the changes.

9.9.4.1.4 DELETING ONE OR SEVERAL FIREWALL RULES

A firewall rule can be deleted, whether it is enabled or disabled. When the firewall rule is deleted, it disappears from the **Enabled Rules** or **Disabled Rules** areas.

Deleting a rule

Click the corresponding **Delete** hypertext link.

Deleting several rules

1. Select the firewall rules by checking the box preceding the rule's name.
2. Click the **Delete the Selection** button.

9.9.4.1.5 ENABLING ONE OR SEVERAL FIREWALL RULES

When you enable a rule, it disappears from the **Disabled Rules** area and it appears in the **Enabled Rules** area.

Enabling a rule

In the **Disabled Rules** area, click the corresponding **Enable** hypertext link.

Enabling several rules

In the **Disabled Rules** area:

1. Select the rules by checking the box preceding the rule's name.
2. Click the button **Enable the Selection**.

9.9.4.1.6 DISABLING ONE OR SEVERAL FIREWALL RULES

When you disable a rule, it disappears from the **Enabled Rules** area and it appears in the **Disabled Rules** area.

Disabling a rule

In the **Enabled Rules** area, click the corresponding **Disable** hypertext link.

Disabling several rules

In the **Disabled Rules** area:

1. Select the rules by checking the box preceding the rule's name.
2. Click the **Disable the Selection** button.

9.9.4.1.7 CHANGING THE FIREWALL SETTINGS

Important:

It is recommended to read the online help available before taking any action concerning the firewall.

1. Click on **Firewall** in the navigation bar. The **Firewall Rules Editor - Outbound Rules** window is displayed.
2. Click the **Firewall Settings** hypertext link. The **Firewall Settings** window appears.
3. In the **Firewall protection scope** area of the **General** tab, you can disable control of the firewall filtering the packets passing between the LAN and the WAN, by unchecking the **WAN-LAN Filtering** box.
4. In the **HTTP/HTTPS** tab, you can make Internet services accessible from the WAN.
   a. Check the **HTTPS Services** box to make the following HTTPS services available:
   - ACD
   - Management server
   - Software download
   - Taxation
   - Music on hold
   - Monitor

- Webdiag
- Web services

b. Check the **Web-Based Management (WBM)** and/or the **Web Communication Assistant** box to open access the these applications.

c. Check the **HTTP Services** box to make telephony services available through HTTP and the Intranet Web Server:

Note 1:
At this time the list of available HTTP telephony services is empty.

5. In the **Other Services** tab, you can make the following services available from the WAN using other protocols:
   - Email Server (SMTP, POP3, and MAP4)
   - Web Proxy
   - DNS Server
   - Intranet file servers (FTP and SMB)
   - Ping
   - IP Softphone

Note 2:
Adding or removing firewall rules is not applied to the established data flow.

9.10 Anti-Virus

9.10.1 Overview

An anti-virus software is an application or application suite that detects viruses and suppresses them.

This service is not provided by Alcatel-Lucent OmniPCX Office Communication Server. The anti-virus software is installed on a dedicated LAN server and protects the following solutions in Alcatel-Lucent OmniPCX Office Communication Server:

- E-mail
- Web page transfer (HTTP protocol)
- File transfer (FTP protocol)

Remark 1:
The dedicated must have a static IP address.

The same anti-virus software can be used for E-mail, file transfers and Web page transfers. The anti-virus software for e-mail and HTTP/FTP flows can function on two different servers.

Remark 2:
It is not recommended to use the dedicated server as a client station. In this case, a special configuration is needed.

In the sections below, a general presentation is given of how to protect e-mails and the HTTP/FTP flows against viruses, and then we explain how to configure this protection on Alcatel-Lucent OmniPCX Office Communication Server.

9.10.1.1 Alcatel-Lucent OmniPCX Office Communication Server e-mail protection

The anti-virus software is only enabled when Alcatel-Lucent OmniPCX Office Communication Server is the mail server.

Incoming e-mails (including attached files) are sent directly to the anti-virus server and tested. Non-infected e-mails are forwarded to the recipients.

9.10.1.2 Protection of HTTP and FTP flows

The Web pages and files transferred by FTP are sent directly to Alcatel-Lucent OmniPCX Office Communication Server, and then tested by the anti-virus software. Non-infected Web pages and files are forwarded to the recipients.

Remark:

It is impossible to bypass the anti-virus software. If the dedicated hardware or software is out of service, the customer cannot access Internet, or transfer files.

For the HTTP flow, if a virus is detected an alert window is displayed during navigation on Internet. For the FTP flow, if a virus is detected the program indicates that they system has detected a virus. In both cases, the administrator can be informed.

9.10.2 Configuration procedure

To configure an external anti-virus software:

1. Click on **Wizards** in the navigation bar. The assistants" icons appear.
2. Click on the **Anti-Virus Wizard** icon. The **Anti-Virus Wizard** window is displayed.
3. In the **External anti-virus on the LAN** area, check the:
   - **E-mail verification** box to enable the anti-virus for e-mails.
   - **HTTP/FTP flow verification** box to enable the anti-virus on HTTP and FTP flows.
4. Type in the address of the dedicated PC connected to the LAN in the:
   - **Location of e-mail anti-virus** field, if you've enabled the anti-virus for e-mails.
   - **Location of the HTTP/FTP anti-virus** field, if you've enabled the anti-virus for HTTP and FTP flows.
5. Click on **Next**. The **Summary** window displays. This window lists all the options you've chosen. Click **Previous** to return to the previous screens and modify the desired parameters.
6. Click **Finish** to validate the parameters. The **Anti-virus Management** window is displayed, showing the configuration of your anti-virus software.

9.10.2.1 TESTING THE EXTERNAL ANTI-VIRUS SOFTWARE

To test the external anti-virus software:

1. Click on **Anti-virus** in the navigation bar. The **Anti-virus Management** window is displayed.
2. Click the **Test** button. The test runs all the stages for configuring an external anti-virus software, and gives the causes and related solutions to solve the problem if the test fails.
   - For configuration of an e-mail anti-virus software, the test verifies in succession:
     - the OmniPCX Office SMTP server
     - the ISP SMTP server name
     - the ISP SMTP server

- the OmniPCX Office POP3 server
- the ISP POP3 server name
- the ISP POP3 server
- the address of the external anti-virus software
- the SMTP connection with the anti-virus software

- For configuration of an anti-virus software for HTTP/FTP flows, the test verifies in succession:
  - the address of the external anti-virus software
  - the connection with the HTTP anti-virus software
  - the connection with the FTP anti-virus software

9.10.3 Operation

9.10.3.1 SETTING ANTI-VIRUS PARAMETERS IN Alcatel-Lucent OmniPCX Office Communication Server

To set the external anti-virus software parameters:

1. Click on **Anti-virus** in the navigation bar. The **Anti-virus Management** window is displayed.
2. Click the **Anti-virus Settings** hypertext link. The **Anti-virus Settings** window is displayed. It has the following tabs:
   - **E-mail**
   - **HTTP/FTP**
3. Click on the **E-mail** tab. This tab is used to activate or deactivate the anti-virus software for e-mails.
   a. If you select **None**, the anti-virus software is not activated.
   b. If you select **External anti-virus on the LAN**, the anti-virus software is activated. Enter the address of the dedicated PC connected to the LAN in the **Anti-virus Location** field.
   c. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes. The **Anti-virus Management** window is displayed.
4. Click on the **HTTP/FTP** tab. This tab is used to activate or deactivate the anti-virus software for HTTP/FTP flows.
   a. In the **HTTP/FTP Anti-virus** area, select:
   - **None** if you don't want to activate the anti-virus software.
   - **External anti-virus on the LAN**, if you want to activate the anti-virus software. Enter the address of the dedicated PC connected to the LAN in the **Anti-virus Location** field.
   - Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

   b. In the **FTP Clients** area, check the **Authorizes FTP connections via the anti-virus proxy** box if you want to transfer files between FTP clients and Internet via the anti-virus proxy.
   c. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes. The **Anti-virus Management** window is displayed.

9.11 Security

9.11.1 Overview

To protect the Alcatel-Lucent OmniPCX Office Communication Server Internet services, the following protection mechanisms are integrated into the system:

1. Passwords.
2. Passive security.
3. Active security.

The protection mechanisms provided by Alcatel-Lucent OmniPCX Office Communication Server office make it possible to implement an active and passive approach to security. However, to guarantee the LAN's global security, you must:

- Consider the security of all the LAN's elements, and not just the point of access (e.g. a modem connected to Internet via a PC destroys the security model).
- Use an appropriate methodology (e.g. vulnerability monitoring).

This section deals successively with the different security mechanisms.

9.11.1.1 PASSWORDS

The administrator and operator passwords giving access to the WBM from the LAN, are defined by default.

It is impossible to access the WBM from the WAN with the "admin" or "operator" accounts. To access the WBM from the WAN, you must create a user that has administrator or operator rights.

When migrating from an installation implementing an R1.X or R2.0 solution to an installation implementing an R2.1 solution, the administrator password is restored and the operator password takes the default value.

To make the system secure, it is possible to change the administrator and operator passwords via the WBM.

1. Click on **General** in the navigation bar. The **General** window displays.
2. Click on the **Password** tab.
3. In the **Operator password** area, fill in the following fields:
   - **Old password**
   - **New password**
   - **Confirm password**
4. In the **Administrator password** area, fill in the following fields:
   - **Old password**
   - **New password**
   - **Confirm password**
5. Click **Change** to validate the changes.

Remark:

*If the old password is entered incorrectly, the **Web-Based Management - Error** window is displayed, giv-*

ing the causes and the solutions to the problem.

9.11.1.2 PASSIVE SECURITY

Passive security comprises all preventive actions that protect Alcatel-Lucent OmniPCX Office Communication Server against any attack. The following actions are available:

1. Utilization of the defined password format.
2. Resetting of the administrator password.
3. Closure of the system to the WAN.

9.11.1.2.1 Utilization of the defined password format

The administrator, operator and user passwords must comply with the following rules:

- comprise 6 to 8 characters,
- comprise at least one upper-case letter,
- comprise at least one non alphanumeric character.

The password format is verified when it is crated or changed in the WBM.

9.11.1.2.2 Resetting of the administrator password

When a password is lost, the administrator can reset it by deleting the existing password.

Resetting of the administrator password can be configured by OMC (Expert view). Proceed as follows:

1. **OMC** -> **System Miscellaneous** -> **Password**
2. Select **IA** in the **Level** drop-down menu and click on **Reset**.

Remark:
OMC cannot reset the operator password. However the administrator can change the operator password via WBM. For more information, consult the "Passwords" section.

9.11.1.2.3 Closure of the system to the WAN

By default, Alcatel-Lucent OmniPCX Office Communication Server is not open on the WAN. This prevents any risk of piracy. If Alcatel-Lucent OmniPCX Office Communication Server is opened on the WAN, the firewall protects the system against any attack. For more information about the firewall, consult the "Making Internet access secure" file.

9.11.1.3 ACTIVE SECURITY

Active security groups together the actions that actively control attacks that are external in origin.

9.11.1.3.1 Authentication failed

After 5 consecutive authentication failures, Alcatel-Lucent OmniPCX Office Communication Server puts the relevant PC in quarantine for 30 minutes. During this time, the firewall blocks any request emanating from this PC.

Every authentication failure is logged in a log file. This file contains the PC's IP address and the user account. These log files are accessed via the WBM dashboard. To access the WBM dashboard, consult the "Administration" file.

Remark:

Every attempt to connect with an administrator, operator or user account undergoes this process.

9.12 Administration Tools

9.12.1 E-mail Notification

9.12.1.1 Overview

This service makes it possible to configure in a uniform way all the notifications originating from e-mail services (notifications of user disk space threshold) and PKI certificates (notifications of current certificate's expiry).

The administrator configures a general e-mail address for all notifications, and if necessary a specific address for each service concerned. For more information, consult the "E-mail" and "VPN" sheets.

The general e-mail address can be:

- the address of a user
- a broadcasting list
- an external address
- a user alias

The administrator is able to configure an e-mail address to receive the e-mails automatically sent to the postmaster (e-mail alias that groups all the e-mail addresses of users who have administrator rights). These alerts give notification of service malfunctioning.

9.12.2 Hard Disk Management

9.12.2.1 Overview

Alcatel-Lucent OmniPCX Office Communication Server's hard disk contains all the data pertaining to the offered Internet services, i.e.:

- e-mail messages
- file server files
- Intranet Web server files
- Voice mail messages
- URL filters.

9.12.2.1.1 Hard disk partition

Partitioning a hard drive is convenient because it allows a better organization of the data through assigning a storage space to each feature of the Alcatel-Lucent OmniPCX Office Communication Server and slicing the hard disk into several virtual sub-sections.

Alcatel-Lucent OmniPCX Office Communication Server has two types of partitions. Fixed-size partitions for the applications, and variable sized partitions, depending on the size of the selected hard drive.

The following partitions have been created on the Alcatel-Lucent OmniPCX Office Communication Server hard drive:

- one partition for the software,
- one for swap,
- one partition for the file server,
- one for the electronic messaging,
- one partition for the proxy,
- one for voice mail,
- one for the Intranet.

9.12.2.1.2 Data backup and restoration

To avoid losing data after a hard drive crash, Alcatel-Lucent OmniPCX Office Communication Server is equipped with a backup mechanism for all existing files. This mechanism also creates backup files for the configuration of telephony and Internet services. The backup is done on network equipment.

In the event of a hard disk replacement, all data are restored on the new hard disk from the last backup operation.

The backup can be manual or automatic. If it is automatic, the administrator programmes how often and at what time the backup is carried out. Data restoration is manual.

9.12.3 Information and Statistics

9.12.3.1 Overview

The administrator can obtain advanced statistics on system activity over a period of time or at a given time, and on application aspects, thanks to the statistics tool integrated in Alcatel-Lucent OmniPCX Office Communication Server. These data can be accessed through the WBM interface. These statistics are shown in tables with the possibility of accessing graphics allowing the user to view the evolution over time.

Two types of information are accessible via WBM:

- **Snapshot information**: system activity measures saved in real time.
- **Statistics** : information stored on the Alcatel-Lucent OmniPCX Office Communication Server's hard disk (system activity statistics and applications statistics).

Snapshot information can be viewed in tables. These statistics can be viewed in graphics (by day or fortnight) or in tables.

9.12.3.1.1 Snapshot information

System activity information shown in the statistics tool relate to:

- System information,
- management of the memory and swap, as well as the processor load,
- hard disk utilisation (partition),
- network traffic.

9.12.3.1.2 Statistics

Statistics on the Internet services offered by Alcatel-Lucent OmniPCX Office Communication Server are stored in log files. Three types of statistical analysis are available:

- Statistics on HTTP resources access: Proxy server (HTTP or FTP protocol) and Intranet Web server.
- Statistics on e-mail service.
- Statistics on the various connection types: Internet connections (DSL or ISDN modem), VPN and RAS connections.

9.12.3.1.3 Log file export

Log files (alert messages) contain the raw data. The following types of log files are available:

- E-mail server logs.
- Proxy server logs.
- System event logs.
- Security event logs.
- The logs sent to telephony.

Remark:

These alert messages are also indicated on the Network Management Center (NMC).

9.12.4 Access to the Dashboard

9.12.4.1 Operation

Click on **Dashboard** in the navigation bar. The **System Dashboard** window appears. This window has the following tabs:

- **Statistics**
- **Information**
- **System**
- **Partitions**
- **Network**

1. Click on the **Statistics** tab. This tab shows system application statistics. Three types of statistics are defined:
   - Connection statistics: to access those statistics, click on the hyperlinks in the **Internet connections**, **VPN Connections** or **RAS Connections** areas.
     - The **Available statistics** table lists connection indexes with the appropriate counters.
     - For each month, the hyperlink makes it possible to access the monthly connection details. In case of VPN or RAS connections, the hyperlink list may contain an additional link (User connections) for the analysis period. In those cases, the page contains an additional table listing all users who have established a connection along with their statistics. The **Summary** table contains a counter-based summary. The **Daily Connections** graphic represents all days of the month when

connections have been established. The histograms correspond to the connection duration, and they are labelled in hours. The **Connection List** table lists all connections established in the course of the month. The "Status" column shows a successful connection.

- E-mail statistics: to access those statistics, click on the **See e-mail statistics** hyperlink in the **Internet utilisation** area.
  - The **Mailbox sizes** table lists the local mailboxes with their sizes. The **Available statistics** table lists the months for which statistics are available.
  - For each month, the hyperlink makes it possible to access the monthly index details. The **Summary** table contains a counter-based summary. The **Daily Messages** graphic shows the times at which the mail server has been accessed the most. The first table lists machines with which the local server has processed the most messages: the transmitting machines first, then the external servers. The other two tables show the accounts which received most of the e-mail messages, and those which transmitted the most.
- Webalizer statistics: to access those statistics, click on the **Proxy statistics** and **Intranet web statistics** hyperlinks in the **Internet utilization** area.

2. Click on the **Information** tab. This tab shows system statistics. They are specific to the hardware configuration and the software version. Therefore, they remain unchanged as long as Alcatel-Lucent OmniPCX Office Communication Server is running. They are gathered as Alcatel-Lucent OmniPCX Office Communication Server boots up.
3. Click on the **System** tab. This tab shows system snapshot information. This information shows the system status at a given moment.
   - Click on the **CPU Loads**, **Memory used** or **Swap used** hyperlinks to open the **System Graph** window. Each graphic shows the evolution for the dynamic data period.
     - If necessary, use the **Automatic scaling** option.
     - The drop-down list allows the user to choose between an hourly synthesis and a daily synthesis.
   - Click on the **Process** hyperlink to open the **Process Tree** window. The process tree is mainly used to identify errors.
     - The **Close** button causes the window to close.
     - The **Refresh** button allows the data to be updated.
   - Click on the **Refresh** button to update the dynamic information.
   - Check the **Auto-refresh** box to automatically update the data every 7 seconds.
4. Click on the **Partitions** tab. This tab lists the partitions on the system, their mount points, capacities and occupancy rate.
   - Click on the partition-related hyperlinks to open the **System Graph** window. Each graphic shows the partition occupancy over time.
     - If necessary, use the **Automatic scaling** option.
     - The drop-down list allows the user to choose between an hourly synthesis and a daily synthesis.
   - Click on the **Refresh** button to update the partition rates.
5. Click on the **Network** tab. This tab displays detailed information on the network interface usage.
   - Click on the interface-related hyperlinks to open the **System Graph** window. Each graphic shows the network traffic over time.
     - If necessary, use the **Automatic scaling** option.

- The drop-down list allows the user to choose between an hourly synthesis and a daily synthesis.

- Click on the **Refresh** button to update the information.

a.

9.12.5 Configuring Backup

9.12.5.1 Configuration procedure

The backup configuration consists of three main tasks:

- Configuration of the backup system,
- manual backup management,
- modification of the backup system.

9.12.5.1.1 CONFIGURATION OF THE BACKUP SYSTEM

Click on **Wizards** in the navigation bar. The six wizard icons are displayed.

1. Click on the **Backup Wizard** icon. The **Backup Wizard** window appears.
2. In the **Backup device** area, include the following fields:
   - **Workgroup or domain**: allows your server to be integrated in a Microsoft network.
   - **Network share**: gives the path to a particular directory on a network device.
   - **User Name**: enter the user name of the network device on which you want to store your backup.
   - **Password**
   - **Confirm Password**
3. Click on **Next**. Depending on the parameters already configured, you access the **Option 1: Add a DNS entry** area or the **Option 2: Define the WINS server** area.
   a. In the **Option 1: Add a DNS entry** area, include the following fields:
      - **User Name**: enter the user name of the network device on which you want to store your backup.
      - **IP Address**: Enter the IP address associated with the network device.

   b. In the **Option 2: Define the WINS server** area, include the following field:
      - **WINS Server**: If your network has a WINS server, you may enter its name.
4. Click on **Next**. A new window appears.
5. In the **Backup device** area, include the following fields if necessary:
   - **IP Address**: enter the IP address associated with the network device.
   - **Gateway**: Enter the IP address of the gateway to contact in order to reach the destination address.
   - **Sub-network Mask**: enter the sub-network mask associated with the destination address.
   - **Comment**: comment for identifying the route entered.
6. Click on **Next**. A new window appears.
7. In the **Periodicity** area, select **Backup trigger** in the drop-down menu, the rate of the backup, and in the **Hours** field, enter the time of the backup trigger.
8. Click on **Next**. The **Summary** window appears which displays the various backup features.

9. Click on **Finish**.

9.12.5.1.2 MANUAL BACKUP MANAGEMENT

To access the **Backup Management** window, click on **Backup** in the navigation bar.

1. In the **Manual backup** area, click on the **Backup** button to start the full system backup.
2. The **Backup list** area shows all the backups already carried out. To delete one or more list backups, click on the **Delete** button or on the **Delete Selection** button.

9.12.5.1.3 MODIFICATION OF THE BACKUP SYSTEM

1. In the **Backup Management** window, click on **Backup settings** hyperlink. The **Backup Settings** window appears.
2. Click on the **Settings** tab. This tab displays the information needed to set up the backup of your system on a network device.
   a. In the **Backup device** area, include the following fields:
   - **Workgroup or domain**: allows your server to be integrated in a Microsoft network.
   - **Network share**: gives access to a particular directory on a network device.
   - **User Name**: enter the user name of the network device on which you want to store your backup.
   - **Password**
   - **Confirm Password**

   b. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.
3. Click on the **Behaviour** tab. This tab displays the information needed to set up the backup behaviour.
   a. In the **Periodicity** area, select **Backup trigger** in the drop-down menu, the rate of the backup, and in the **Hours** field, enter the time of the backup trigger.
   b. In the **Backup history** area, include the following field:
   - **Size of backup history**: enter the number of backups you wish to keep on the network device.

   c. Click on **Apply** to validate the data, or on **Cancel** if you do not wish to keep the changes.

9.12.6 Test Management

9.12.6.1 Operation

Click on**Tests** in the navigation bar. The **Test tools** window appears. This window is made up of the following tabs: **Connection**, **Services** and **Network**.

1. Click on the **Connection** tab. This service allows to test the current connection profile. The tool uses the test web site to test the name resolution and the ping in order to verify that the connection profile works properly. Click on the **Test** button to start the connection test tool.
2. Click on the **Services** tab. This service tests e-mail and backup services. Choose the service you want to test, then click **Test** to start the service test tool.
3. Click on the **Network** tab. Click **Ping** or **Traceroute** or **NsLookup** to start testing these

utilities. The **Routing Table** button gives access to the system's internal routing table.

9.12.7 General Menu

9.12.7.1 Operation

Click on **General** in the navigation bar. The **General** window displays. This window is made up of the following tabs: **Software**, **Hardware**, **Configuration Passwords** and **Miscellaneous**.

1. Click on the **Software** tab. This tab lists the software keys installed on your system and indicates whether it is available or not for each service.
2. Click on the **Hardware** tab. This tab indicates whether a specific hardware component is present or not.
3. Click on the **Configuration** tab. This tab allows to download a configuration file into the system and to save your system's current configuration file or to reset to factory settings.
4. Click on the **Password** tab. This tab is used to change the operator and administrator passwords. For more information, consult the "Security" section.
5. Click on the **Miscellaneous** tab. This tab allows to:
   - Install the WBM SSL certificate by clicking the **Install the certificate** button in the **Web-Based Management SSL certificate** area.
   - Define the system's default language by selecting the language of your choice in the **System default language** area's drop-down menu, then clicking on the **Change** button.

9.12.8 Management of E-mail Notifications

9.12.8.1 Operation

Management of e-mail notifications comprises several tasks:

- Configuration of the general e-mail address
- Configuration of the Postmaster's e-mail address

Click on **Notification** in the navigation bar. The **Notification management** window appears. This window comprises several areas:

- The **General e-mail address for notifications** area gives the general e-mail address used when there is no specific e-mail address. This address is configured in the **Notifications** tab of the **Notification Settings** window.
- The **Postmaster e-mail forwarding** area gives the postmaster's address. This address is configured in the **Postmaster** tab of the **Notification Settings** window.
- The **Service Settings** area lists all the services that may send notifications, in the form of a table. To access the pages where you can change these settings, click on the **Change** hyperlink in the **Action** column.

9.12.8.1.1 Configuration of the general e-mail address

1. In the **Notification Management** window, click on the **Notification Settings** hyperlink. The **Notification Settings** window is displayed. This window has two tabs: **Notifications** and **Postmaster**.
2. Click on the **Notifications** tab.

3. Enter the general e-mail address in the **E-mail address** field of the **General e-mail address for notifications** area.

9.12.8.1.2 Configuration of the Postmaster's e-mail address

1. In the **Notification Management** window, click on the **Notification Settings** hyperlink. The **Notification Settings** window is displayed. This window has two tabs: **Notifications** and **Postmaster**.
2. Click on the **Postmaster** tab.
3. In the **Postmaster e-mail forwarding** area, select the required type of forwarding. Three choices are available:
   - **Do not use forwarding of Postmaster e-mails**
   - **Use a specific e-mail address**: an e-mail address is configured to receive e-mails sent automatically to the postmaster. In the **E-mail Address** field, type in the address for reception of these e-mails.
   - **Use the general e-mail address for notification**: the forwarded e-mails are sent to the general e-mail address configured by the administrator.

9.13 Troubleshooting

9.13.1 Troubleshooting procedures and guides

Implementing Alcatel-Lucent OmniPCX Office Communication Server and its functionalities brings into play three main elements which may lie behind any problems encountered on installation and configuration. They are:

- the client station;
- the system (OmniPCX Office);
- the Internet access provider.

9.13.1.1 INTERNET ACCESS

9.13.1.1.1 Nothing works: check that all the network elements can communicate with each other.

1. Alcatel-Lucent OmniPCX Office Communication Server fails to respond to a ping from all PCs. Alcatel-Lucent OmniPCX Office Communication Server does not have LAN access.
   - Check the Ethernet connections, and the IP address on the LAN side.
   - Check that the LAN settings in the **Settings -> Network** menu are correct.
2. OmniPCX Office fails to respond to a ping from a particular PC. There is a network problem on the PC.
   - Check the connections (network cable and board).
   - Check the network settings (**Network** icon in the control panel).
3. Alcatel-Lucent OmniPCX Office Communication Server responds to a ping from all PCs. Alcatel-Lucent OmniPCX Office Communication Server is properly configured at LAN level. The problem therefore lies in the Internet connection.

9.13.1.1.2 Alcatel-Lucent OmniPCX Office Communication Server can't connect up to the

ISP

1. Check the ISDN connection.
2. Check the connection settings provided by the ISP and configured in Alcatel-Lucent OmniPCX Office Communication Server.
3. Check that the ISP profile is active, and that communication has not been deactivated.
4. Use the connection test tool provided on Alcatel-Lucent OmniPCX Office Communication Server (click on **Connection** in the navigation bar, then on **Connection test** in the general information banner or on the **Test** button in the **Selecting the Active Connection Profile**) area. This tool carries out the connection to the ISP step by step, and gives the main causes of the problem and the solutions, if a connection step fails.

9.13.1.1.3 The browser on the PC can't access web sites.

1. Alcatel-Lucent OmniPCX Office Communication Server fails to respond to a ping from the PC. See the instance above.
2. Alcatel-Lucent OmniPCX Office Communication Server responds to a ping from the PC. This is caused by either:
   - an Internet navigator configuration problem. Check that this configuration corresponds to the Alcatel-Lucent OmniPCX Office Communication Server security function (proxy software key active or not).
   - a security problem:
     - If user access control is enabled, check that the user has been properly declared. If necessary, change the password.
     - If web access control is enabled, check that the site is authorized.
     - If a particular protocol is being used, check that it is correctly configured in Alcatel-Lucent OmniPCX Office Communication Server.

9.13.1.2 E-MAIL

When a client station can't send and/or receive e-mail, check the following:

1. The POP3 mailboxes are hosted by the ISP.
   - Check the mail server configuration on Alcatel-Lucent OmniPCX Office Communication Server.
   - Check the POP3 account settings (name and password) for the user created in Alcatel-Lucent OmniPCX Office Communication Server.
   - Test the mail server configuration using the testing tool included in Alcatel-Lucent OmniPCX Office Communication Server. The tool will test the ISP's mail server and suggest appropriate solutions in the event of failure.
   - Contact the ISP to check that the POP3 accounts are valid.
   - Check the mail client configuration. Alcatel-Lucent OmniPCX Office Communication Server should be the POP3 and SMTP server. The POP3 login and password for each user should correspond to the OmniPCX Office settings.
2. The ISP is the SMTP relay for the messaging service.
   - Check the mail server configuration on Alcatel-Lucent OmniPCX Office Communication Server.
   - Test the mail server configuration using the testing tool included in Alcatel-Lucent OmniPCX Office Communication Server. The tool will test the ISP's mail server and

suggest appropriate solutions in the event of failure.

- Contact the ISP.
- Check the mail client configuration. Alcatel-Lucent OmniPCX Office Communication Server should be the POP3 and SMTP server. The POP3 login and password for each user should correspond to the OmniPCX Office settings.

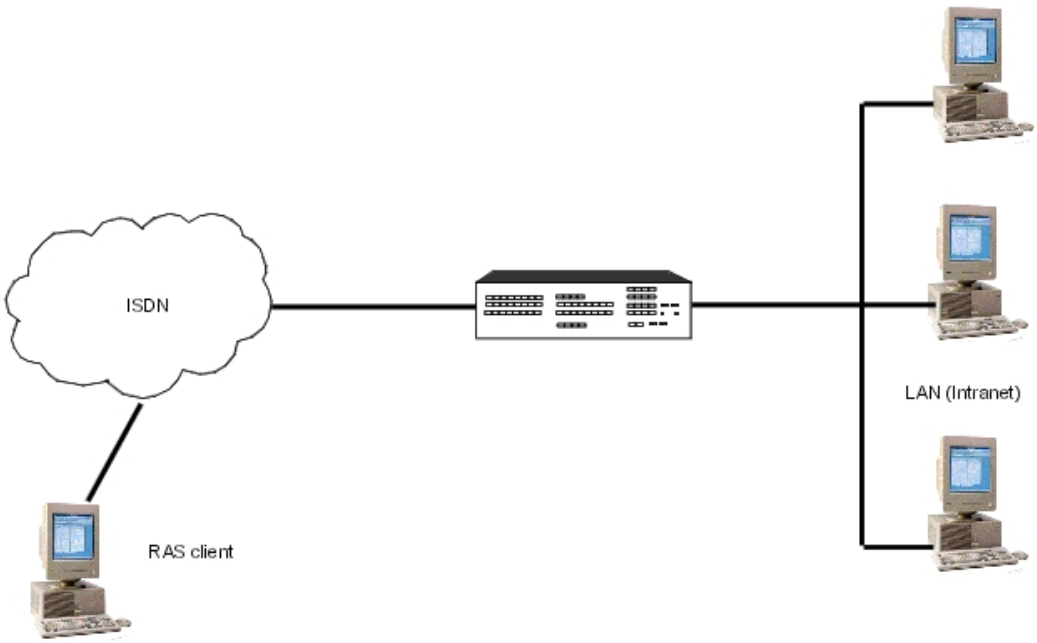
3. The ISP has a direct SMTP connection to Alcatel-Lucent OmniPCX Office Communication Server. Check the configuration of Alcatel-Lucent OmniPCX Office Communication Server, and of the ISP.

9.14 Remote Access Server

9.14.1 Overview

The RAS (Remote Access Server) feature allows remote clients to connect seamlessly to the corporate network from the outside.

This section describes the **dialling remote access** mode offered by Alcatel-Lucent OmniPCX Office Communication Server. This mode allows a remote client to use the ISDN network to connect to the corporate LAN. Once they are connected, the RAS clients (telecommuting or mobile workers) can use the corporate LAN resources as if they were connected locally. They can share files, query databases, access their e-mails, print files, etc.).



Note:
*Alcatel-Lucent OmniPCX Office Communication Server also allows the **remote access via VPN** mode where a remote client uses an IP sub-network to establish a virtual point-to-point connection to Alcatel-Lucent OmniPCX Office Communication Server.*

9.14.1.1 AVAILABILITY

RAS is available with the following solutions:

- Business (CPU, CPU-1/CPU-2)
- e-Business (CPUe-1/CPUe-2)

9.14.2 Services provided

9.14.2.1 On-demand bandwidth

With MPPP (Multi-link Point-to-Point Protocol), an RAS client can dynamically make/release a second ISDN call to the RAS server in order to decrease/increase its bandwidth from 64 to 128 Kbps.

Thus, an Alcatel-Lucent OmniPCX Office Communication Server system with 16 simultaneous RAS accesses can support a maximum of:

- 16 accesses with a bandwidth of 64 Kbps
- or 8 accesses with a bandwidth of 128 Kbps
- or, more generally, N accesses at 64 Kbps + P accesses at 128 Kbps (with N + 2P < or = 16)

Note:

An RAS client can directly establish a connection at 128 Kbps.

9.14.2.2 Callback

Alcatel-Lucent OmniPCX Office Communication Server offers two types of recalls:

- Call-back of the requesting party's number where he/she is.
- Call-back of a predefined number wherever it is (it is the secured form of the call-back).

RAS Alcatel-Lucent OmniPCX Office Communication Server uses the CBCP (Call-back Control Protocol) protocol to negotiate the call-back's use.

Note:

When the call-back is used, the connection's bandwidth cannot exceed 64 Kbps.

9.14.2.3 Quality of IP Service (QoS)

Alcatel-Lucent OmniPCX Office Communication Server offers the following QoS mechanisms:

- DiffServ (Differentiated Services) : QoS at the IP level
- Multi-Class Extension to MPPP: QoS at the PPP level (RFC 2686)

Note:

To be fully effective, QoS should also be applied on the RAS client's side.

9.14.2.4 Data compression

Alcatel-Lucent OmniPCX Office Communication Server offers the following compression algorithms:

- PPP header
- Van Jacobson

- STAC/MS-STAC and BSDCOMP

The compression rules are negotiated between the RAS client and the server during the LCP (Link Control Protocol) phase.

9.14.2.5 RAS service availability

The remote access availability can be defined globally or for each connection:

- By time range: access to the RAS server can be limited to certain times of the day and/or to some days of the week.
- Inactivity timeout: period during which an RAS client can be connected without any data being transferred.

9.14.2.6 Security

Since RAS is designed to seamlessly connect a remote client to a network, the security of these connections is important. The following security mechanisms are available:

- User authentication: The CHAP (Challenge Handshake Authentication Protocol) and PAP (Password Authentication Protocol) protocols are supported.
- Log: this log enables the administrator to detect connection issues easily. The following information is available:
  - User name, connection time, calling number, date, connection type (direct/call-back), bandwidth used (64 or 128 Kbps).
  - Authentication failure, date, calling number.
  - Failure during LCP phase (IP addresses have run out, unauthorised bandwidth).

9.14.2.7 IP services

When the RAS client has successfully completed the authentication phase, it is assigned an IP address by the server. This assignment is made individually in static mode (user always obtains the same IP address) or in dynamic mode (user obtains an address from an address pool).

Note:

The RAS clients" IP addresses are on the same sub-network as the RAS LAN.

After this address has been assigned, the client can use the IP services (FTP, HTTP, POP3, etc.). If the DNS and WINS services are used, it is important to ensure that the server is configured with the IP addresses of the appropriate DNS and WINS servers.

9.14.3 Setting the Server

9.14.3.1 Detailed description

9.14.3.1.1 REQUIRED EQUIPMENT ON SYSTEM

Hardware

A CoCPU-1 or CoCPU-2 board and the RAS software key are required for the RAS function to be available with a maximum of 16 accesses. A system can only have one RAS CoCPU-1/CoCPU-2 board.

The number of available remote accesses should be a multiple of 2.

The system should have at least the same number of ISDN accesses as RAS connections.

Software

The system should have the Internet Access software installed (RAS is included in the software).

The corporate LAN should use the IP protocol.

9.14.3.1.2 REQUIRED EQUIPMENT ON CLIENT PC

Hardware

The PC should be equipped with an ISDN adapter, typically a basic access with 2 64-Kbps B-channels

Software

The remote client PC should be equipped with the following software:

- Microsoft Windows NT 4.0 SP with patch 5997
- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows ME
- Microsoft Windows 2000 SP1
- Microsoft Windows XP

9.14.3.1.3 SYSTEM CONFIGURATION by OMC

RAS accesses are considered as virtual S0 interfaces, when it comes to telephones. These interfaces follow the distribution procedures of the system's calls (discrimination, traffic sharing, etc.).

Direct access

- By default, all RAS accesses belong to a sequential grouping. Assign a DID number to that grouping so that it can be called from the outside:

Numbering plan -> Public Numbering Plan

Callback

- Allow Main trunk group seizure (outgoing and incoming) for all RAS interfaces; assign the correct CL2 link categories:

• for the users: **Subscribers/Base stations List -> Subscribers/Base stations List -> Details -> Barring** • for the trunk groups: **External Lines -> Trunk Groups -> Details -> Link Cat.** • for access: **External Lines -> Access -> Details -> Link Cat.**

Time Ranges

- RAS activation is performed in normal or restricted mode (defined by time ranges). In restricted mode, the RAS grouping should be inaccessible; for example, do not allow data calls.

Time Ranges

9.14.3.1.4 INTERNET ACCESS CONFIGURATION BY WBM

Global Parameters

- Authorized on-demand bandwidth for all users
- Authorized callback for all users
- IP address range
- Disconnection timeout in case of inactivity

User-specific parameters

- On-demand bandwidth
- Authentication mode (use of PAP in case of CHAP failure)
- Recall mode: predefined number (static mode), requesting party (dynamic mode) or forbidden recall
- Recall number in static mode
- Fixed IP Addresses

Chapter 10

OmniTouch Call Centre Office

10.1 General Presentation

10.1.1 Overview

Alcatel OmniTouch Call Center Office is a call centre application of Alcatel-Lucent OmniPCX Office Communication Server and is used to distribute calls automatically to the most appropriate agent, while also managing call queuing.

Alcatel OmniTouch Call Center Office is made up of the following modules:

- Automatic Call Distribution (ACD) for the distribution of calls. The ACD is used to manage a large number of calls using a small number of agents through control of flows, proportionate distribution of calls between agents, and call queuing. The caller is immediately connected to an agent or to the most appropriate service, the agents being identified by skills group.
- An Agent Assistant application to optimize management of agents, their activity and organization into skills groups.
- An Agent Configuration application to parameterize some features and give specific rights to the agents.
- A Supervisor Console application.
- A Statistic Manager application to allow analysis of calls managed by the ACD.

The ACD is used to:

- improve call distribution and processing,
- process a larger number of calls,
- improve the output and efficiency of human resources,
- supervise service quality,
- anticipate incoming calls using the statistics module,
- minimize operating costs.

Remark:

In this document, the term ACD, Automatic Call Distribution, is synonymous with call centre.

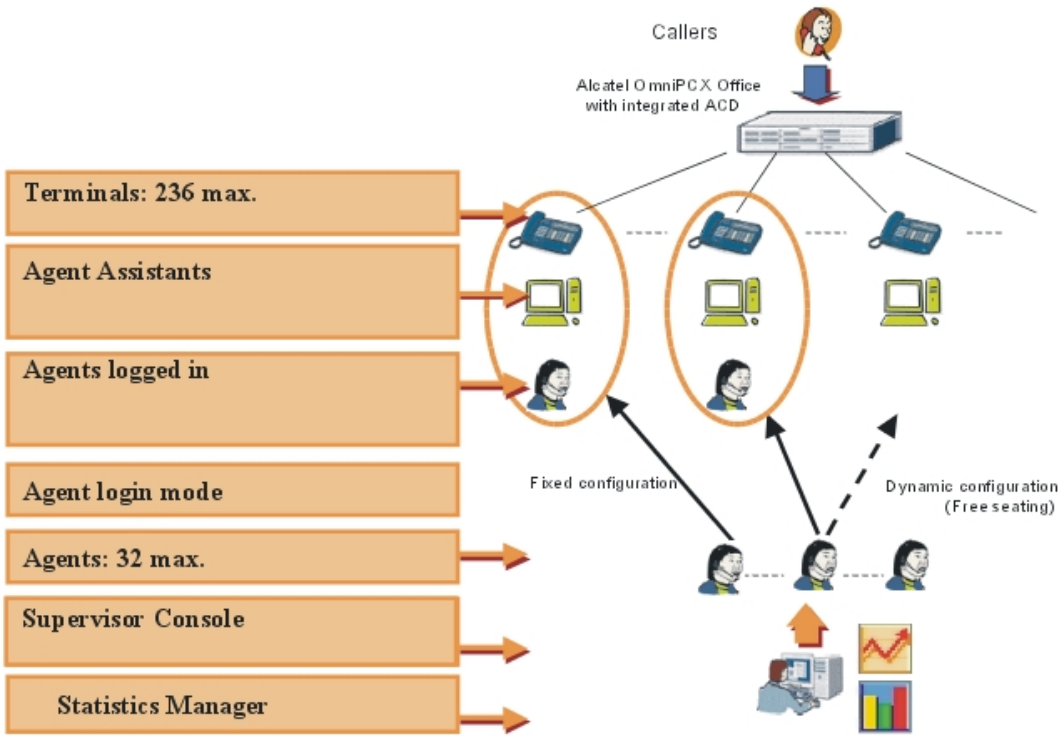
10.1.1.1 Licences

The Alcatel OmniTouch Call Center Office offer is available in four versions: Alcatel-Lucent Contact Easy Office, Alcatel-Lucent Welcome Office, and Alcatel-Lucent Welcome Office Pro. The fourth licence extends the Alcatel-Lucent Welcome Office Pro licence to allow up to 32 active agents. The associated rights of these licence versions are summarised by hardware configuration in the following table:

		Contact Easy Office	Welcome Office	Welcome Office Pro	Welcome Office Pro up to 32 agents
Alcatel-Lucent OmniPCX Office Premium Edition CS	Max agents logged in	5	10	20	32
	Supervisor console	N/A	option (max 4)	option (max 4)	option (max 4)
	Agent Assistant	N/A	option (max 10)	option (max 20)	option (max 32)
	Statistic Manager	N/A	option (max 1)	1	1
Alcatel-Lucent OmniPCX Office Advanced Edition CS with hard drive	Max agents logged in	5	10	20	32
	Supervisor console	N/A	option (max 1)	option (max 1)	option (max 1)
	Agent Assistant	N/A	option (max 10)	option (max 10)	option (max 10)
	Statistic Manager	N/A	option (max 1)	1	1
Alcatel-Lucent OmniPCX Office Advanced Edition CS without hard drive	Max agents logged in	5	10	N/A	N/A
	Supervisor console	N/A	option (max 1)	N/A	N/A
	Agent Assistant	N/A	option (max 10)	N/A	N/A
	Statistic Manager	N/A	N/A	N/A	N/A
Alcatel-Lucent OmniPCX Office Compact Edition with hard drive	Max agents logged in	5	10	20	32
	Supervisor console	N/A	option (max 1)	option (max 1)	option (max 1)
	Agent Assistant	N/A	option (max 10)	option (max 10)	option (max 10)
	Statistic Manager	N/A	option (max 1)	1	1
Alcatel-Lucent OmniPCX Office Compact Edition without hard drive	Max agents logged in	5	10	N/A	N/A
	Supervisor console	N/A	option (max 1)	N/A	N/A
	Agent Assistant	N/A	option (max 10)	N/A	N/A
	Statistic Manager	N/A	N/A	N/A	N/A

10.1.1.2 Terminology and Capacities

This section describes further the capacities of the ACD, as shown in the following diagram:



Terminal Types: The following terminal types are available: Alcatel-Lucent 8 series, Alcatel-Lucent 9 series, Reflexes, analog, DECT Reflexes.

Maximum number of agents: The maximum number of agents is 32 regardless of the hardware platform (Alcatel-Lucent OmniPCX Office Advanced Edition CS or Alcatel-Lucent OmniPCX Office Premium Edition CS) or package (Contact Easy Office, Welcome Office, or Welcome Office Pro) used. An agent can use any terminal of the system.

Maximum number of agents logged in: An agent must be logged in to a terminal on the system in order to use the call centre services. The maximum number of logged in agents is 5, 10, 20, or 32 depending on the licence package selected.

Login mode: Agents can be logged in to a terminal on the system in two different ways:

- **fixed mode**: By configuration. In this case, the agent is permanently logged in to the same terminal.
- **dynamic mode**: The agent logs in to a free terminal of his/her choice using either the Agent Assistant (free seating operation) or the terminal login function. The agent logs out and frees up the terminal either by leaving the agent application or using the terminal logout function.

Agent Assistant Licences: A licence is required for each active connection of the Agent Assistant. The number of licences necessary corresponds to the maximum number of simultaneous connections required. The maximum number of licences possible depends on the licence package (Welcome Office or Welcome Office Pro) and the hardware platform (Alcatel-Lucent OmniPCX Office Advanced Edition CS or Alcatel-Lucent OmniPCX Office Premium Edition CS) selected.

Supervisor Console Licences: A licence is required for each active connection of the Supervisor Console. The number of licences necessary corresponds to the maximum number of simultaneous connections required. The maximum number of licences possible depends on the hardware platform selected (Alcatel-Lucent OmniPCX Office Advanced Edition CS or Alcatel-Lucent OmniPCX Office Premium Edition CS).

Statistic Manager Licence: This licence is used to activate the Statistics application. It is included with the Welcome Office Pro packages and available as an optional extra with the Welcome Office package.

10.1.1.3 Additional Information

Auto-answer mode is applicable for ACD.

10.1.2 Services provided

This section describes the services provided by the ACD and associated applications.

10.1.2.1 ACD Services

The table below summarizes the ACD general services.

Services	Description
Type	Informal and integrated
Queue	Management of incoming calls with dynamic sizing based on predefined parameters.
Distribution mode	Distribution of calls via 3 possible configuration modes (longest idle time, fixed, rotating).
ACD groups	Possibility of defining the parameters of 8 independent ACD groups.
Opening criteria	Automatic open/closed parameters for each ACD group. Up to 100 entries for exceptional closing opening days can be defined and applied to selected or all groups. Groups can be opened/closed by: - forcing via the configuration, - time slot, - forcing via the Supervisor Console application.
ACD announcements	Broadcasting of 6 ACD announcements (welcome, 3queue announcements, deterrence and closure).
Priority ranking	Managing the priority of agents in relation to the groups which the agent is assigned to.
Dynamic queue	Depends on agent availability.
Leave queue	Through reception of DTMF code.
Agents belonging to several groups	An agent can belong to several ACD groups.
Overflow	1 group can overflow to another group (no cascading permitted).
Management	Configuration of the ACD.

Services	Description
Group mailbox	The group mailbox can be used if the caller is deterred, leaves the queue or if the group is closed.

10.1.2.2 Agent Assistant Services

The Agent Assistant allows agents to associate their telephone set with their PC.

Agents can indicate their status (on duty, off duty, temporary absence, clerical work) in a more user-friendly environment. They can also access the following functions: observation of real-time statistics, noting of call types, multi-skills management, free seating and customer information screen pop-ups.

The table below describes the agent services.

Services	Description
ACD statuses Service code	Management of the 4 agent statuses (on duty, clerical work, temporary absence, off duty) by service code.
ACD statuses UPK keys	Management of the 4 agent statuses using the programmable keys on Reflexes sets.
ACD statuses Agent Assistant	Management of ACD statuses by the Agent Assistant.
ACD Login/Logout Service code	Agent Login/Logout on a terminal by service code.
ACD Login/Logout UPK keys	Agent Login/Logout on a terminal using a programmable key on Reflexes sets.
ACD tab of the Alcatel-Lucent 8 series and Alcatel-Lucent 9 series sets	Management of agent login/logout, statuses, groups, and passwords on an ACD dedicated tab.
ACD group	Possibility of joining/leaving an ACD group on a PC via the Agent Assistant interface. Also available in the ACD dedicated tab of the Alcatel-Lucent 8 series and Alcatel-Lucent 9 series sets.
Call supervision	Real-time supervision of the ACD call (caller number, number called, heading of the ACD group, call queuing time and timer)
Agent supervision	Real-time statistics (activity rate, call counter, call types, queues of the groups which the agent is assigned to)
Free seating	Allows several agents to share one telephone terminal over time. Free seating operation allows an agent to use any workstation with the Agent Assistant installed.
Information screen pop-up	Screen pop-up on an ACD call via several modes (integrated, Outlook script, Goldmine, specific mode, etc.) while the call is being presented.

10.1.2.3 Statistic Manager Services

The Statistic Manager is used to display statistics on the operation of the call center. The table below summarizes the Statistic Manager services.

Services	Description
Groups	Daily, monthly and periodical consolidated statistics of ACD groups.
Agents	Daily, monthly and periodical consolidated statistics of ACD agents.
Line statistics	Used to check how busy and overloaded the lines are.
Call statistics	Used to quantify the number of calls per line and the lost calls.
Lost call reading	Statistics on the type and number of lost calls due to port saturation on the ACD.
Configuration	Used to configure certain parameters.
Export	Used to export statistics to the binary or .CSV format.

10.1.2.4 Supervisor Console Services

The Supervisor Console gives the supervisor real-time access to call center activity. The information can be displayed in the form of a table on his/her PC.

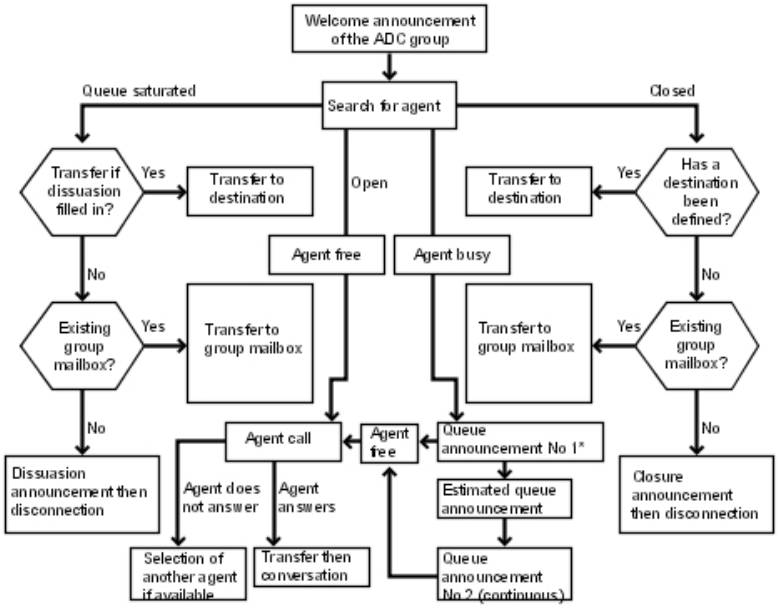
Services	Description
ACD groups	Real-time global supervision of ACD groups
ACD agents	Real-time global supervision of ACD agents
ACD calls	Real-time global supervision of ACD calls (calls answered, being routed, in queue, deterred, closed etc.)
Forcing of group statuses	Assignment of agents to groups
Forcing of agent statuses	Forcing an agent to change his status

10.1.3 Architecture

10.1.3.1 General Description of Call Flows

The figure below shows how calls are processed.

Figure 1: Call flows



*Callers can leave the queue by pressing *, to the group mailbox or to a transfer number.

10.1.3.2 Call Distribution

The ACD receives all incoming calls and plays a greeting message. It manages the distribution of the calls according to the status of the group (open or closed), the status of the agents that belong to the group, and the order in which the call is received (first in, first out).

If the group is open and an agent is available, the call is routed to this agent. If the agent is busy, the ACD will look for another available agent according to the call distribution rules (fixed, rotating, longest idle period).

If there are no available agents in the group, the ACD plays a message asking the caller to hold the line and places the call in the queue. As soon as an agent becomes available, the call is transferred to the available agent without waiting for the end of the hold message.

If there are no available agents and the queue is full (all ACD ports are busy), an incoming call is routed to a deterrence message, inviting the caller to call back later (default option). It is possible to configure the ACD to place the call in the group mailbox, or to transfer it to a specified number.

The maximum number of waiting calls is 12 (two of the 14 ACD ports are used for deterrence).

If the ACD group is open and no agents are active (logged in and not in the sleeping status), the first call to this group will be routed to the transfer number if entered. Subsequent calls will then be placed directly in the queue. If the transfer number is not entered, the calls are routed to the deterrence message.

If the group is closed, the call is routed to a closed message (default option).

It is possible to configure the ACD so that a caller waiting in a queue can press the star key to escape from the queue. The call can be routed to the group voice mail box, or transferred to a specified number.

All events are monitored by CSTA protocol, so you can use the agent and ACD group statistics

to optimize the ACD functions.

10.1.3.3 Recommendations

Certain rules should be observed in order to guarantee that the system is as user-friendly as possible:

- Take the caller into account when thinking of an ACD group.
- When setting up the ACD group mail boxes, ask the people receiving the calls (operators, sales departments, technicians, etc.) what the main requests from callers are.
- Do not forget to define what happens outside working hours and during the weekends.
- Do not forget to define what happens when an internal telephone is not answered.
- Start by drawing the total structure on a piece of paper based on the fixed tree of the ACD and the relations between the automated attendant, mailboxes and info-text if necessary.
- At each stage, think carefully about the content of the voice message concerned.

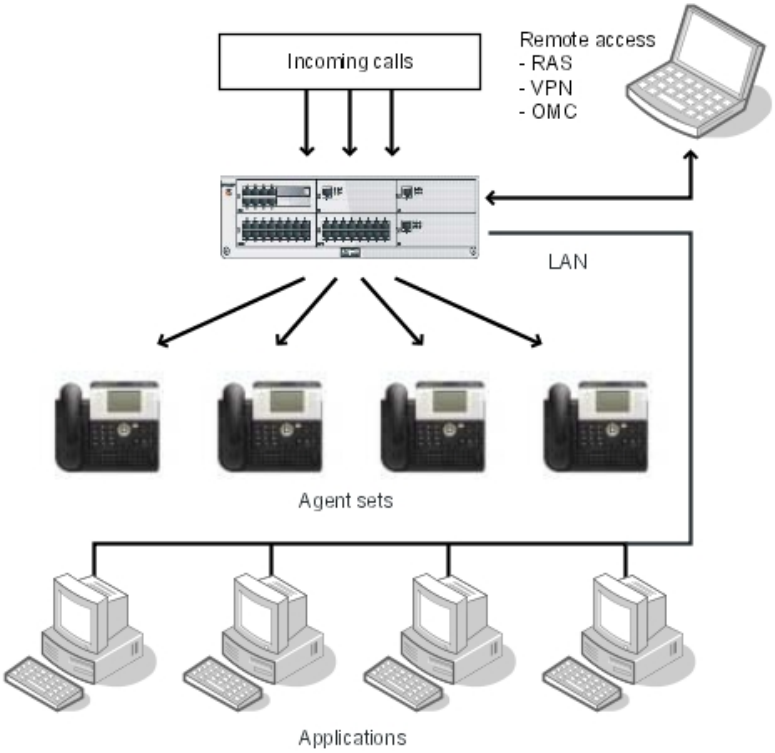
10.1.3.4 Hardware Configurations

Alcatel OmniTouch Call Center Office can operate in a stand-alone configuration or in a network configuration.

10.1.3.4.1 Network configuration

The drawing below shows a configuration example using a local area network to connect Alcatel OmniTouch Call Center Office.

Figure 2: Network installation

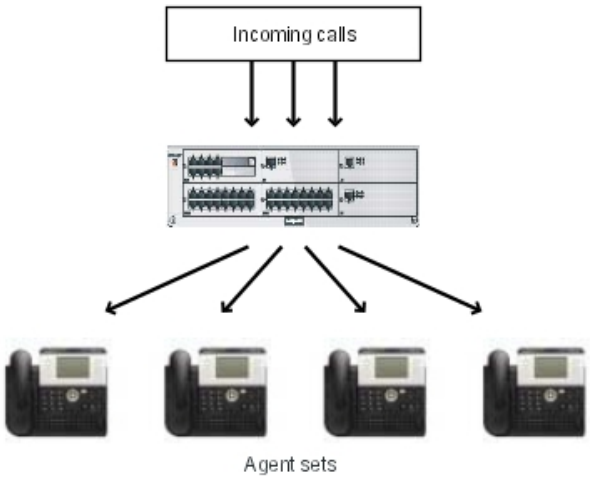


This configuration uses a local area network to connect Alcatel-Lucent OmniPCX Office Communication Server. It manages the call center from client PCs connected to the local area network by using the applications **Agent Assistant**, **Agent Configuration**, **Supervisor Console**, **Statistic Manager**, and **PIMphony** .

10.1.3.4.2 Stand-alone configuration

The drawing below shows a configuration example when Alcatel-Lucent OmniPCX Office Communication Server is stand-alone and not connected to the local network, and therefore has no associated applications.

Figure 3: Local installation



10.2 Installation and Startup

10.2.1 Overview

10.2.1.1 Overview of the Configuration Procedure

Alcatel OmniTouch Call Center Office is supplied pre-installed. Only the necessary licenses have to be loaded in the PCX.

The applications **Supervisor Console**, **Statistic Manager**, **Agent Assistant**, and **Agent Configuration** can be installed on any PC.

The Alcatel OmniTouch Call Center Office (ACD) is configured using OMC. In an OMC session, use the path **OMC/PCX Client/Automatic Call Distribution**, to access the following four menus:

- **ACD Setup**: used to configure the parameters of the ACD in the PCX.
- **ACD Services**: used to configure the ACD groups, agents, and lines.
- **ACD Voice messages**: used to configure the ACD announcements.
- **ACD Statistic manager**: accessible only if installed.

Configuring the ACD involves the these operations:

Caution 1:
Check the Alcatel-Lucent OmniPCX Office Communication Server settings described in the Pre-requisites section before running ACD Setup.

1. Configuring the ACD parameters in the PCX using ACD Setup:
   - Checking prefixes in the main numbering plan for login and logout.
   - Creating ACD Group mailboxes.
   - Generating ACD profiles.
   - Assigning profiles to agent and supervisor phone sets.

2. Configuring ACD Services:

   Caution 2:
   Run ACD Setup before configuring ACD services.

   - Configuring general parameters: Defining ACD group parameters, call types, and ACD maintenance parameters.
   - Configuring agents.
   - Configuring the lines table.

3. Creating the announcements using ACD Voice Messages.

10.2.1.2 Hardware and Software Requirements

10.2.1.2.1 Platforms supported by ACD applications

The following platforms are supported for the Agent Assistant, Supervisor Console, and Statistics Manager applications:

- Windows XP (Service Pack 1 and Service Pack 2)
- Windows 2000 (Service Pack 4)

10.2.1.2.2 Hardware required on the PCX

The hardware required on Alcatel-Lucent OmniPCX Office Communication Server is:

- CPU-1, CPUe, CPUe-1, CPUe-2 with a 20 Gb hard disk
- CPU-3 with or without a 20 Gb hard disk

Note:
The RAS and ACD functions cannot be installed on the CPUe board simultaneously. The CPUe-1 board is required. The ACD function is not available on the CPU boards.

The ACD function can be offered on a platform without hard disk. Consequently, some functions will not be available:

- No **Statistic Manager** application (even if the license is present),
- Limitation on the number and the recording time for ACD messages,
- Size parameters for voice messages:

	ACD messages number	**Recording time**
With hard disk	6 messages/group	All messages: 60 seconds except waiting (5 min.)
Without hard disk	6 messages for all the groups	5 minutes for all the messages

10.2.1.2.3 Requirements for client workstation running OMC

OMC runs on the following platforms:

- Windows 2000 (with Service Pack 4)
- Windows 2003 (with Service Pack 1)
- Windows XP (with Service Pack 1 or 2)

The following platforms are no longer supported for OMC:

- Windows 9x
- Windows ME
- Windows 2003 without Service Pack 1

The following items are also required on the workstation:

- The licenses necessary for the ACD
- Internet Explorer (release 6 or later) or Netscape Navigator (release 7 or later)

10.2.1.3 Prerequisites to Running ACD Setup

To ensure that the ACD setup works properly, check the following settings in Alcatel-Lucent OmniPCX Office Communication Server before running ACD Setup.

- Check that you have the correct ACD licenses.
- Check that the **Group Call Mode with Signaling Mode** box is unchecked in **OMC/PCX Client/System Miscellaneous/Feature Design/Part 2**.
- Check that there are enough directory numbers remaining for the 14 ACD ports in the main numbering plan.
- Check that the parameters of the internal numbering plan in **OMC/PCX Client/Numbering/Dialing Plans/Internal Dialing Plan** are configured in accordance with the following rules:
  - For local calls: local call function / start / end / base.

    Note 1:
    The base is always equal to the start of the numbering range

    Example 1:

Function	Start	End	Base	
Local call	3000	3199	3000	OK
Local call	3000	3199	1000	Forbidden

  - For group calls: group call function

    Example 2:

Function	Start	End	Base	
Group call	600	619	600	OK
Group call	600	619	500	Forbidden

- Check that the directory numbers are allocated to the Hunting Groups in **OMC/PCX Client/Hunting Groups.** The hunting group directory numbers may be available in the main numbering plan, but not assigned in the hunting group list. In this case, ACD Setup may not find the hunting groups available. To avoid this situation, assign enough directory numbers in the hunting group list.
- Check and/or modify the login and logout prefixes in the main numbering plan.

  Example 3:

Function	Start	End	Base	
ACD prefix	680	681	0	OK

Note 2:
680 gets the function "Request of ACD log out".
681 gets the function "Request of ACD log in".

10.2.1.4 Restrictions

The use of the "Call Pick-up" feature on ACD calls is forbidden. When using Call Pick-up on an ACD call to an agent (the agent extension is ringing), ACD does not understand this action and transfers the call to an agent extension supervised via CSTA: it is then an unknown extension which answers the call. ACD is not informed and the call may be lost and rerouted, and the statistics will be incorrect.

If the ACD agent profiles are used and loaded to the agents, the "Call Pick-up" feature is automatically disabled in the "feature design" of the agent extension.

The use of the "Call Forwarding" feature for an ACD agent is authorized only for external calls.

10.2.2 ACD Setup

10.2.2.1 First Initialisation of the ACD

Running ACD Setup:

- creates 14 media virtual terminals.
- creates hunting groups with 14 ACD ports.
- creates virtual terminals for the voice mail boxes of the 8 ACD groups (optional).
- creates ACD key profiles and their links to the various agent and supervisor stations.
- allocates the key profile according to the profile's definition: 1 login/logout key; 4 agent status management keys and 1 supervision key per ACD group voice mail box.
- modifies the services category for the agent sets. Call interception is deleted.
- modifies the dynamic routing for the agent sets. External call forwarding is permitted. Internal call forwarding is possible if the queue wait threshold S1 is longer than the maximum ringing duration (defined in **OMC/ACD Services/General Parameters/General** tab).

Remark:
Many parameters are modified during the allocation of profiles to the agent stations:

To initialise the ACD, run ACD Setup (as described below) and on the **General** tab, enter the direct dialling-in (DDI) number associated with each hunt group.

Caution 1:
You must not change directory numbers, virtual terminals used for ACD ports, group mail boxes and hunting groups for ACD after running the ACD Setup. This will result in incorrect operation and the ACD ports will lock up.

ACD Setup will perform a consistency check of the main parameters. If Setup detects an inconsistency, it will display a warning message indicating in brackets the origin of the problem.

Caution 2:
The ACD directory is not automatically updated during the modification of the system's directory or during the creation of a phone set. It is necessary to reset the ACD (or reset OmniPCX Office) to have an identical image of the directory of OmniPCX Office in the ACD part for the creation or modification of the list of agents.

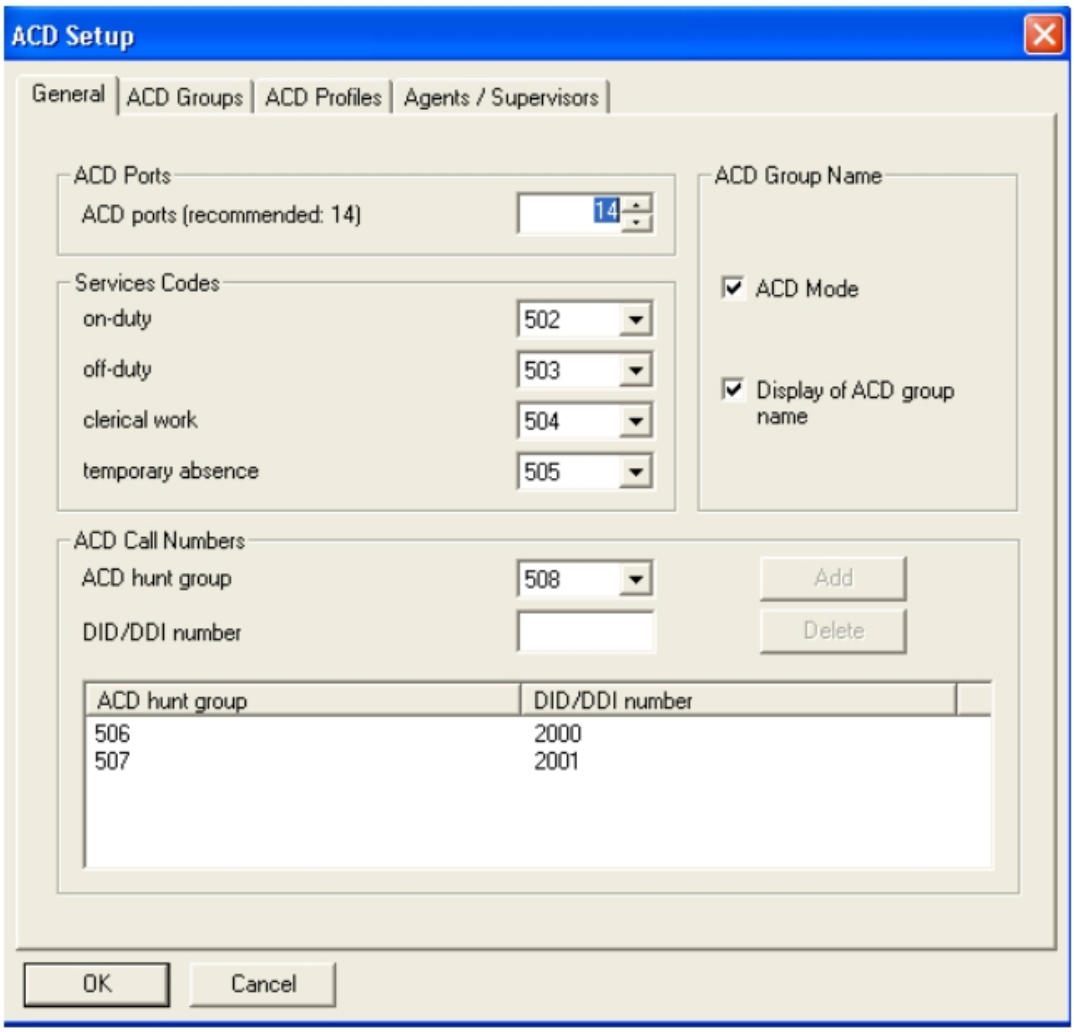
To run ACD Setup, select the path **OMC/Automatic Call Distribution/ACD Setup**. The **ACD Setup** window appears with four tabs:

- **General:** shows the number of media virtual terminals created by Alcatel-Lucent OmniPCX Office Communication Server when the call centre was installed (or ACD ports).

  Caution 3:
  the default value is 14. This figure must never be changed.

- **ACD group**: used to create and associate mailboxes with the ACD groups.
- **ACD profiles**: used to assign profiles to agent sets and supervisor sets.
- **Agents/Supervisors**: lists the numbers of agent and supervisor sets.

10.2.2.2 ACD Setup General Tab



The **General** tab consists of the following areas:

- **ACD Ports**: The **ACD Ports** drop-down box shows the number of virtual terminals required to start up the call centre.

  Caution 1:
  The recommended value of 14 must not be changed.

- **ACD Group Name**: This feature controls the display of information on the agent's set about incoming calls. When the **ACD Mode** box is checked, the **Display of ACD group name** box is available. When this box is checked, the ACD Group name and the customer waiting time will display on the agent's set for an incoming call.

  When the **ACD Mode** box is unchecked, the box label becomes **Multi-secretary mode** and the second box is greyed (inactive). In multi-secretary mode, the DDI number or the corresponding name of the incoming call is displayed on the agent's set. This mode is used when several DDI numbers are assigned to a unique ACD group.

- **Services Codes**: Four drop-down boxes show the prefixes used to change the status of

agents. These prefixes are programmed in the numbering plan of the Alcatel-Lucent OmniPCX Office Communication Server and correspond to the groups containing the ACD ports. The statuses are:

- **on duty**: The agent is assigned to an ACD group.
- **off duty**: The agent has withdrawn from all groups.
- **clerical work**: The agent temporarily withdraws from the call distribution chain to perform an operation following a call, for example filling out an information screen. At the end of this clerical work period, agents must come back on duty so that they are available again to process a new ACD call. Clerical work periods are considered as work time for call distribution criteria.
- **temporary absence**: the agent withdraws temporarily from the call distribution chain for a break. At the end of this break, agents must come back on duty so that they are available again to process a new call. Periods of temporary absence are not considered as work/service time.

- **ACD Call Numbers** shows the group number available for the call centre and the associated DDI number. If the DDI number is entered, it will be automatically created in a line of the Public Numbering Plan of Alcatel-Lucent OmniPCX Office Communication Server. For each DDI number created, a new group (containing the 14 ACD ports) will be automatically generated.

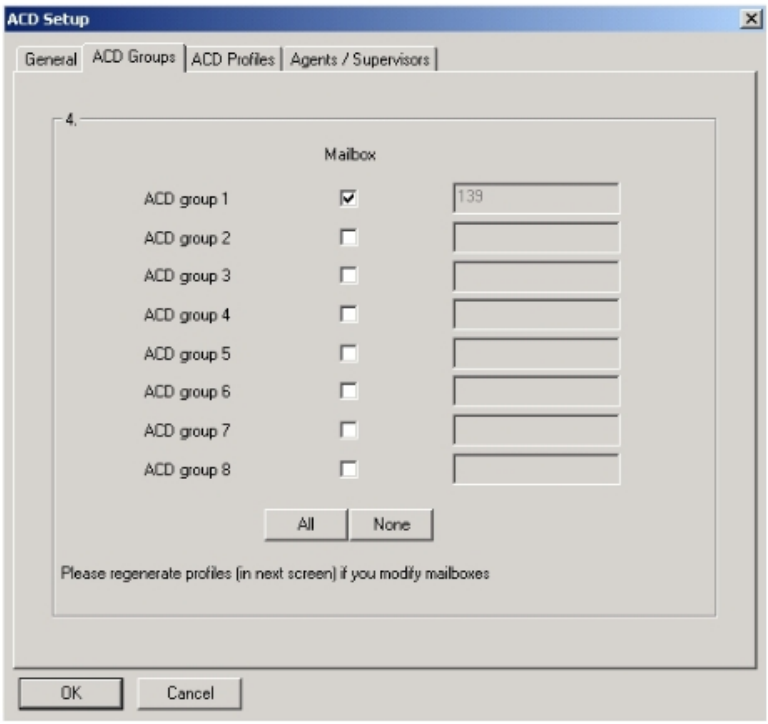
  Caution 2:
  The group number and DDI number must be manually entered in the line parameter table in ACD Services.

Click **OK** to save the data entered.

10.2.2.3 ACD Setup Groups Tab

Use the **ACD Groups** tab to create a mailbox for the ACD groups. The mailbox created can be used when an ACD group is in deterrence or closure mode, or when a caller leaves the queue.

1. Click the **ACD Groups** tab. The **ACD Groups** window is displayed:



2. Check the **Mailbox** box of the group that you want to select.
3. Click **All** to select all groups. All the boxes are automatically checked.
4. Click **None** to cancel the selection.
5. Click **OK** to confirm. The PCX creates mailboxes for the groups selected.

Remark 1:
the number of the associated mailbox is the same as the number of the virtual terminal.

Remark 2:
It is possible to customise the ACD groups voice mail boxes using the "Remote custo" mode. The password to access the mail box is "1515" by default.

It is also possible to manage the mail box of a virtual terminal on adedicated set, using the "Voice mail unit" feature key with the virtual terminal destination.

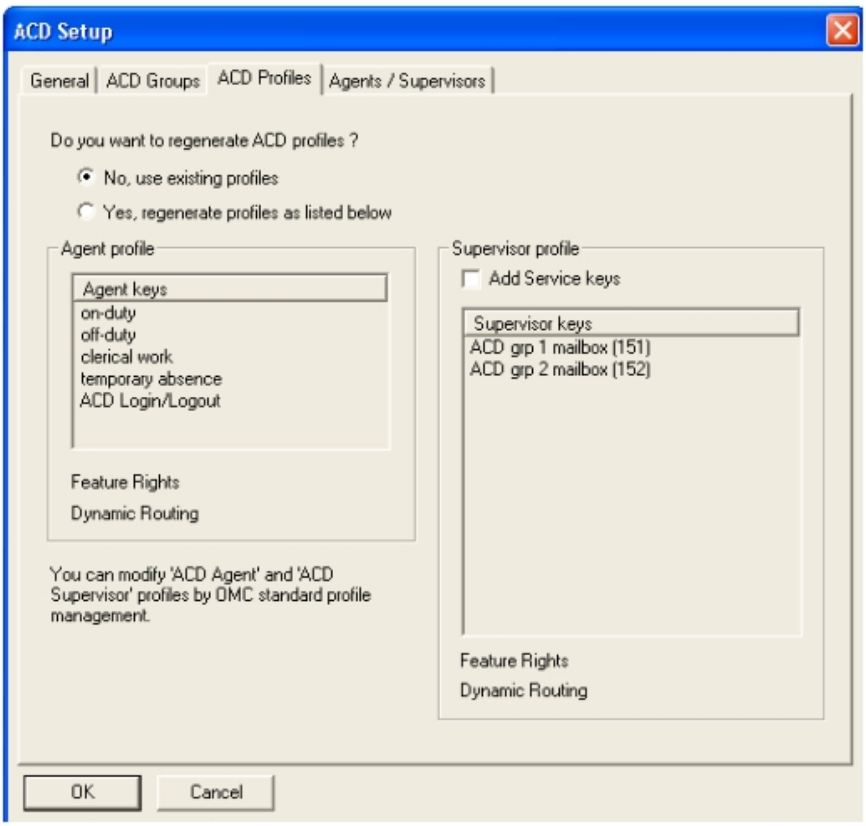
10.2.2.4 ACD Setup Profiles Tab

Alcatel OmniTouch Call Center Office allows you to manage two types of ACD key:

- Keys for the operating status of agents corresponding to the groups previously created.
- Supervision keys for the mailboxes of ACD groups.

Once the **General** tab has been confirmed, the ACD profiles must be generated if you want to use them.

1. Click the **ACD Profiles** tab. The **ACD Profiles** window appears:



2. To generate the profiles, select **Yes, regenerate Profiles as listed Below**.
3. Click **OK** to confirm the new profiles.

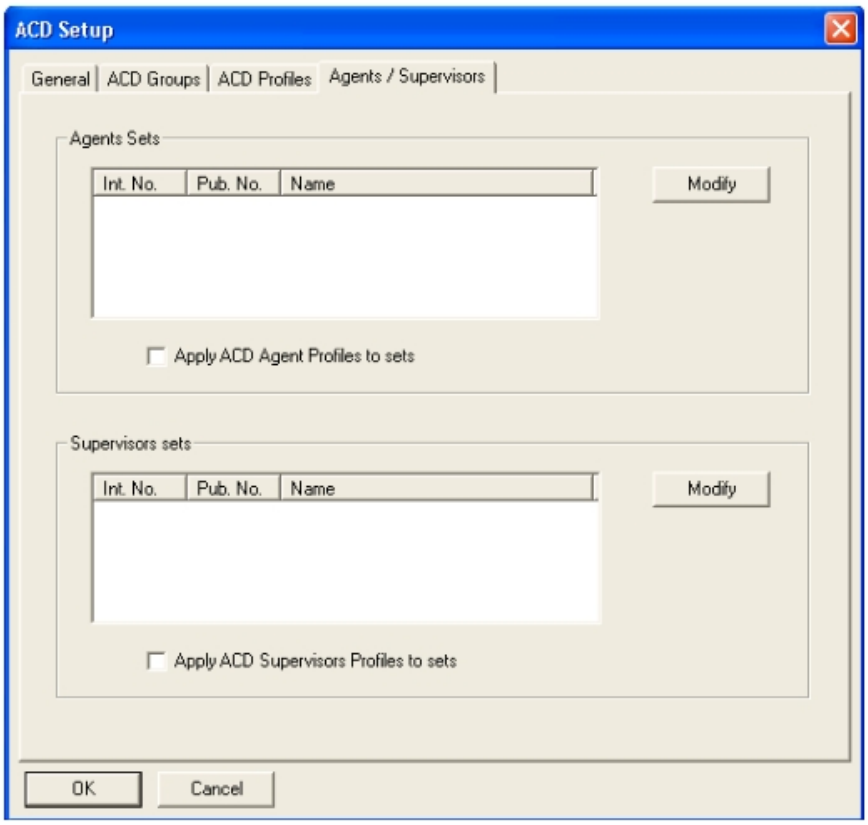
Remark:
*- The definition of the profiles obtained is predefined in the system. However, it is still possible to modify them through standard management of profiles by selecting the path **OMC / PCXClient / Users-Base station List / Profiles**.*

- These profiles have an influence on service categories and transfers, given that calls to an agent set must neither be transferred nor intercepted.

10.2.2.5 ACD Setup Agent/Supervisor Tab

10.2.2.5.1 Automatic assignment of keys

1. Click the **Agents/Supervisors** tab. The **Agents/Supervisors** window appears:



2. In the **Agent Sets** area, click **Modify**. The **Change List of ACD Agents** window is displayed. It can be used to select agent sets.
3. In the **Non-member(s)** area, select the objects to be added and click the **Add** button. The objects selected appear in the **Member(s)** area.
4. Click **OK**.
5. To automatically assign profiles to sets, check the **Apply ACD Profiles to Sets** box.
6. Click **OK**.
7. Follow the same procedure to assign supervisor profiles.

Important:

Assigning an ACD profile to a set has the effect of:

- adding the following keys: 2 RGX, 2 RSB, 4 CTI, 1 login/logout function key and/or 8 supervision keys for ACD group mail boxes.
- deleting internal dynamic transfers and inhibiting any type of internal transfer.

Remark:

ACD calls do not support any type of call transfer or interception.

10.2.2.5.2 Manual assignment of keys

To assign an agent key manually, do the following:

1. Select the path **OMC / PCXClient /Users-Base station List** and select the set whose keys you want to modify. Click **Details**, then **Keys**. A window displaying the keys of the set opens.
2. Click on the button of the key to be modified.
3. Select the **Function Key** type of key.
4. Click **OK** to confirm.

Agent keys correspond to the following function keys:

- CTI, Application 12, service 1 for "on duty" status,
- CTI, Application 12, service 2 for "off duty" status,
- CTI, Application 12, service 3 for "clerical work" status,
- CTI, Application 12, service 4 for "temporary absence" status,
- The login/logout key is an ACD key function

For the **Supervision** keys of mailboxes, simply create **Voicemail** function keys for the virtual terminal corresponding to the mailbox of the ACD group.

Remark:
the assignment of profiles to sets is not checked (no checking of whether the set is an agent set or not).

10.2.3 ACD troubleshooting

In some rare cases, ACD does not start correctly and the ACD does not answer ACD calls.

10.2.3.1 Troubleshooting

- Start an OMC session and check:
  - That the 14 virtual terminals for ACD ports are created and specified as media (in the subscribers list/details).
  - That the default ACD prompts are already loaded.
  - That the ACD line parameters are correctly programmed.
  - That you have the correct ACD licences.
  - That you have enough free directory numbers remaining for the ACD ports in the numbering plan and that the bases are correct.
  - That the hunting group directory numbers are available in the **hunting group** list.
  - That the **group called in signalling mode** feature is not selected in **System/miscellaneous/Feature design/Part 2**.
- Check that all the prerequisites to running ACD Setup have been met.
- Try to open a supervisor session and check the lines' status (ACD ports) when making an incoming call.
- Try to set up traces when restarting the system.

10.2.3.2 Restarting the ACD

1. Before starting, make sure there are enough free directory numbers for the ACD ports, ACD mail boxes and ACD hunting groups.

2. Select the path **OMC/Automatic Call Distribution/ACD Setup**.

The **ACD Setup - General Tab** will appear.

3. Set the ACD ports to 0.
4. Click **OK** to restart the system.
5. Click **Yes**.
6. Select the **Automatic Call Distribution/ACD Setup** menu again in OMC.
7. Set the ACD ports to 14.
8. Click **OK** to restart.
9. Click **Yes**.
10. Select the path **OMC/Automatic Call Distribution/ACD Services/ACD General parameters/Maintenance**.
11. Select **Stop the ACD function** and click **OK**. The system asks "Do you really want to stop the ACD function?".
12. Click **Yes**.
13. Restart the ACD function by selecting **Start the ACD function**. The system asks "Do you really want to start the ACD function?".
14. Select **Yes**. The system is now operational.

10.2.3.3 ACD default factory configuration

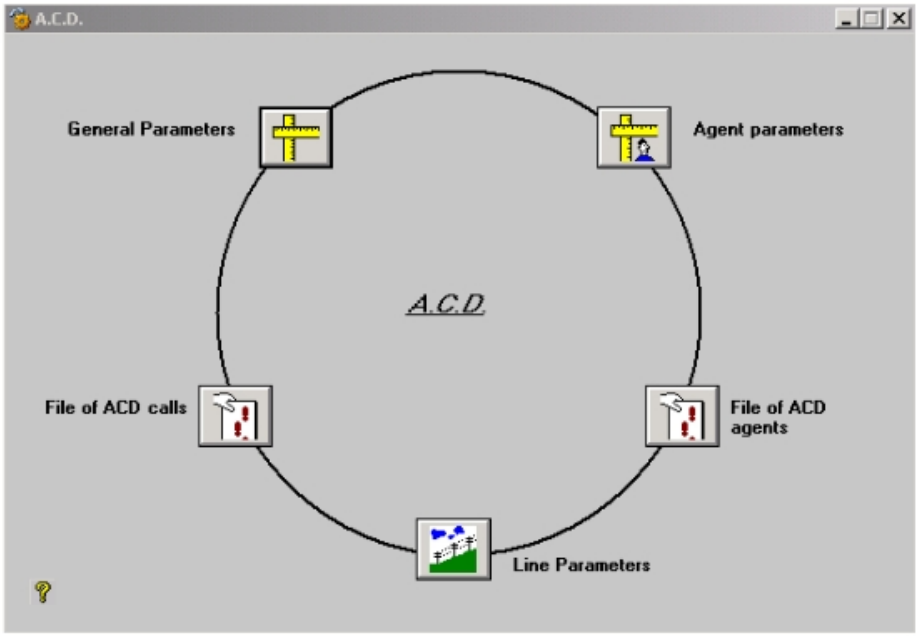
If it necessary to return the system to the default configuration, follow this procedure:

1. Perform a reset to clear the call server.
2. Select the path **OMC/Automatic Call Distribution/ACD Services/General parameters/Maintenance**.
3. Select **Reload the factory configuration** and click **OK**.
4. Reload the default ACD messages.

10.3 ACD Services

10.3.1 Overview

The detailed configuration of ACD can be set from the ACD services menu available in **OMC / PCX Client / Automatic Call Distribution / ACD Services**



Three sub-menus are available to access the configuration of the ACD services:

- **General Parameters** to configure the call center general parameters, group parameters, types of calls, and call center maintenance parameters.
- **Agent Parameters** to configure the agent parameters and assign agents to groups.
- **Line Parameters** to configure the lines table used to associate caller or called numbers with groups and agent status.

Two trace files are available used to obtain information on agent activity and calls.

10.3.2 General Parameters

10.3.2.1 Setup Parameters Overview

To set the parameters of the call centre services, select the path **OMC / Automatic Call Distribution / ACD Setup**. The **ACD Setup** window appears.

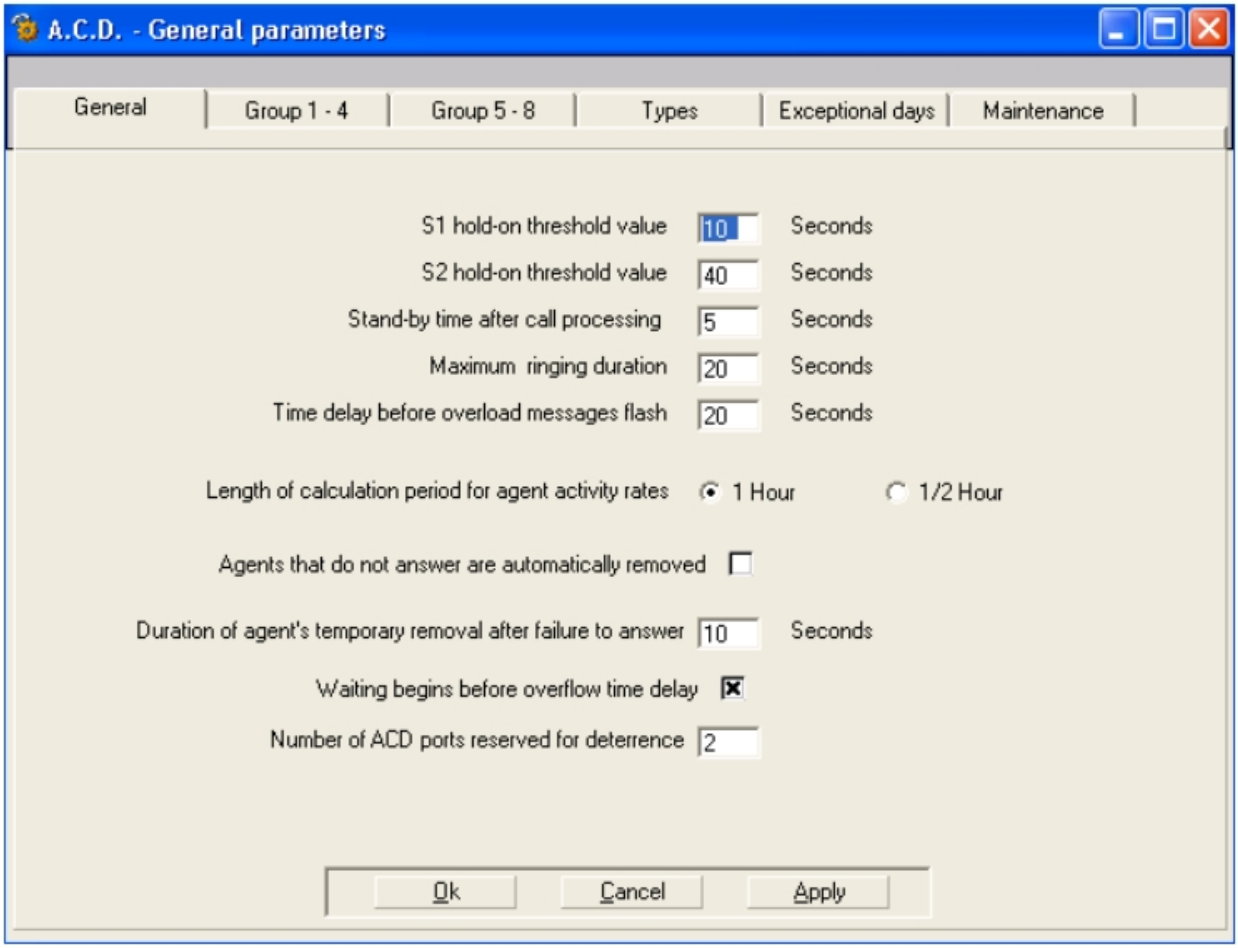
This is used to configure:

- Port number
- Service codes
- ACD Hunting groups
- Group Mailboxes
- ACD Profiles
- Agents sets
- Supervisor sets

10.3.2.2 General Parameters Overview

To set the parameters of the call centre services, select the path **OMC / Automatic Call Distribution / ACD Services**. The **ACD Services** window appears.

1. Click the **General Parameters** icon. The **A.C.D. - General Parameters** window appears:



The **General Parameters** window has six tabs:

- **General**: Use to configure parameters general to the call centre.
- **Groups 1 - 4**: Use to define parameters for groups 1 to 4.
- **Groups 5 - 8**: Use to define parameters for groups 5 to 8.
- **Types**: Use to define the type of call an agent receives.
- **Exceptional days**: Use to define up to 100 exceptional days, which can be applied to selected or all groups.
- **Maintenance**: Use to stop, start, and restore the ACD, and to perform log and statistics file maintenance.

10.3.2.3 General Tab

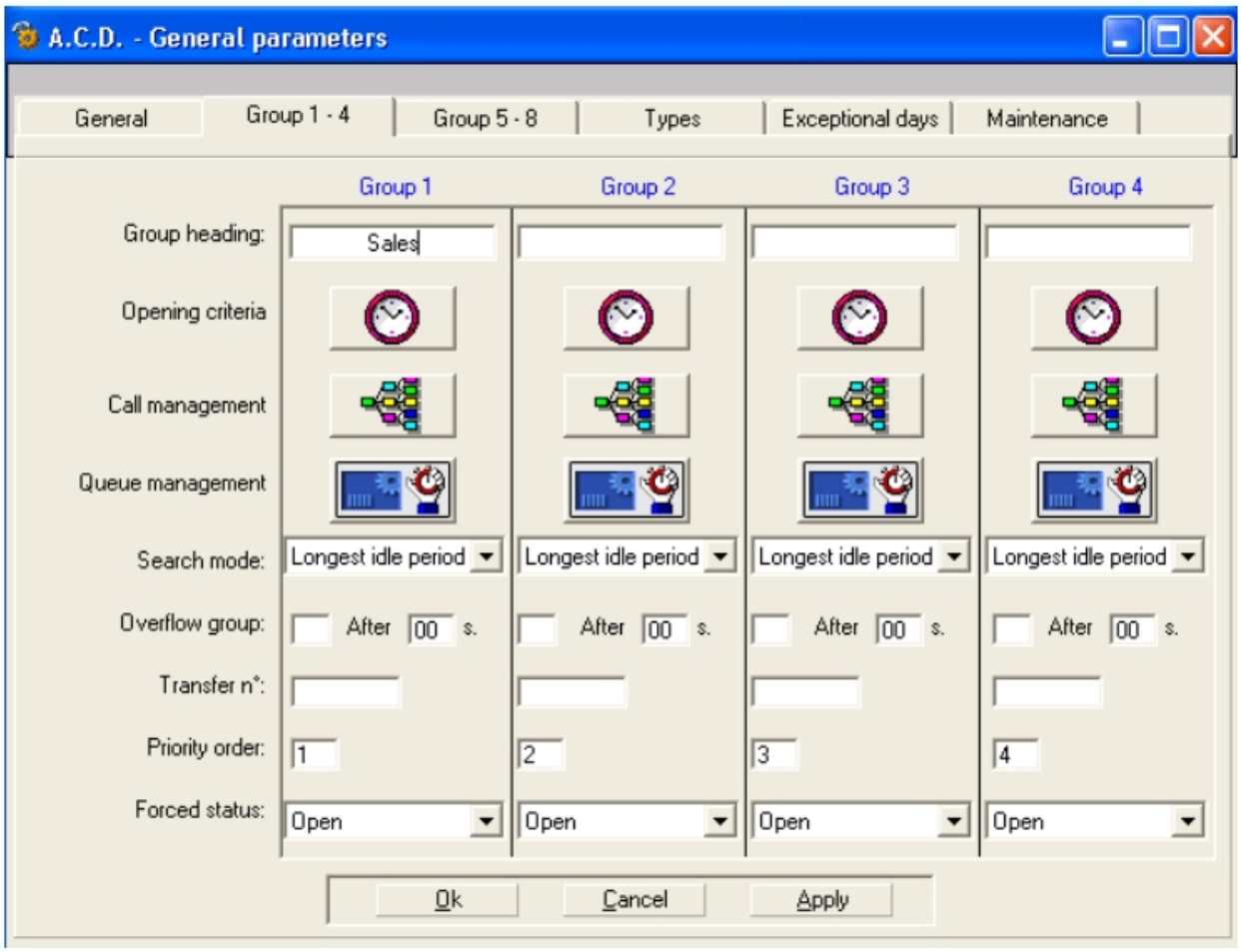
Use the **General** tab to configure the call centre general parameters. These parameters are common to the 8 groups.

1. Click the **General** tab.
2. Enter the **Value of queue threshold S1 and S2** to define service quality criteria. The Supervisor Consol application uses these values to indicate, in real-time, the number of calls in the groups waiting for a period of time longer than S1 and S2. These values are also used in the publication of statistics.
3. Enter the **Stand-by time after call processing**, the minimum time between two consecutive calls for the same agent.
4. Enter the **Maximum ringing duration**. If an agent does not answer within the number of seconds entered, the call is routed to another agent or returned to the queue. The ACD also uses this time delay when transferring a call to an internal or external called party or to a mailbox. If the called party does not answer within this time delay, the call is automatically returned to the queue.
5. Enter the **Time delay before overload messages flash** , the number of seconds before which the ACD will change the colour of the group overload messages displayed on the Supervisor Console.
6. Enter the **Length of calculation period for agent activity rates**. You can choose to have the activity rates print every hour or every half hour within the Supervisor Console.
7. Check the **Agents that do not answer are automatically removed** box to cause an agent not answering to be removed from the ACD group either for 10 seconds (see the following parameter), or permanently. In the latter case, he/she must be put back "on duty".
8. Enter the **Duration of an agent's temporary removal after failure to answer**, the period of time for which an agent who fails to answer is removed from the ACD group.
9. Check **Waiting begins before overflow time delay** to start the statistics counter related to customer waiting times as soon as the call centre answers. Otherwise, the counter starts after the overflow time delay of the call.
10. Enter the **Number of ACD ports for deterrence**. Two ports are used for deterrence by default. These are not specific ports but the 2 last available ports out of 14.
11. Click **OK** to confirm or **Apply** to confirm and stay in the current menu or **Cancel** if you do not want to keep the changes.

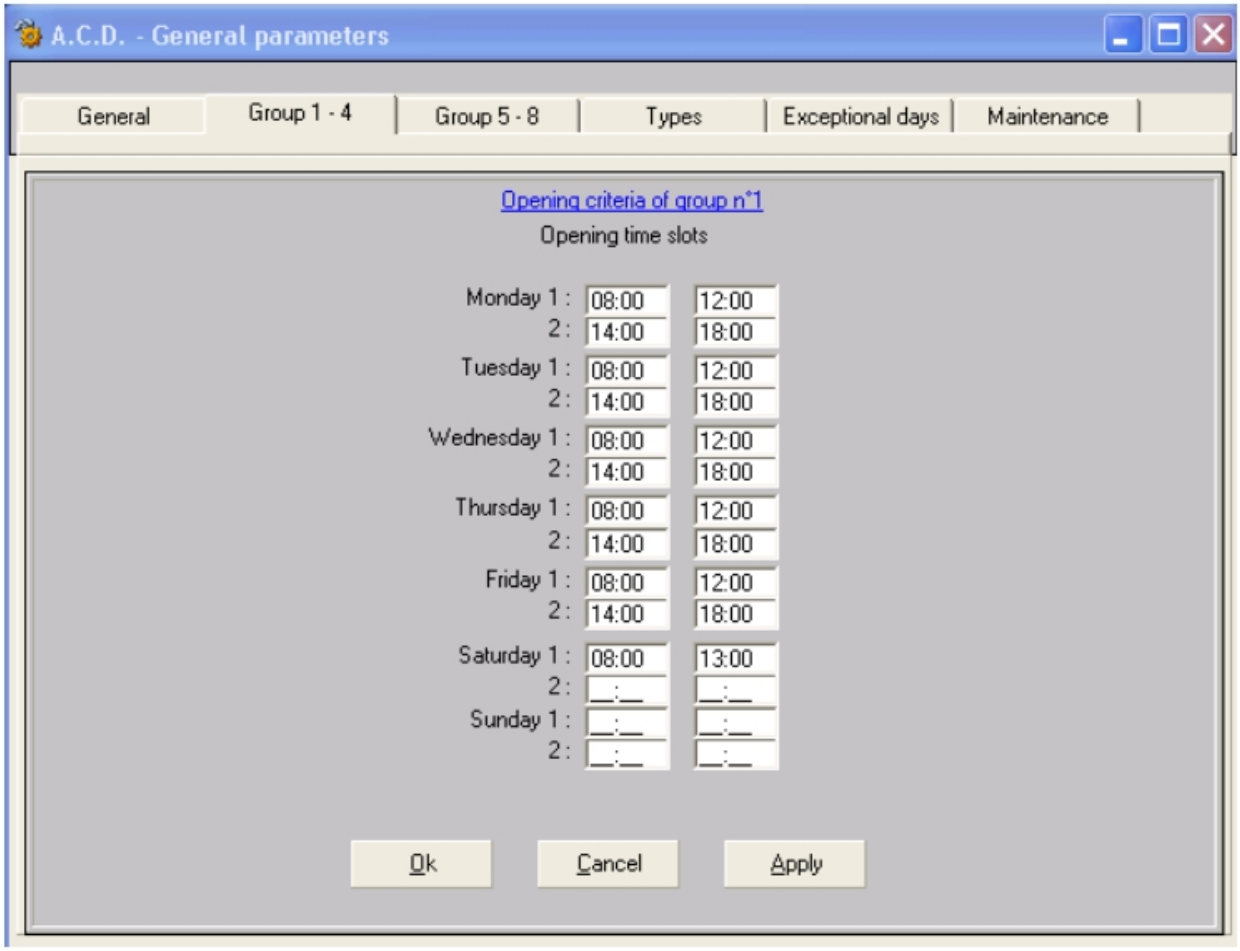
10.3.2.4 Group 1 - 4 and Group 5 - 8 Tabs

Use the tabs **Groups 1 - 4** and **Groups 5 - 8** to define the parameters of the groups.

1. Click the tab of the corresponding group(s). The following window appears where you can enter parameters for each group:



2. Enter the name of the group in **Group Heading**. The group heading is displayed on the Observation and Agent Assistant application screens, and on the agent's set if the **Display ACD Group name** option has been selected on the **ACD Setup General** tab.
3. Enter the opening and closing hours of the group:
   a. Click the **Opening Criteria** button. The following window appears:



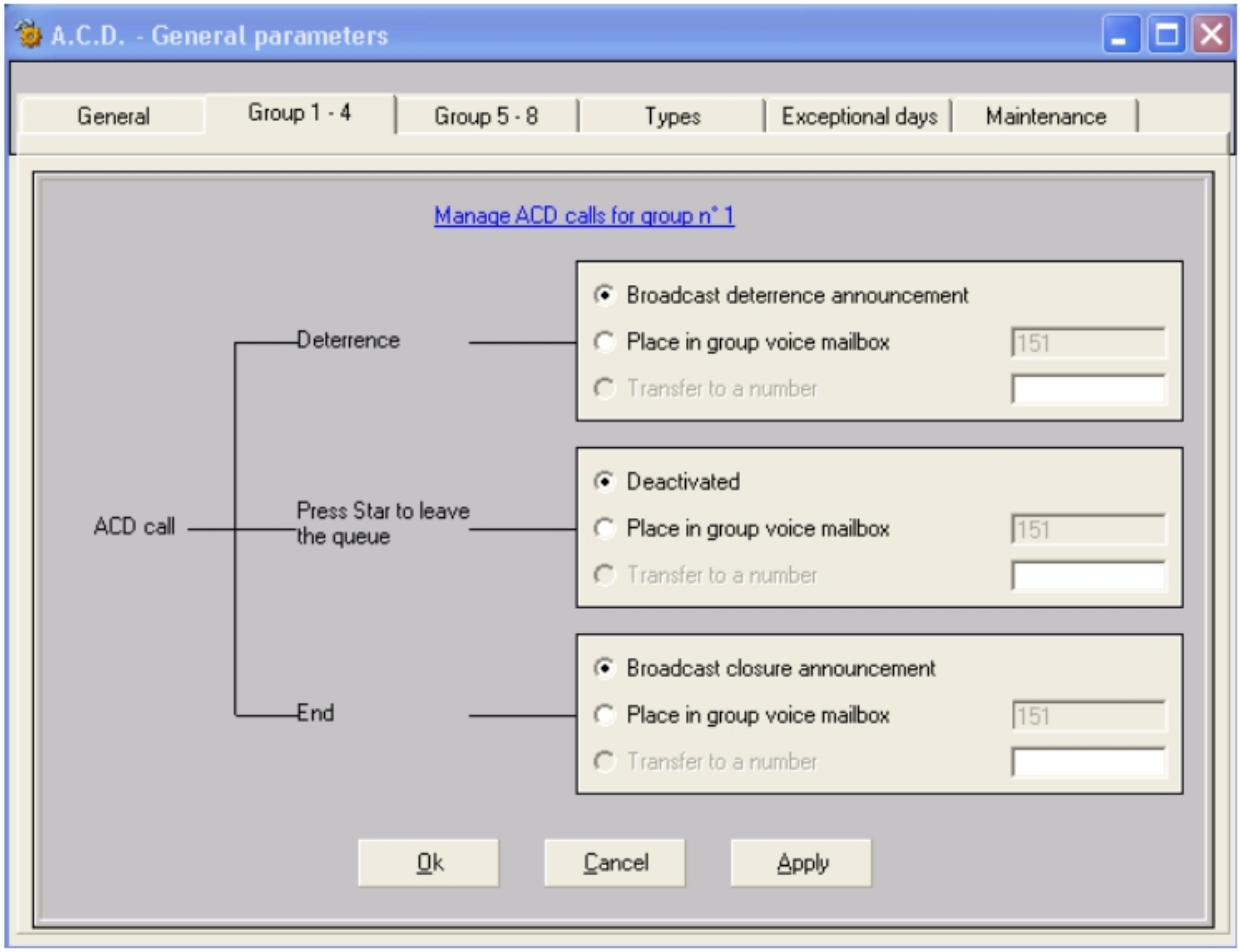
b. In the **Opening Time Slots** column, define one or two time slots for each day of the week.

Remark 1:
this data can be modified in real-time.

c. Click **Apply** to save the changes and stay on the same screen, or click **OK** to save the data and leave. Click **Cancel** if you do not want to keep the changes.

4. Enter the **Call Management** criteria:

a. Click the **Call Management** button of the required group. The following window appears:



b. Select one of three possible actions in the event an ACD call is deterred:
- Broadcast the group deterrence announcement.
- Place the call in the group mailbox.
- Transfer to an internal or external number (6 digits max.). In case of failure, the call will be transferred to the deterrence message.

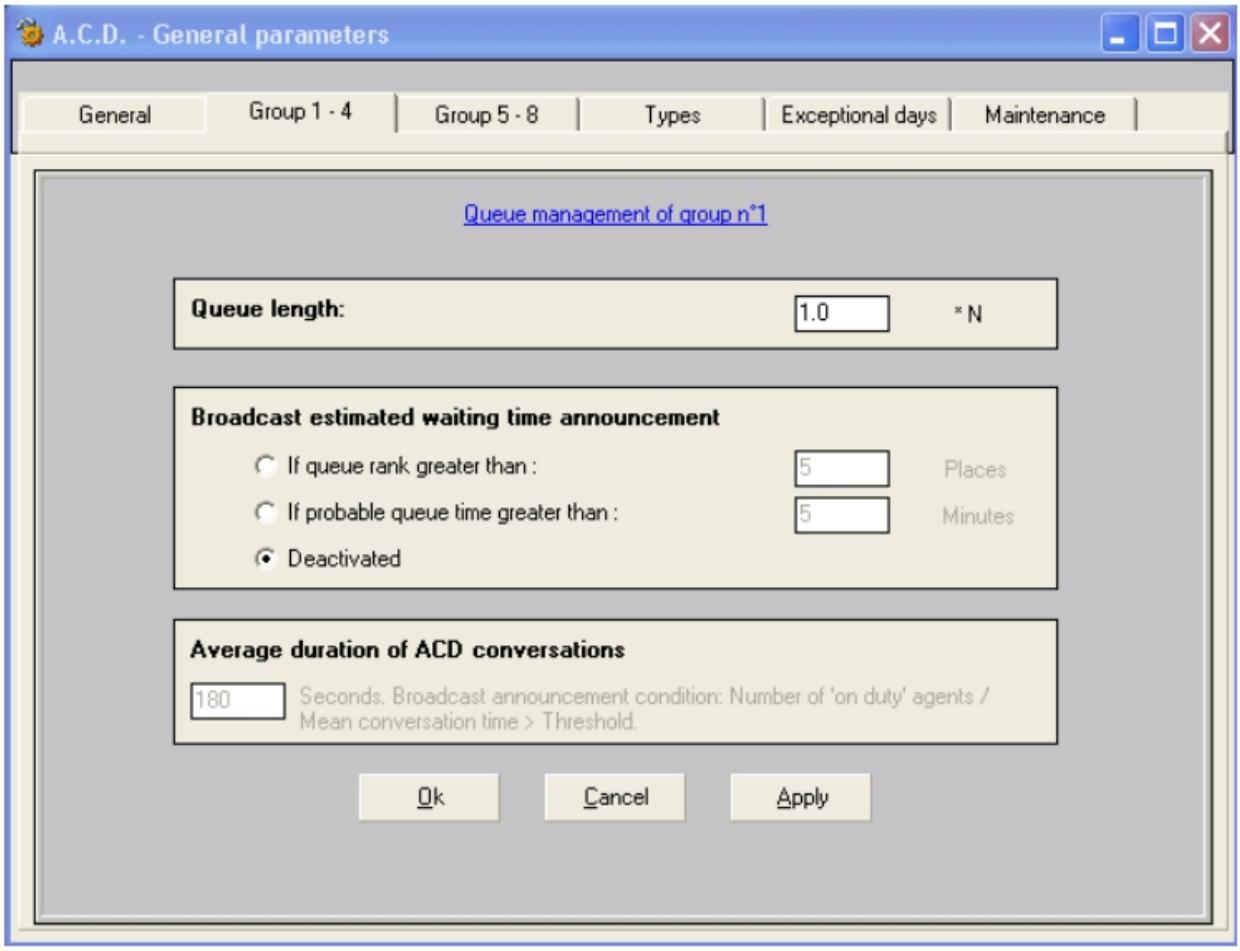
c. Select one of three possible actions in the event an ACD caller presses Star to leave the queue:
- Deactivate.
- Place the call in the group mailbox.
- Transfer to an internal or external number (6 digits max.). In case of failure, the call will be transferred to the deterrence message.

d. Select one of three possible actions in the event an ACD caller ends the call:
- Broadcast the group closure announcement.
- Place the call in the group mailbox.
- Transfer to an internal or external number (6 digits max.). In case of failure, the call will be transferred to the deterrence message.

e. Click either **OK** to save the data, or **Apply** to save and stay in the same screen. Click

Cancel if you do not want to keep the changes.

5. Enter parameters related to the management of the queue of the waiting calls for a group:
   a. Click the **Queue management** button for the appropriate group. The following screen appears:



   b. Enter the **Queue Length**. The length is equal to **N** x **k** where,
      - **N** = number of agents logged in to a terminal in the group (one licence for each login).
      - **k** = coefficient between 0 and 9, in steps of 0.1. The default value is: 1.0.

      The queue is considered to be saturated when the condition **N** x **k** is true.

      If **N** x **k** is not a whole number, the value of the queue is rounded up to the next whole number.

      Example 1:
      *If 3 agents are logged in, regardless of their status (on duty status, pause status and complementary status) in the group, and if **k**=0.5, the length of the queue is: 0.5 x 3 =1.5, i.e. 2 agents. One off duty agent is not taken into account.*

   c. Enter when to **Broadcast estimated waiting time announcement** according to the queue status of the ACD group. Three choices are possible:

- Broadcast an announcement if the rank in the queue is superior to x (this value can be defined and it specifies the alert rank in the queue). Possible value: between 0 and 32.

  Example 2:
  If x = 3, the announcement broadcast starts when the call enters the queue if 3 other calls are already queued. Once the announcement is broadcast, the ACD queues the call normally and informs the caller about the queue status and the possibility of leaving the queue.

- Broadcast an announcement if the possible queue time is superior to xx minutes. Possible value: between 1 and 99. For the estimated queue time, the "average time for an ACD conversation" parameter must be typed.

  Example 3:
  If the possible queue time is superior to 5 minutes after the announcement broadcast, the ACD queues the call normally and informs the caller about the queue status and the possibility of leaving the queue.

- Broadcast is deactivated.

Note:
There is only one announcement per ACD group. The announcement by default is "system prompt for the queue specific for group x". It can be modified with OMC or MMC Station.

d. **Average duration for ACD conversations** is the possible queue time calculated by the system taking into account the number of queued calls, the number of agents on duty in the group, and the average time defined by this parameter for an ACD conversation. Possible values are between 0 and 9999 seconds.

6. Enter the **Search Mode** used to define the method for distributing calls within the group. Select the type of search from the drop-down menu. The following choices are possible:

- **longest idle time**: The ACD assigns the call to the agent whose last ACD call took place the longest time ago.

  Remark 2:
  Non-ACD calls and the status of "temporary absence" are counted as "idle time".

- **Fixed**: The ACD assigns the call to the first free agent based on the priority rank of the agent in the group.
- **Rotating**: The ACD assigns the call through cyclical distribution.

7. Enter the **Overflow Group**, the number of another group called in the event of overflow. The time period is used to define after how many seconds the overflow function starts. The time delay is enabled if no agent is free in the group requested.

Remark 3:
This function allows a group which is under loaded to receive calls from a group which is overloaded.

If overflow occurs, the calls continue to stay in the queue of the group initially requested.

From a statistical point of view, calls are always assigned to the group initially requested.

Example 4:
Group 2 is specified as the overflow for group 1:

When a call arrives for group 1 and no agent is free in this group, a free agent is searched for in group 2. If no agents in groups 1 and 2 are free, the call is placed in the queue of group 1.

When an agent in group 2 becomes free, if no calls are waiting for this group, the calls waiting for group 1 overflow to group 2.

8. Enter the **Transfer Number**, used to define which set should be warned when an abnormal status occurs in a group. Enter a number with no more than 5 digits in this field.

The transfer number can be:

- any internal set number (preferably, the supervisor number of the application),
- an abbreviated number of Alcatel-Lucent OmniPCX Office Communication Server.

When an abnormal status is detected (group open and no agent on duty), the first call is routed to the transfer number, and the following calls are routed to the queue. It is the responsibility of the supervisor to re-establish normal operation.

Remark 4:
If the transfer number is busy or does not answer, the call is returned to the queue.

9. Enter the **Priority Order**, used to define the priority group when simultaneous calls are received or when calls are waiting and agents belong to several groups. Enter a number between 1 and 8. The same level of priority can be assigned to several groups. In this case, searches for available agents for waiting calls are conducted using the criteria of maximum queue time only.

10. Enter the **Forced status**, used to define the status of the group regardless of the status of the open/closed parameters of the time slot. Select the status from the drop-down menu. The available choices are:

- **Closed**: forces the group to be closed (for example, in the evening before the normal closing time).
- **Open**: forces the group to stay open (for example, in the evening after the normal closing time).
- **Automatic**: allows the system to return to the criteria defined in the time slot.

  Remark 5:
  switching from one status to another is never automatic; a command to return to normal mode must be sent in order to re-examine the normal open and closed parameters again.

Forcing to open or closed status is indicated on the Supervisor screens by the letter M for Manual. The group statuses are:

- OPEN M : group forced open
- CLOSED M : group forced closed
- OPEN : group open (in accordance with time slot or contact)
- CLOSED : group closed (in accordance with time slot or contact)

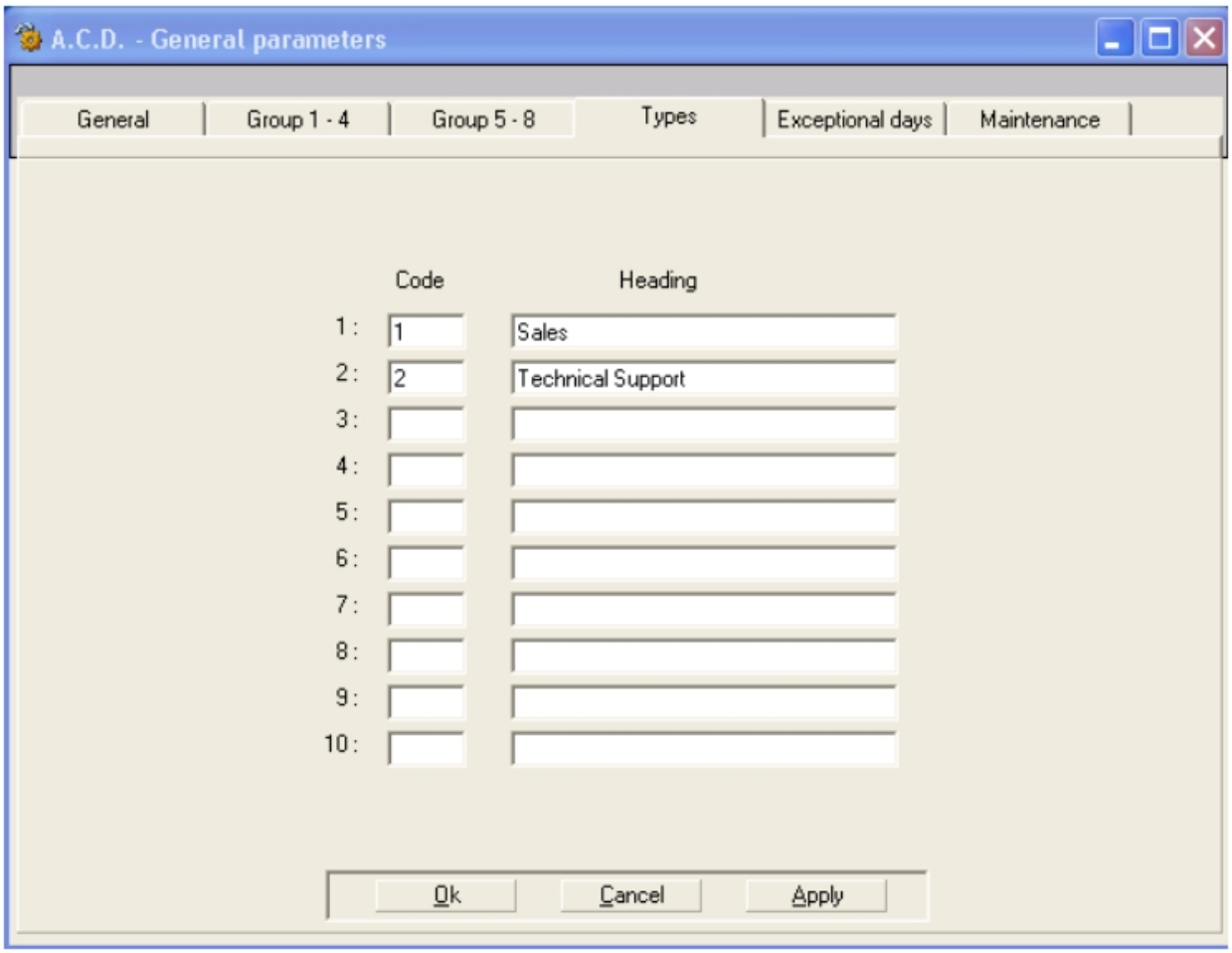
11. Click **OK** to save the group data for groups 1-4, ,or **Apply** to save the data and and stay in the same screen. Click **Cancel** if you do not want to keep the changes.

12. Follow the same procedure for groups 5 to 8 if necessary, by clicking the **Group 5 - 8** tab.

10.3.2.5 Types Tab

Use the **Types** tab to define the types of calls received by agents by assigning a heading and code for calls being processed with the Agent Assistant.

1. Click the **Types** tab. The following screen appears:

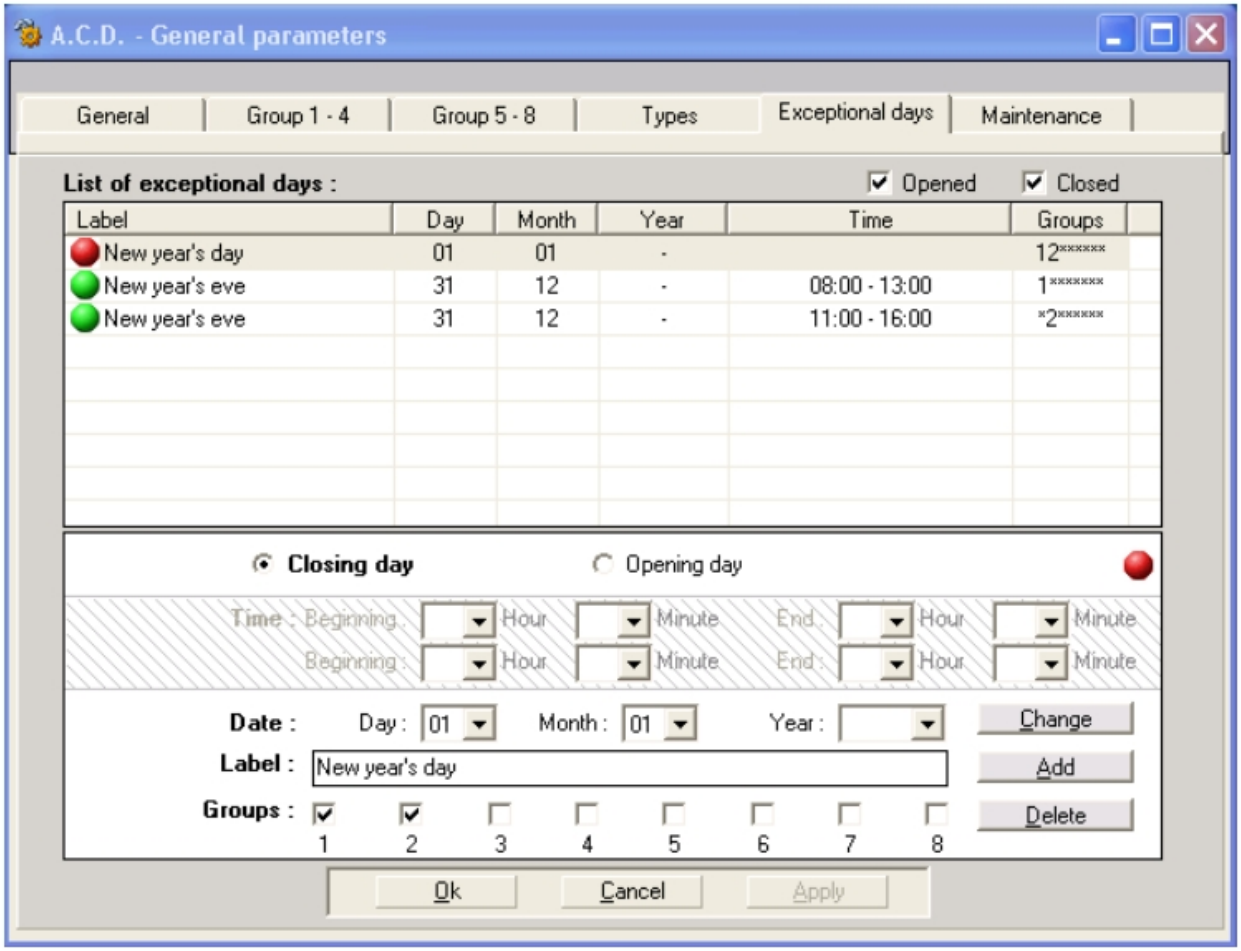


2. Enter up to ten service codes with corresponding descriptions. These type codes can be used to define the call type during an ACD call with the Agent Assistant application.
3. Click **OK** to save the data or **Apply** to save the data and stay in the same screen. Click **Cancel** if you do not want to keep the changes.

10.3.2.6 Exceptional Days Tab

Use the **Exceptional days** tab to define the exceptional closing and opening days for all groups.

1. Click the **Exceptional days** tab. The following screen appears:



The defined exceptional days are listed in the table. To list opening days, check the **Opened** box at the top of the list. To list closing days, check the **Closed** box. Both opening and closing days are listed by default.

Rules for defining exceptional days:

- If a particular day is defined both as an exceptional closing and exceptional opening day, the criteria for the exceptional opening day applies.

  Example 1:
  A full month can be defined as exceptionally closed. To remove just one day, define it as an exceptional opening day.

- If a day is defined as an exceptional opening day as well as a standard opening day (defined in the **Opening Criteria** of the **Groups** tab), the exceptional opening day criteria applies.

  Example 2:
  To define an exceptional opening time, define the day as an exceptional opening day with the exceptional opening time.

- If a day is defined as an exceptional closing day as well as a standard opening day, the exceptional closing day criteria applies.

- To define different opening times for different groups for the same exceptional opening day, enter the day more than once, applying different opening times to different groups.

2. To add an exceptional day:
   a. Select whether the day is closing (click the **Closing day** button), or opening (click the **Exceptional opening day** button).
   b. If the day is an opening day, enter the exceptional opening times in the **Time** drop-down boxes.

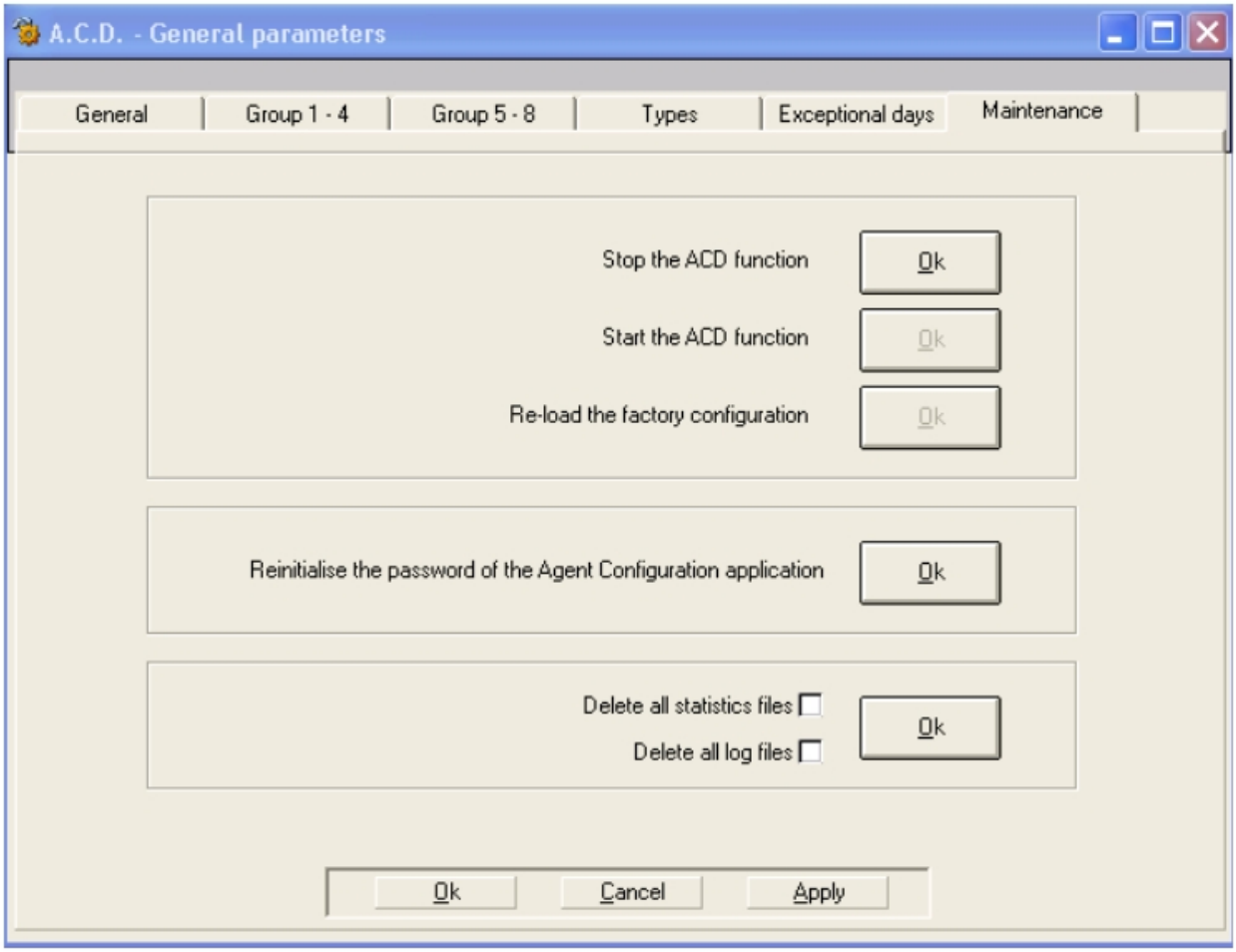
   Important:
   If an opening day has no opening times entered, the opening will not be recorded.

   c. Enter the **Day** and **Month** of the exceptional day in the **Date** drop-down boxes. To define a full month, leave the day blank. The **Year** is optional.
   d. Enter a **Label** for the exceptional day.
   e. Select the **Groups** to which this exceptional day applies by checking the box above the group number.
   f. Click the **Add** button.
3. To change the criteria for a defined exceptional day:
   a. Select the day from the list of exceptional days.
   b. Make the desired changes.
   c. Click the **Change** button.
4. To delete a defined exceptional day:
   a. Select the day from the list of exceptional days.
   b. Click the **Delete** button.
5. After adding, changing, or deleting days, click **Apply** to save the modifications and stay on the Exceptional days screen, or click **OK** to save modifications and leave the screen. Click **Cancel** if you do not want to save the modifications.

10.3.2.7 Maintenance Tab

Use the **Maintenance** tab to stop, start, and restore the ACD, and to perform log and statistics file maintenance. When the ACD application is stopped, the ACD function is completely inhibited in the system. Stopping and restarting the ACD function may be useful during maintenance and debugging operations.

1. Click the **Maintenance** tab. The following screen appears:



2. Click the associated **OK** button to perform the following tasks:
   - **Stop the ACD function**: The ACD is stopped in the system.
   - **Start the ACD function**: the ACD is started in the system.
   - **Reload factory settings**: the default ACD configuration is reloaded in the system.

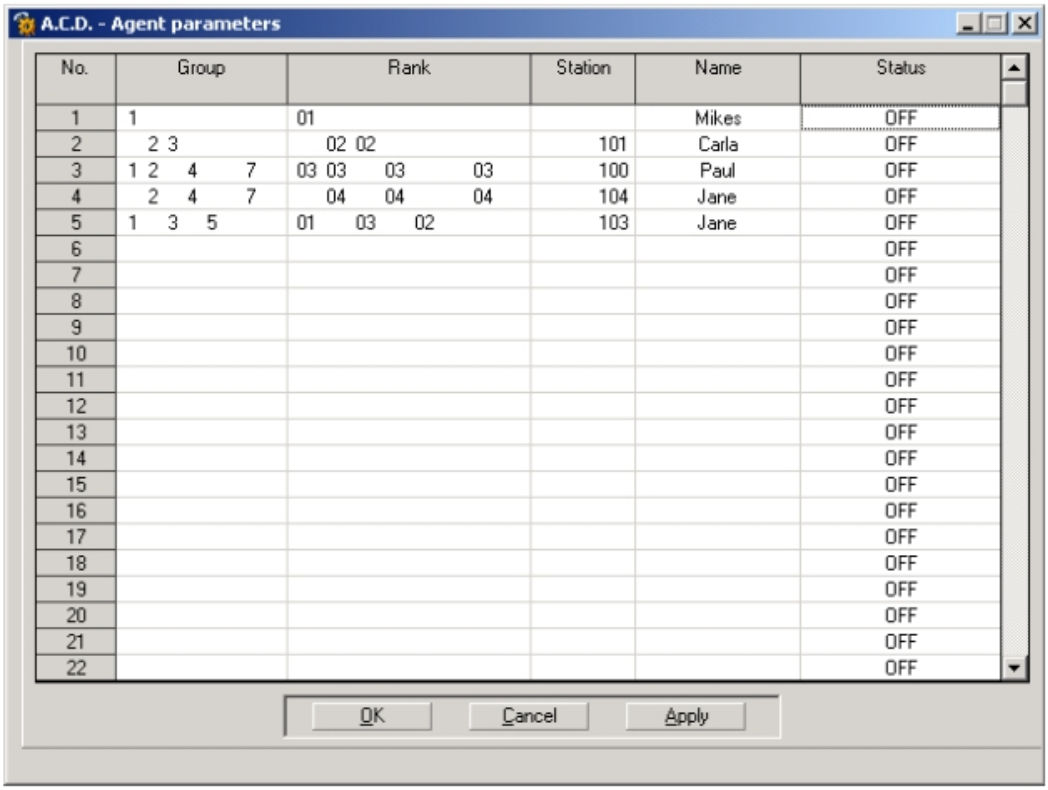
     Note:
     *A cold reset of the system does not delete the ACD configuration. To do this, use the **Reload Factory Settings** button. The announcements are never deleted.*
   - **Reinitialise the password of the Agent configuration's application** to **help1954**.
   - **Delete all statistics files**: erase all the statistics files from PBX.
   - **Delete all the log files**: erase all the log files from PBX.

10.3.3 Agent Parameters

10.3.3.1 Configuration of agent parameters

10.3.3.1.1 Modification of the agent parameters

1. Click the **Agent Parameters** icon. The **A.C.D. - Agent Parameters** window appears.



- **N°: Agent Number**: identification number of each agent (number of the lines, 1 to 32)
- **Group: Associated Groups**: the agent's group; an agent can belong to several groups.
- **Rank**: priority rank assigned to each agent, in each of the groups they belong to.
- **Station**: directory number of the agent's set.
- **Name**: the agent's name.
- **Status**: operating status of the agent (on duty, off duty, clerical work or temporary absence).

2. For each line of the table (1 to 32), double-click on one of the headings. A data entry window appears for the current line. You can define the parameters of:
   a. The groups to which the agent belongs, by checking and unchecking the **Associated Groups** boxes (1 to 8).
   b. The priority rank of the agent in the groups he/she belongs to, by entering a number in the **Rank** field (1 to 32). The priority rank is predefined if the group is using **Fixed** distribution.
   c. The set number of an agent, by entering a directory number in the **Set Number** field.
   d. The name or identifier of the agent by entering a name in the **Name** field.
   e. The status of the agent, by selecting **On Duty**, **Off Duty**, **Temporary Absence** or **Clerical Work** in the **Status** drop-down menu.
3. Click **OK** to confirm the data or **Apply** to stay in the current menu.

Caution:
During the modification of the system's directory or during the creation of a phone set, the directory of ACD is not automatically updated. To obtain an identical image of the directory of OmniPCX Office in the ACD part, for the creation or modification of the list of agents, it is necessary to reset the ACD engine (or reset OmniPCX Office).

10.3.3.1.2 Assignment of agents to groups and operating status

The agent is characterized by his/her phone set and the operating status of the set. In order to optimize their management, agents are organized into groups (skills groups for example).

An agent can belong to one or more groups. An agent can have one of the 4 operating statuses below:

1. **On duty**: the agent is assigned to ACD groups.
2. **Off duty**: the agent has withdrawn from all ACD groups.
3. **Temporary absence**: the agent has temporarily gone off duty for a break. At the end of this break, agents must come back on duty so that they are available again to process a new ACD call.
   Periods of temporary absence are not considered as work/service time in the statistics.
4. **Clerical work**: following a conversation, the agent may need to assess the call and fill out an information screen for example; he/she temporarily withdraws from the call distribution chain.
   Once this work is complete, agents must come back on duty so that they are available again to process a new call.
   Clerical work periods are considered as work time for the call distribution criteria in the statistics.

   Remark:
   For the statistics, the "idle time" is processed differently, depending on whether the agent is temporarily absent or is doing clerical work,

   - if the agent is temporarily absent, the activity time is taken into account from the last ACD conversation (when the agent hangs up),

   - if the agent is doing clerical work, the activity time is taken into account from when the agent comes back on duty following this period of clerical work.

The PC-based Agent Assistant application provides agents with an interface to:

- change their status (on duty, off duty, temporary absence, clerical work) via an intuitive interface,
- access functions such as:
  - real-time observation of statistics,
  - definition of call types,
  - multi-skills management (agents belonging to several ACD groups),
  - free seating,
  - customer information screen pop-ups.

For more information, refer to the "Agent Assistant application" chapter.

This section describes the parameters that must be defined to declare the agents and the group(s) they belong to.

10.3.3.1.3 Login/logout from a phone set

The functionality "login/logout on phone set" is available from version R4.0 . This allows any phone set to log in and log out in one or several ACD groups.

It will then appear automatically in the list of agents.

This service is available with all the phone set types (Analog, Reflexes, DECT Reflexes, Alcatel-Lucent 8 series, and Alcatel-Lucent 9 series sets).

It is accessible via a UPK function key (ACD Login/logout) or via a service code of the main numbering plan (ACD function: base 1 for login and 0 for log out).

A password is required only if it was created with the Agent Assistant application or an Alcatel-Lucent 8 series or Alcatel-Lucent 9 series phone set. This password consists of exactly 4 numeric characters. No other types of character are allowed, otherwise an agent equipped with Analog, Reflexes or DECT Reflexes will not be able to log in.

Caution:

Each time an agent is logged in, the agent automatically appears in the list of agents and therefore uses an agent's license. There are 5, 10, 20, or 32 licenses available, according to the purchase.

10.3.4 Line Parameters

The lines table is used to associate caller numbers(CLI) and/or called numbers (DDI number, cyclical group number) with the different ACD groups (1 to 8) and agent status functions (on duty, off duty, clerical work or temporary absence).

When defining the system parameters, the complete table will be filled in either by importing the data collection file, or manually, on a number by number basis.

It is also possible to use the line table to enter VIP caller numbers in order to route them to a priority ACD group.

It is possible to use specific hunting groups to call the different ACD groups in order to limit access, the number of calls waiting, or the traffic of each ACD group; this is done by simply adjusting the number of ACD ports contained in the different groups.

Note:

When a call is transferred from the MLAA application to ACD groups, Calling Line Identification information is included in the transfer.

10.3.4.1 Configuration of lines

The parameters of lines can be configured to make an application number correspond to:

- A "Caller" number
- A "Called" number (DDI)
- A combination of the two numbers

For example, it is possible to make the access to each agent group correspond to:

- a "Caller" number depending on the country the call comes from (for example, depending on the language of the caller);
- a given "Called" number, in order to reach the correct ACD group (corresponding to a given service);
- a combination of both (country + service).

Remark:

Several numbers can correspond to the same application.

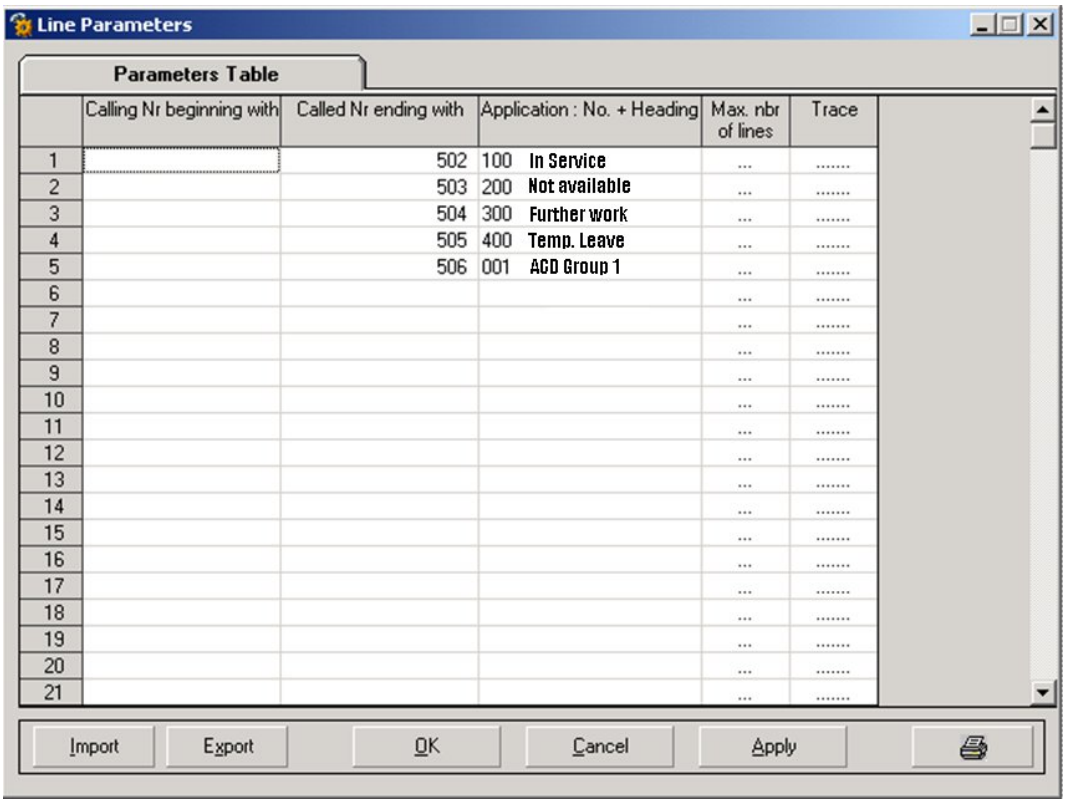
1000 different numbers can be assigned in this way.

This list is created during the data collection process.

10.3.4.1.1 Procedure

To fill in the line table, do the following:

1. Click the **Line Parameters** icon. The **Line Parameters** window appears. It contains a tab with the following columns:



- **Caller No. beginning with**: corresponds to the caller numbers likely to be received by the server.
- **Called No. ending with**: corresponds to the DDI numbers likely to be received by the server.
- **Application: No. + Heading**
- **Max. number of lines**: used to limit the number of ACD ports to specific services.
  Remark: Not compatible with the function of ACD ports reserved for deterrence.
- **Trace**: used to trace specific routing problems.
  Remark: Set on this parameter for a short period only and under the supervision of the technical support.

2. To fill in or modify the fields, double-click the area of the table to be modified in order to access the corresponding data entry area. The data entry window will differ depending on the column selected.
   - **Caller No. beginning with** (CLI) data entry window
     The number on each line of the table can be a complete number, but it is also possible to make selections of blocks of digits in order to:
     - analyse the country code (from 1 to 3 digits on the left),
     - analyse the region code (from one to six digits depending on the country of installation),
     - analyse the complete number, or part of the number (for example, the last digit on the right to distribute traffic between groups of agents).

     Remarks:
     - Numbers are analysed from left to right.
     - The maximum number length is 20 digits.
     - The character X can be used as a joker.
   - **Called No. ending with** (DDI) data entry window
     Numbers are analysed from left to right.
     If a number received is not shown in the list, an error message appears in the Events file. The server does not answer and the caller hears the ringback tone.
   - **Application: No. + Heading** data entry window
     From the list of applications, choose the one which corresponds to the number received. The same number received can be assigned to two different applications. Calls will be routed as a priority to the application registered at the highest level of the table.
     Analysis process
     A call entering the server is characterized by the pairing [DDIr - CLIr]. The output event of the process described here is either the Application Number, or an execution command taking the physical access configuration into account.

     Caution 1:
     the comparison stops as soon as the first entry satisfying the condition is found. As a result, it is important to fill in the table starting with particular cases (the longest numbers) and ending with general cases (the shortest numbers).
     The analysis process is as follows:
     - 1st operation: CLIr/CLIs and DDIr/DDIs comparison. The system searches in the principal table for the entry matching the condition: CLIr = *CLIs and DDIr = *DDIs
       If it exists, it is unique. In this case, the output event of the process is the application number associated with this pairing.
       If it does not exist, the system moves to the second operation.
     - 2nd operation: comparison of CLIr/CLIs and DDIs not entered. The system searches in the principal table for the entry matching the condition: CLIr = *CLIs and DDIs = *0
       If it exists, it is unique. In this case, the output event of the process is the application number associated with this pairing.
       If it does not exist, the system moves to the third operation.
     - 3rd operation: comparison of DDIr/DDIs and CLIs not entered. The system searches in the principal table for the entry matching the condition: DDIr = *DDIs and CLIs = *0.
       If it exists, it is unique. In this case, the output event of the process is the application number associated with this pairing.
       If it does not exist, the output event of the process is a command taking the

physical access configuration into account.

Caution 2:
this is not a case of simple equality. The conditions of equality are outlined below.
Method for comparing numbers

- **CLI**:
  Condition 1: condition based on content (the number). The CLIr/CLIs comparison is made starting with the digit of the greatest weight. It continues digit by digit and ends by comparing the digit of the least weight of the shortest number.
  The condition CLIr=CLIs is fulfilled if condition 1 is fulfilled. In other words, there are no conditions related to the format. As a result, there can be no equality if one of the Network or System parameters is not entered.
- **DDI**:
  Condition 1: condition based on content (the number). The DDIr/DDIs comparison is made starting with the digit of the least weight. It continues digit by digit and ends by comparing the digit of the greatest weight of the shortest number.
  The condition DDIr=DDIs is fulfilled if condition 1 is fulfilled. In other words, there are no conditions related to the format. As a result, there can be no equality if one of the Network or System parameters is not entered.

Importing/exporting files

1. Click **Import** to import data ("caller" numbers or others) from a database or spreadsheet. The **Import a List** window is used to access the .csv file that you want to import.

   Remark:
   if you also import application numbers, these applications must exist on the server, otherwise the field will remain blank.
   The character used to separate the columns is ";".
   In general, the first line corresponds to the column headings. In order to avoid this first line being taken into account during the import operation, the relevant headings must start with the character "/".

   Example 1:
   in Microsoft Excel:

	A	B	C
1	**/ CLI No**	**DDI No**	**Application No**
2	33 1		701
3	33 2		702
4	33 3		702
5	33 4		703
6	33 5		703

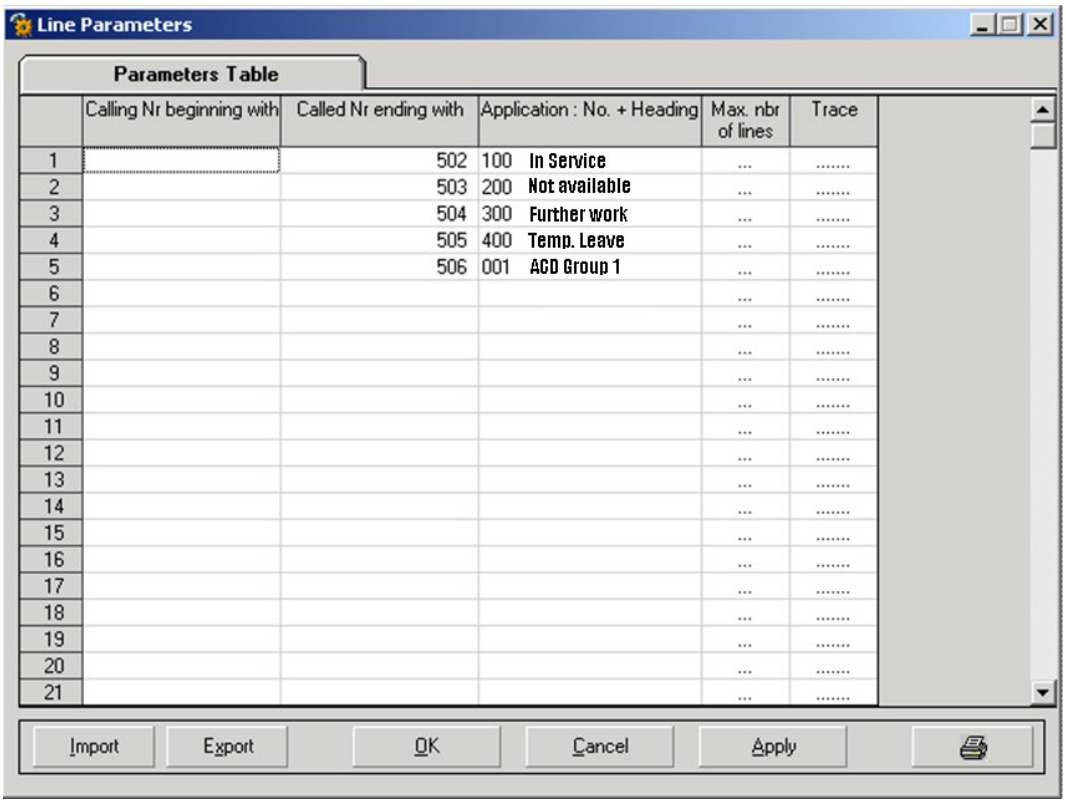
   Only the first four columns will be imported. It is not obligatory to fill in the columns on the right. The file must be saved in .csv format. To print, click the Printer icon.

2. Click **Export** to export the file from the server to the spreadsheet in order to update it.
3. Click **OK** to confirm.

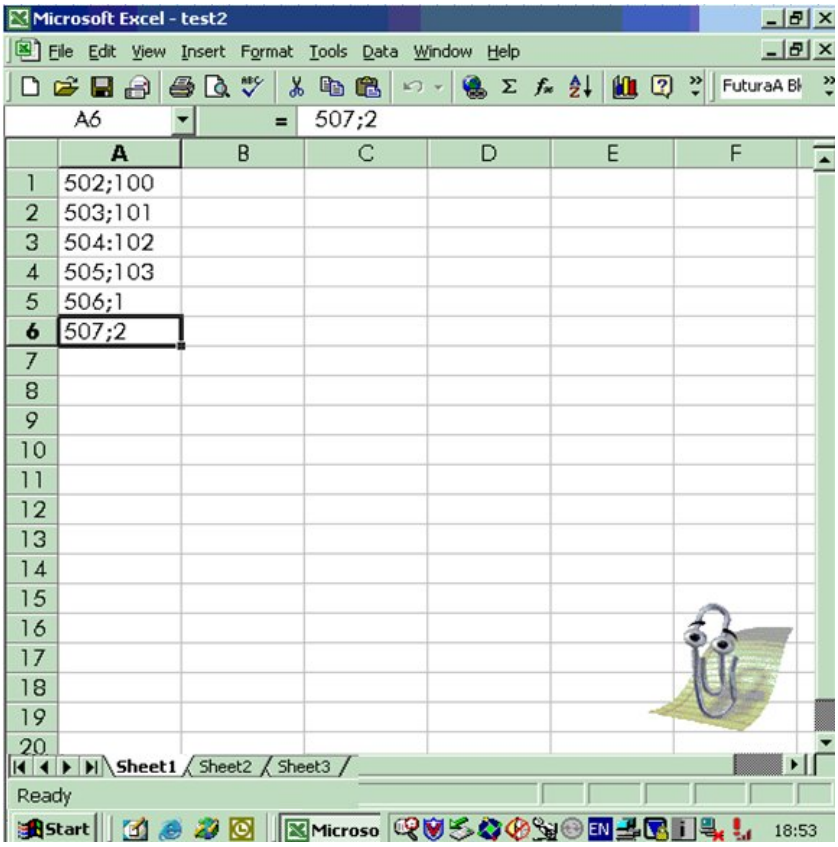
Example 2:

importing/exporting line parameters

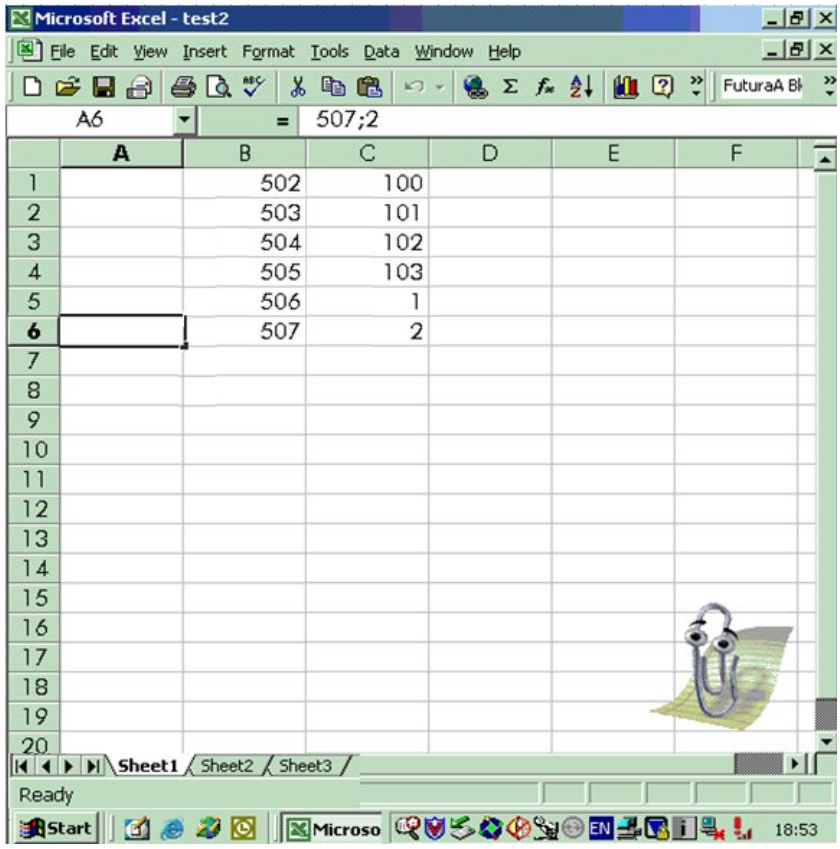
The parameters of the lines existing in the ACD are defined in the following screen:



Export the parameters by clicking **Export**. The .CSV Excel file is displayed.



In this Excel file, select column **A**, then modify the format by selecting **Data/Convert**. An assistant is displayed. Click in succession **Delimited**, **Next**, **Semi-colon**, **Next**, **End**, **Save**. The next file is displayed.



Complete this file and then re-import it.

10.4 Announcements

10.4.1 Overview

Announcements are broadcast while telephone traffic is being processed. No default announcements are provided by the call center, but default announcements (A-law and µ-law) designed for test purposes are available for download in OMC. For a running system, customized announcements must be created and downloaded.

10.4.1.1 DESCRIPTION OF THE ANNOUNCEMENTS

The different types of announcement are:

- **Welcome announcement** This announcement is broadcast when a call arrives in the group.
- **Queue announcements (Waiting 1, Waiting 2, Estimated Waiting Time)**
  - Waiting 1 is used when the call joins the queue for the first time; it is broadcast once only.
  - Waiting 2 is used after Waiting 1 or Estimated Waiting Time; it is broadcast

continuously until the call leaves the queue (this announcement may contain music).

- Estimated Waiting Time is broadcast to advise the caller that they are likely to have a certain minimum waiting time in the queue before their call is answered.

- **Deterrence announcement** This announcement is broadcast when the queue is saturated. It can also be broadcast when the ACD ports dedicated to ACD traffic are saturated (this depends on the configuration of the ACD ports dedicated to deterrence).
- **Closing announcement** This announcement is broadcast when the ACD group is closed.

The permissible durations of the announcements depend on whether the system has a hard disk, as follows:

- For a system without a hard disk, only one set of announcements for all ACD groups is permitted. The total recording time for all six announcements is 120 seconds.
- For a system with a hard disk, a set of announcements for each ACD group is permitted. The minimum and maximum durations of the announcements in a set are shown in the table below.

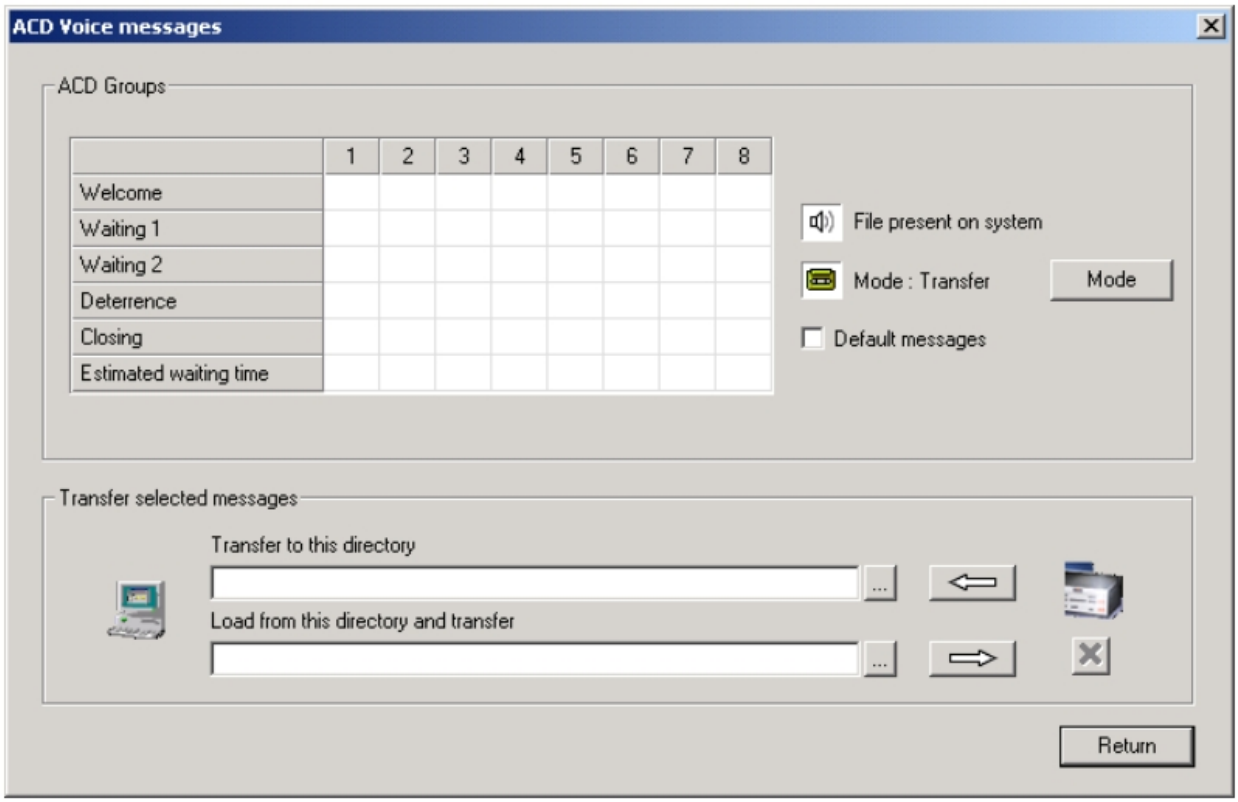
Announcement	Minimum Duration	Maximum Duration
Welcome	0 seconds	60 seconds
Waiting 1	0 seconds	60 seconds
Waiting 2	20 seconds	300 seconds
Estimated Waiting Time	0 seconds	60 seconds
Deterrence	0 seconds	60 seconds
Closing	0 seconds	60 seconds

10.4.2 Operation

10.4.2.1 SELECTING ANNOUNCEMENTS

To select the announcement you want to use, do the following:

1. Click **ACD Voice Messages**. The **ACD Voice Messages** window appears. This window has the following two areas:
   - The **ACD Groups** area is used to select the announcements for each group or all the groups.
   - The **Transfer Selected Messages** area is used to import or export announcements to the call center or to the system.



The **ACD Groups** area contains a table allowing you to:

- see which announcements are present in the system,
- select an announcement to be added or replaced.

To change from Transfer mode to Delete mode, click on the button **Mode**.
It is not possible to delete announcements at the same time as adding or replacing announcements.

Note 1:
Default messages are available which take into account the coding (A-law or µ-law) used in your country.

2. In the **Transfer Selected Messages** area, click the button to the right of the field **Load From This Folder and Transfer**.

   The **Select Folder** window is displayed.

   The announcements are by default saved in:

   C:/Program Files/PCXTools/OMC/R500_xxx/VoiceMessages/a_law

   48 messages are available (6 for each ACD group). Each message is identified by a file made up of 3 figures x, y and z and with the extension .wav:

   - **x** corresponds to the number of the ACD group (1 to 8)
   - **y** is always equal to 0
   - **z** corresponds to the message of the ACD group (1 to 6)

   The messages types are as follows:

   - **1** corresponds to the Welcome message

- **2** to the Waiting 1 message
- **3** to the Waiting 2 message
- **4** to the Deterrence message
- **5** to the Closing message
- **6** to the Estimated Waiting Time message

For example, file 305.wav corresponds to the Closing message for group 3.

Remark:
on starting the ACD, the system does not contain any messages. To conduct tests, it is therefore essential to load the default ACD messages.

3. Select the announcements and click the transfer button **(=>)**. The messages selected are transferred to the call center.
4. Click **OK**. The **ACD Voice Messages** window disappears.

Note 2:
*When deleting an announcement, the action is not executed using the transfer button **(=>)** but using the delete button (**X**) instead (this button is only accessible in Delete mode).*

10.4.2.2 CREATING ANNOUNCEMENT MESSAGES

To create your own announcement messages, you can use the recording software available on your PC (Window/Accessories/Multimedia/Sound Recorder) or any multimedia application.

10.4.2.2.1 Recording announcements (.wav) on a PC

Proceed as follows:

1. On your PC, open a recording tool by clicking **Start > Programs > Accessories > Multimedia (or Entertainment) > Sound Recorder**. The following window is displayed:

In order to record the message, your computer must be fitted with a sound card. Otherwise, a message informs you that the recorder is operating in restricted mode.

2. If the sound card is available and configured, start to record your message by clicking on the red button in the bottom right of the window.
3. To stop the recording, click the rectangular button.
4. To check and listen to the recorded message, click the triangular button.
5. If you are happy with the message, record it by clicking **File > Save**. Give it a file name and check the message format.

Caution:
announcements must have the format CCITT A-law/µ-law 8 KHz, 8 bits, mono. The announcements created must have the same name as the default messages.

6. If the format is not correct, click **Change** and select the format CITT A-law/µ-law 8 KHz, 8 bits, mono. Click **OK** to confirm and **OK** again to save the message.

10.4.2.2.2 Recording ACD messages using a phone set

You can record ACD messages using a Reflexes 4035 (Advanced) telephone or any one of the following telephones: Alcatel-Lucent IP Touch 4038 Phone, Alcatel-Lucent 4039 Digital Phone and Alcatel-Lucent IP Touch 4068 Phone. A special menu allows you to record each announcement message for each ACD group. To access this menu:

- on a Reflexes 4035 (Advanced) telephone, follow the path System/install/voice/ACD,
- on a Alcatel-Lucent IP Touch 4038 Phone, Alcatel-Lucent 4039 Digital Phone or Alcatel-Lucent IP Touch 4068 Phone telephone, follow the path Menu/operator/Advanced/Voice/ACD.

10.4.2.2.3 Converting an announcement file

If the format of your file is not compatible, convert it using the following procedure:

- Open the .wav file to be modified in **Sound Recorder** and click **File > Properties** to check the file format.
- If the format shown is different from CCITT A-Law/µ-law 8 KHz, 8 bits, mono, click **Convert Now...**. A window opens; select the format CCITT A-Law or CCITT µ-law and click **OK** to confirm.
- Save your file.

10.4.2.2.4 Recording ACD messages using a professional studio

For optimum quality, the services of a professional recording studio should be used. If this option is chosen, observe the file format required.

10.5 Agent Assistant

10.5.1 Overview

The Agent Assistant is a user interface available on the agent's PC. By associating agents' telephone sets with their PCs, they have a user-friendly working environment in which to manage their sets.

Agents can use this window to more easily declare the status of their set (on duty, off duty, temporary absence, clerical work) as well as accessing functions such as real-time observation of statistics, definition of call types, multi-skills management, free seating or extraction of a customer information screen.

10.5.1.1 Introduction to the application

Thanks to a gateway integrated in the call centre, each agent PC is in contact with the call centre via the local network. When a call is distributed, the PC starts communicating with the call centre. For example when the set rings, the application knows the number of the caller and the time spent in the queue, and can display this information on the screen.

10.5.1.2 Description of functions

The Agent Assistant provides three groups of functions:

1. Control functions.
   These are used to identify the agent, the status of the agent's set, the skills group to which he/she belongs and they also provide information on calls.
2. Statistical functions.
3. Information screen pop-up functions.

10.5.1.2.1 Control functions

The control functions are:

- free seating,
- status declaration,
- skills management,
- provision of information on calls.

Free seating

This function is used to identify agents via their identifiers and access codes. This means that any agent can occupy any position in the call centre without having to change any of his/her details.

When a session opens, agents must identify themselves by selecting the identifier assigned to them and by entering their password. If necessary, they can click the **Change** button to change their password.

Status declaration

Agents can easily declare the different activity statuses possible:

- **On duty**: agents are assigned to take calls in the groups to which they belong.
- **Clerical work**: the agent withdraws temporarily from the call distribution chain. For example, when the agent is required to perform a task related to the call, such as filling in a form, sending an e-mail or fax, etc.
- **Temporary absence**: the agent goes temporarily off duty for a break. Periods of temporary absence are not considered as work time.
- **Off duty**: the agent is no longer available to receive ACD calls.
- **Information**: the information button is used to warn the agent of a change in status or that he/she has been assigned to a different group, this change being conducted outside the Agent Assistant. The information button flashes to inform the agent of a forced change. To acknowledge the message, the agent must click this button.

The call centre manager can force the status of an agent. In this case, an icon in the Agent Assistant flashes to show the agent that his/her status has been forced.

Skills management

When they come on duty, users can declare their skills (hotline, purchasing, sales for example). The call centre manages this information dynamically in order to route calls efficiently.

Call information

When the agent's set starts ringing, the application is activated with the data related to the call. The agent can be provided with the following information:

- Caller number.
- Called number.
- ACD group requested.
- Caller queuing time.
- Conversation time.
- Activation of the customer information pop-up, if the screen pop-up does not appear automatically or if the pop-up was closed before the end of the conversation.
- Choice of call type.

Definition of call types

The call type is noted by the agent processing the call, using coding specified in advance by the call centre manager. The call type can only be noted during the call itself. The agent selects the call type from a drop-down menu showing the predefined types.

This function is used to improve call analysis and relate calls directly to the activity and profitability of the call centre.

The call centre manager can define the call types in the window **A.C.D. - General Parameters** in the configuration module menu, in the **Types** tab. Ten types can be entered, by specifying a number and heading for each type.

10.5.1.2.2 Statistics functions

The statistics functions allow the agent to manage his/her work effectively.

Personal data

The agent is provided with counters (counters related to status, call activity rate or distribution by type) to directly manage his/her work and time.

- **Status counter**: displayed as a graph, this counter shows the time spent by the agent in the different statuses possible (on duty, clerical work, temporary absence and off duty) since the counter was last reset and only while the application is running. The data is expressed in minutes. The agent can reset the counter whenever required, or choose to reset the values whenever he/she leaves the Agent Assistant.
- **Activity rate**: displayed as a graph, this counter shows the time spent by the agent on ACD calls over the last hour or last half-hour, depending on the parameters configured in the ACD. This rate is given as a percentage; it can be used to assess whether the agent is receiving too many or too few calls.
- **Call types table**: displayed as a table, this information is used to determine the total number of calls defined by the agent and broken down by call type (maximum of 10). The difference between the total calls answered and the number of call types defined can be used to determine the number of calls where the type was not defined. The agent can reset the counter whenever required, or choose to reset the values whenever he/she leaves the Agent Assistant.

Supervision

This function is used to determine the total load of the ACD in real time. Each agent is both the manager and supervisor of his/her work. By combining supervision of traffic and declaration of skills, the agent can directly participate in the smooth running of the ACD and in the smooth flow of his/her traffic, by monitoring changes in indicators.

Statistical indicators provide the following information for each ACD group which the agent is connected to:

- the number of calls waiting as a function of the wait time for each call,
- the number of calls answered,
- the number of calls which can be held in the queue of each group,
- the status of each group (open, closed, saturated).

List of calls

The list of calls is used to keep a record of all the agent's calls. It allows the agent to accurately monitor his/her work.

The following call information is provided:

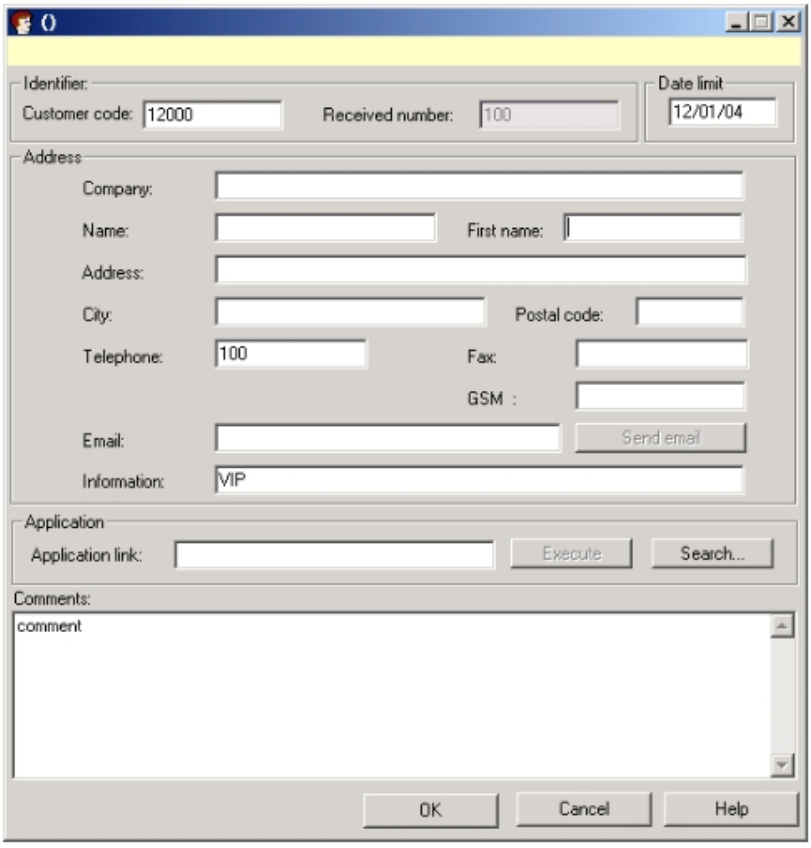
- Caller: number received,
- Called number: number called by the customer,
- Customer code: customer code which may be entered by the agent in the **Customer Code** field,
- Group: ACD group requested,
- Type: name of the call type,
- Date: date of the call,
- Time: time of the call,
- Conversation: conversation time,
- Queue: time spent in the queue before being connected to the agent.

The list is deleted on a cyclical basis (this option must be defined in the configuration menu of the ACD), or can be deleted by the agent at any time in the consultation interface.

10.5.1.2.3 Customer information screen extraction function

This function allows an agent to extract information on a customer. The call centre administrator must define the type of "file pop-up" using the agent configuration application. The client information file is automatically extracted if the agent has selected the "automatic file pop-up" option in the configuration.

In other cases, the agent can ask for a "manual file pop-up" available in the toolbar. The list of clients is then displayed and it is possible to choose the corresponding client file:



The file pop-up may be executed via three different modes:

Integrated mode: using the built-in tools.

Connected mode: using an application which can be instantiated as a Com Server. For example, with the applications in the Microsoft Office range, such as Microsoft Outlook.

Specific mode: using a third-party CRM (Customer Relations Management) application.

This feature is only available on PCs using Windows NT SP6, Windows 2000 SP4 and Windows XP operating systems.

Integrated mode in local

The Agent Assistant includes a built-in contact management application. This is a database in Microsoft Access format which can be shared over a network. The database contains the standard fields for contact management requirements: name, telephone, address, e-mail, etc. Each customer information screen can be displayed in "standard" or HTML format.

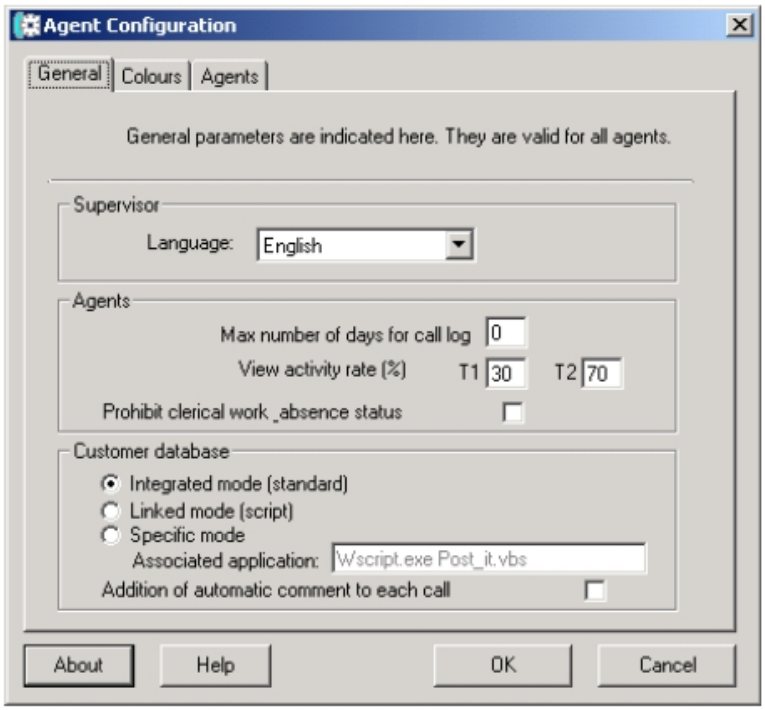
Users can add additional fields specific to the management of their area of expertise; these modifications do not, however, appear on the information screen.

Agents can be made responsible for updating the database, their writing rights being opened via an access code. They can then make the information screens available to other agents when the call is presented.

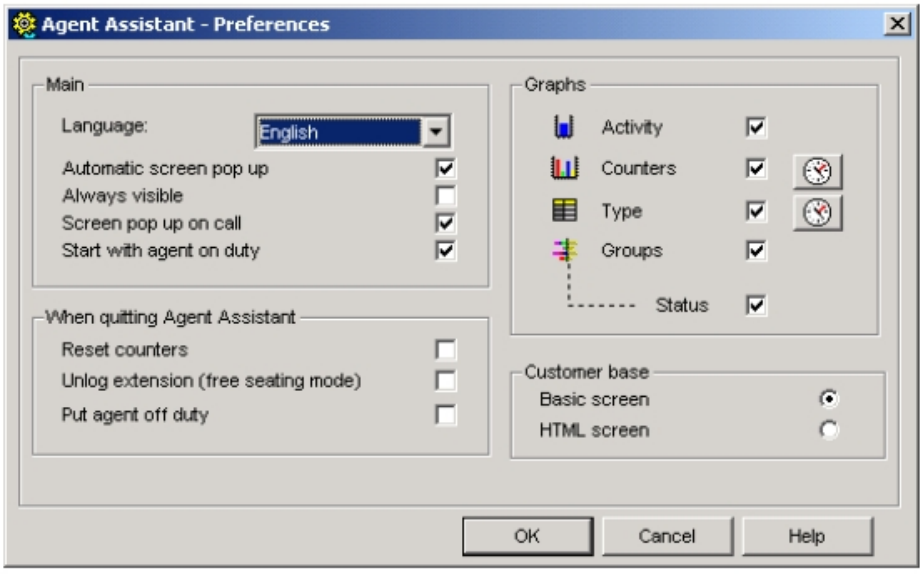
The database has a direct link with messaging services. An e-mail can be sent to a contact by clicking their information screen.

Integrated mode with standard format

To enable the file pop-up in standard mode, it is necessary to select **Integrated mode standard** in the Agent Configuration application:



Then, to activate the file pop-up, the **Automatic screen pop-up** option must be selected in the **Agent assistant preference** menu:



During an ACD incoming call, if Automatic file pop-up is enabled at the Agent Assistant level, the system will access the preconfigured access database. The database is available in dam.mdb.

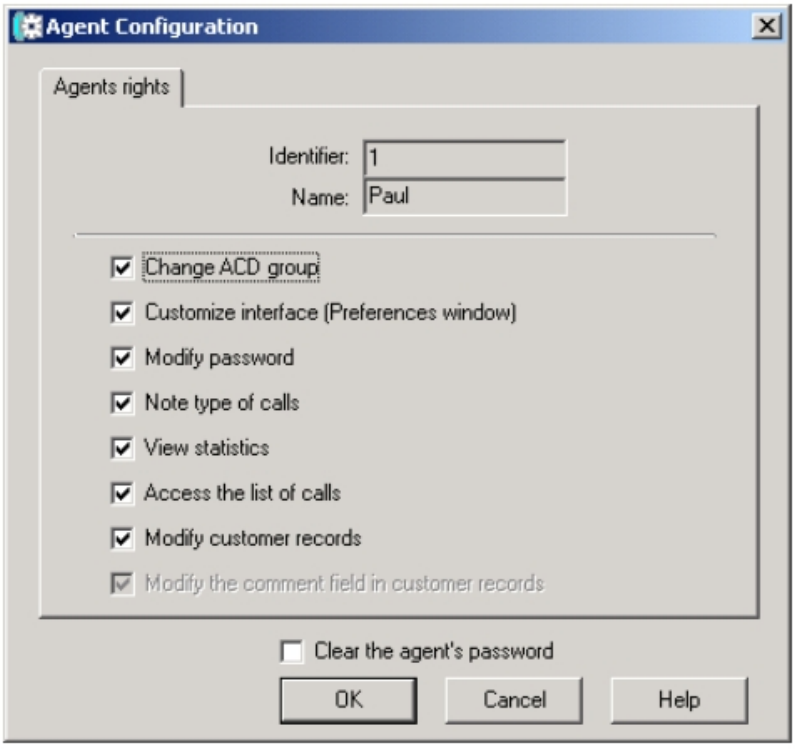
During the file pop-up to the agent assistant application, the system checks the database path defined in the following file available in dam.ini.

The database path is under "[database]" parameter: [database] PATH_database=

If nothing is specified, the repertory with the agent assistant remains. It is therefore easy to modify the database path. If the database is located under C: (C:\dam.mdb), specify the new path in the "damn.ini" file: PATH-database=c:\dam.mdb.

The database is automatically upgraded and the response time depends on the memory available at the PC level.

The customer file may be modified (partially or completely) to allow rights to the agent via **Agent configuration/Agents/properties**. The **Agent rights** window opens:



a- The **Modify customer records** field allows the modification for all the fields.

b- The **Modify the comment field in customer records** field allows the modification for the comment field only. It is only available when the **Modify customer records** field is disabled.

Integrated mode with HTML format

The HTML file pop-up allows the same access integrated database than the standard file pop-up. The only difference is that the HTML format is used to display the file.

The file can be selected manually via the standard format using the manual file pop-up available in the Agent Assistant tool bar or automatically via the HTML format. To set up the automatic HTML file pop-up, it is necessary to enable the HTML screen in the **Agent Assistant/Preferences** menu. Once the HTML file is extracted, it is not possible to modify any other field. The file can only be modified via the standard format.

Integrated mode in network (shared database)

To share the database between several agents and PCs on the same network (LAN), it is necessary to install it on a server. To do so, it is for example possible to use the OmniPCX Office file server function (Premium solution only). The database will automatically be updated according to the network capacities and the memory available on each PC. All the agents can access the same database.

Remark:

If 2 agents access simultaneously the same customer file and modify the file, only the modifications made by the first agent closing the file will be saved. When the second agent closes the same file, the system offers 2 possible choices:

- *Recording the file, saving the modifications and erasing the modifications made by the previous agent.*
- *Recording the file without saving the modifications (the modifications made by the previous agent are displayed and saved).*

Linked mode

The Agent Assistant can be interconnected with message or contact management software such as Microsoft Outlook.

Connected mode allows execution of a script (Windows Scripting Host) when the call is received and access to the database. The application is supplied with a default script file which can be changed by the call centre manager. This operating mode is usually used to access a customer database in Outlook.

If the administrator chooses to use Outlook messaging, the Outlook contact record will appear when a call is received. To make this interoperational system possible, the application activates the "script" to run Outlook by sending it the necessary parameters (caller number).

Using the same procedure as in integrated mode, the contact database is directly accessible from the Agent Assistant.

Linked mode in local

Outlook 2000 must be installed on the client PC. A predefined script is integrated to the Agent Assistant application to refer to Outlook 2000.

During an ACD incoming call to the agent, an Outlook contact will be automatically opened for the agent to enter and record the information about the customer. The information is automatically stored in the Outlook Contact directory.

Linked mode in network (shared database)

The only way to share Outlook Contacts is to create a public contact directory. The administrator must install a Microsoft Exchange server compatible with Outlook 2000 and shared Outlook public contact databases. All the agents must have Outlook 2000 and a specific account (login) to access the Microsoft Exchange server and the public directory. It is also compulsory to modify the Script.vbs file in order to reference it to the database.

Specific mode

This mode is used to provide interconnection between the Agent Assistant and a third-party application. This is useful as many companies use their own Customer Relations Management software.

To connect the Agent Assistant to another customer application, the call centre manager specifies with the agent configuration application, an application which will be called by the Agent Assistant when an ACD call is received. When a call is assigned to an agent, the associated Agent Assistant executes the command line entered in this section, followed by two parameters specific to the call, the caller number and the number called.

The syntax is as follows:

program [option] /1:caller_number /2:called_number

By default, by way of example, "program [option]" is "Wscript.exe post_it.vbs"

Example 1: post_it (available by default)

By default, the Wscript.exe post_it.vbs example will be used. The file Post_it.vbs is available under C:/Program files/alcatel/agent_assistant/....

When an ACD call is assigned to the Agent Assistant application, the 2 following parameters are delivered:

- Argument 1: /1/XXX>Calling phone number (CLI)
- Argument 2: /2/XXX>Called phone number (SDA).
  The execution of Post_it.vbs generates an Outlook note including the date, time, CII and DDI information. This memo is stored in the Outlook note directory.

Example 2: DemoH.exe

This example explains what can be done using a "shared secretaries management". Several DDI numbers are used for the same OmniPCX Office to contact several secretaries. Each DDI ACD corresponds to a specific doctor. Any agent or secretary answering the call must know which doctor is requested to give the corresponding greeting.

The file pop-up is used to inform the agent about the called party. A specific pop-up window provides the information to the agent. According to the parameters sent by the Agent Assistant application during the incoming ACD call presentation, the window displays the caller and the called names.

Conclusion

It is possible to develop many solutions such as executing scripts or developing programs and managing the parameters sent by the agent assistant application.

The databases can be used and located on a LAN server.

10.5.1.2.4 File pop-up with PIMphony

PIMphony may also be used for the file pop-up feature. It supports the following contact managers:

- Microsoft Outlook.
- Act! (Sage Contact from Sage group).
- Goldmine from Sage group.
- Microsoft Access.

10.5.1.2.5 SETTING PREFERENCE PARAMETERS

Preferences allow agents to set the parameters of their working environment. They can:

- Select the language used in the Agent Assistant.
- Define whether the customer information screen pops up automatically on the call centre or is activated by the agent.
- Leave the application always visible in relation to the other applications open on the PC.
- Make the application appear in front of all applications already open.
- Place the phone set on duty when the application is launched.
- Reset the counters on leaving the application or whenever required.
- Disconnect on leaving the application.
  This parameter is used in free seating scenarios when agents disconnect to leave the application; this allows them to register their presence on another computer. If they are not disconnected on leaving the application, a message informs them that they are not

disconnected when they identify themselves on another workstation.

- Select the information screen type: HTML or standard (on the call centre).
- Select the graphs to be displayed.
- Reset their counters.

10.6 Agent Configuration

10.6.1 Overview

The configuration application allows the call center manager to set the parameters of the agent application.

10.6.1.1 STARTING THE APPLICATION

To access configuration of the agent application, a **Login** window allows the call center manager to authenticate him/herself. A password is necessary to establish the connection. The default password is help1954.

10.6.1.2 CONFIGURATION OF THE AGENT APPLICATION

The call center manager has a password-protected configuration module which is used to change the different agent application options and assign rights to agents. The configuration menu has three tabs:

- **General**: used to define preference parameters.
- **Colors**: used to define the colors used in the display of graphs and counters.
- **Agents**: used to list all agents.

10.6.1.2.1 GENERAL TAB

The general parameters can be divided into three groups:

- **Supervisor**
  The call center manager specifies the language he/she wants to use in the configuration module and customer information screen manager.
- **Agent**
  List: the call center manager enters the number of days of data which must be saved in the list of calls. Each agent has a list in which he/she can consult the latest calls. This list is never deleted (value "0") or is deleted on a cyclical basis. This parameter is the same for all agents.
  Activity rate: the call center manager enters the values of the activity rates to be displayed on agent PCs. These parameters are the same for all agents.
- **Customer database**
  The call center manager enters the mode used to connect to the customer database, this mode being identical for all agents. The three available modes are:
  - Integrated mode (standard),
  - Connected mode (script),
  - Specific mode.

  For more information on these modes, refer to the section on "Customer information screen extraction function" in this chapter.

10.6.1.2.2 COLORS TAB

The administrator can change the colors of all the graphs made available to agents.

10.6.1.2.3 AGENT TAB

By default, the agent application manages 32 ACD agents. Each agent is located by his/her identifier and name. These parameters can only be changed by the call center manager using the call center configuration module.

To change **Agent Rights**, select the ACD agent to be changed and click the **Properties** button.

Agent Rights

This window shows all the agents declared in the call center configuration module.

Double-click on the agent or click **Properties** to display the agent's window and confirm or disable the associated right:

- **Change ACD Group**: this right makes the **Group** button visible on the toolbar, allowing agents to change the groups they belong to.
- **Customize Interface** (Preferences window): this right makes the **Preferences** button visible on the toolbar, allowing agents to select their own parameters.
- **Change Password**: this right allows agents to change their own connection password when the application is launched.
- **Define Call Types**: this right makes the drop-down call type menu visible in the call information bar.
- **Display Statistics**: this right makes the **Statistics** button visible on the toolbar, allowing agents to view different types of statistical data.
- **Access Call List**: this right makes the **Calls List** button visible on the toolbar, allowing agents to access their list of calls.
- **Change Customer Information Screens**: this right is only used in integrated mode (standard). Agents can access the screens in the customer database, in read or write mode. If this right is unchecked, the agent can still consult the customer database and use screen pop-ups.
- **Change the Comment Field in Customer Information Screens**: this right is only used in **Integrated Mode** (standard). Agents can access the information screens in the customer database in read mode only, but they can change the comment field in these screens.
- **Delete Agent Password**: this right allows the call center manager to delete the agent's password.

10.7 Statistic Manager

10.7.1 Overview

The call server keeps a database of daily statistics on groups, agents, lines (also called ACD ports) and calls over a period of 14 months. The statistics application is used to access this information and present it in the form of tables and/or graphs.

This application is typically used by the person or people in charge of the call centre (for example, the supervisor(s)).

10.7.1.1 OPENING THE STATISTICS APPLICATION

Open the **Statistic Manager** application in your programme manager. The **Statistic Manager** window is displayed.

The functions available in this window are:

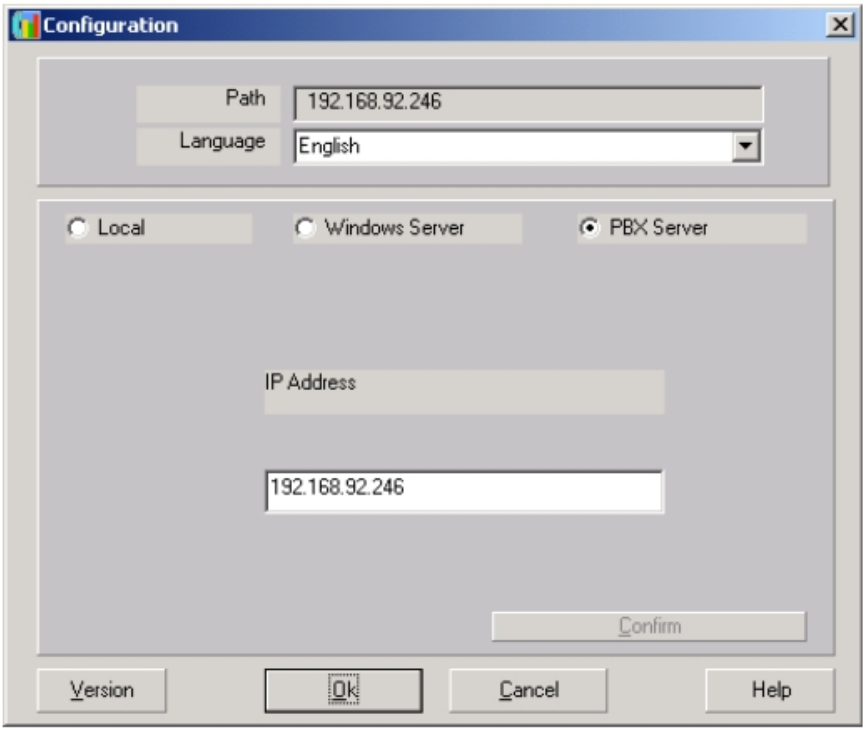
- **Configuration**: used to configure the **Statistic Manager** application.
- **A.C.D.**: used to access the statistics of groups or agents and to automatically print them.
- **Line Statistics**: used to check the sizing of the call centre.
- **Call Statistics**: used to access the statistics on calls.
- **Export**: used to export the statistics files using the binary format for use in local mode and the .csv format for an independent use.
- Click on the open door icon to leave the application.

10.7.2 Configuration

The application can be configured to define the language required and provide information on the system used (server and IP address).

In the **Statistic Manager** window, click the **Configuration** icon: 

1. The configuration window appears.



2. In the upper part, select a language for the application.
3. In the lower part, select:
   - **PBX Server (Call Server Service)** when using the statistics application for the first time and enter the IP address of the system in the field **IP Address**.
   - **Local** when using the application for the second and subsequent times and after repatriation of the system statistics. The statistics application operates locally and the repatriated statistics are stored in the local directory.

     Remark 1:
     it is possible to produce statistics locally without being connected to the system.
   - **Windows Server**: if it exists, a server outside the system.

     Remark 2:
     this option is not used.
4. Click the **Version** button to display the copyright window of the application.
5. Click **Confirm** apply your choices.
6. Click **OK** to exit the screen.

Remark 3:
When connecting to a call server, the statistics files are repatriated to a folder named from the MAC address of PBX

10.7.2.1 Remote access statistics

To execute remote access statistics, use the following procedure:

1. Open a OMC connection on the remote server.
2. Launch the Statistic Manager from OMC using the ACD Statistic Manager link under Automatic Call Distribution.
3. Run the statistics (wait several minutes).

10.7.3 Line Statistics

The line busy rate is the time for which line(s) is(are) busy in relation to the maximum busy time possible. The value is expressed as a percentage.

Note:
information on lines (also called ACD ports) shows how the internal resources of the call center are being used.

The busy rate can be calculated using the following criteria:

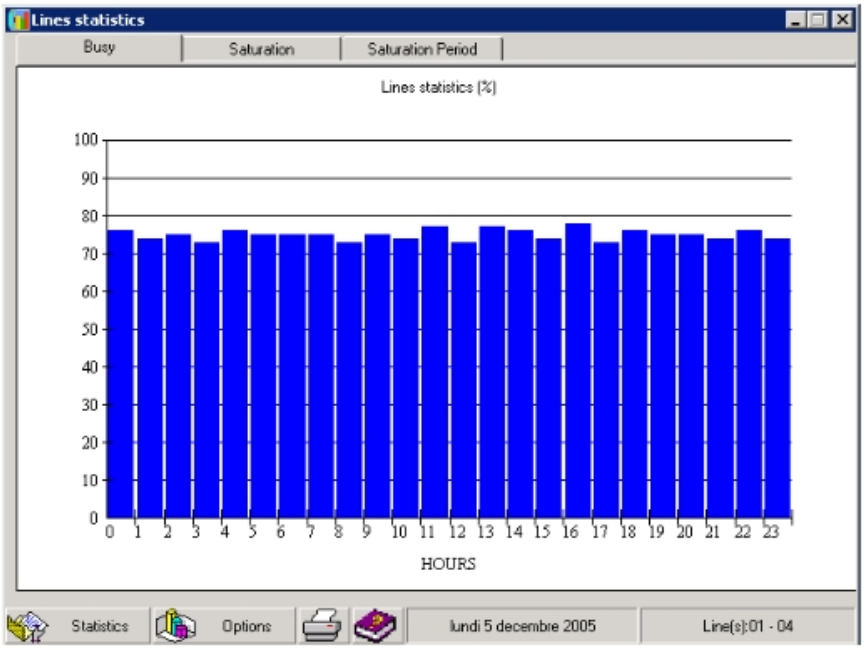
- **Day**: the calculation is performed for 1/2 hour or hour slots with statistics produced over 24 hours or over a given time slot.
- **Period**: the calculation is performed for a 24-hour time period over several consecutive days.
- **Month**: the calculation is performed for a 24-hour time period.
- **Lines**: line by line or for several lines.

To access the line statistics window, do the following:

Open the **Statistic Manager** application. The **Statistic Manager** window is displayed.

To open the **Line Statistics** option, click the icon: 

The following window opens:



10.7.3.1 DEFINING THE PARAMETERS OF LINE STATISTICS

The window includes the tabs **Busy**, **Saturation** and **Saturation Period** that are used to select the elements you want statistics on. The **Statistics**, **Options** and **Print** buttons at the bottom of the screen are respectively used to display options on how often statistics are printed, how they are displayed, and printing of the statistical information selected. These options are displayed to the right of the tab you are in currently.

1. Click the **Busy** tab. This tab is used to display a graphical representation of the line busy rate.
   a. Click the **Statistics** button to display the window for selecting line statistics.
      i. In the **Lines** area, select the line(s) to be observed by clicking in the corresponding boxes.
      ii. In the **Statistics** area, select the frequency with which the statistics are printed. The available choices are:

      • **daily**:
      Select a day from the drop-down menu. The selected day appears in the list to the left of the window.
      Select **Full Day** or define the time slot that you want statistics on, and select whether they are presented every hour or half-hour.

      • **period**:
      Select the start day and end day of the period. The selected days in this period are displayed in the list to the left of the window. You can delete a day from this list by double-clicking on it.

      • **monthly**:
      Select a month from the drop-down menu. The days considered in this month are displayed in the list to the left of the window. You can delete a day from this list by

double-clicking on it.

Remark 1:
*for all these choices, it is possible to select the time slot over 24 hours or over a value defined in the drop-down menus of the option **Between**.*

iii. Click **OK** to confirm your choices or **Apply**.

b. Click the **Options** button to choose how the graphs are displayed (colors, shapes and gridlines) and to define the type of statistics. A window appears in the right-hand part of the screen.

c. Click the **Print** button to open a print options window and start printing the screen.

2. Click the **Saturation Period** tab. This tab is used to display a graphical representation of the line saturation rate.

a. Click the **Statistics** button to display the window for selecting line statistics.

b. Click the **Print** button to open a print options window and start printing the screen.

Remark 2:
*the **Options** button cannot be accessed in the **Saturation Period** tab.*

10.7.3.2 SATURATION RATE

To access the saturation rate, click the **Saturation** tab.

The saturation rate is calculated for a given day; it is therefore possible to select only the daily statistics mode. The statistics modes **Period** and **Monthly** cannot be used to display the saturation rate.

The information is displayed over the 60 minutes following the time selected. The busy rate of the line or lines is expressed as a percentage.

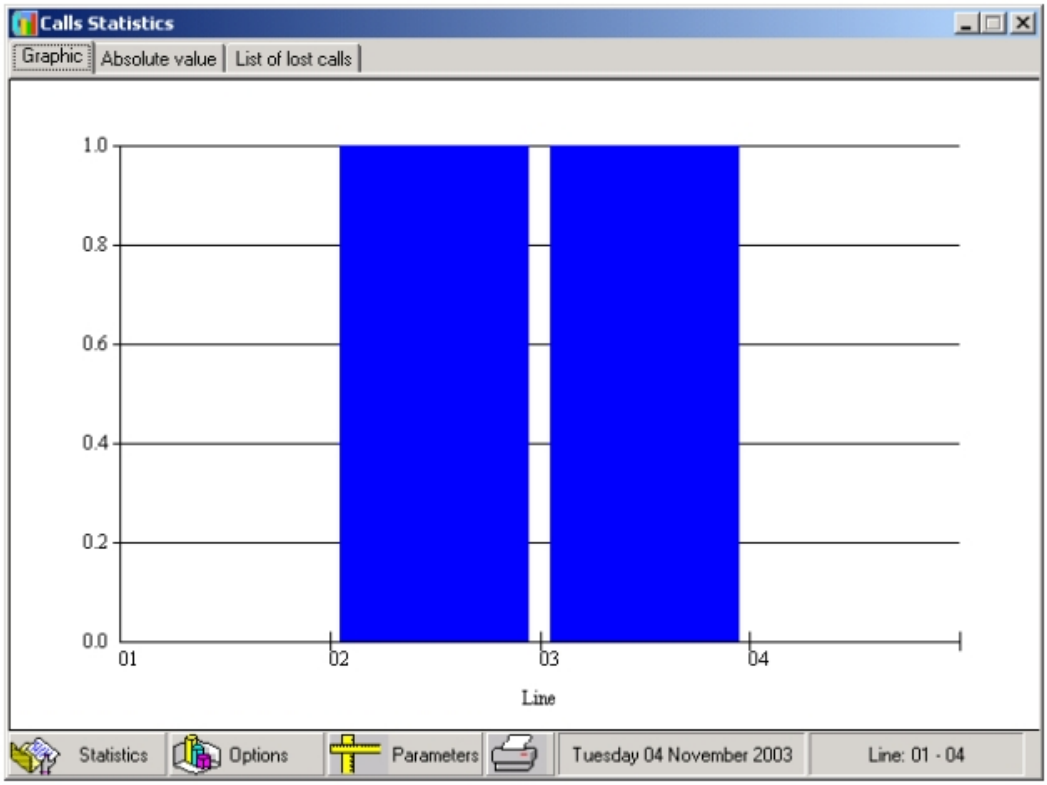
The saturation represented by the value 100% corresponds to a time at which the line or lines cannot handle other calls.

10.7.4 Detailed description

The **Call Statistics** option provides information on the traffic coming into the call centre.

To open the **Call Statistics** option, click the **Call Statistics** icon: 

The following window opens:



10.7.4.1 DEFINING THE PARAMETERS OF CALL STATISTICS

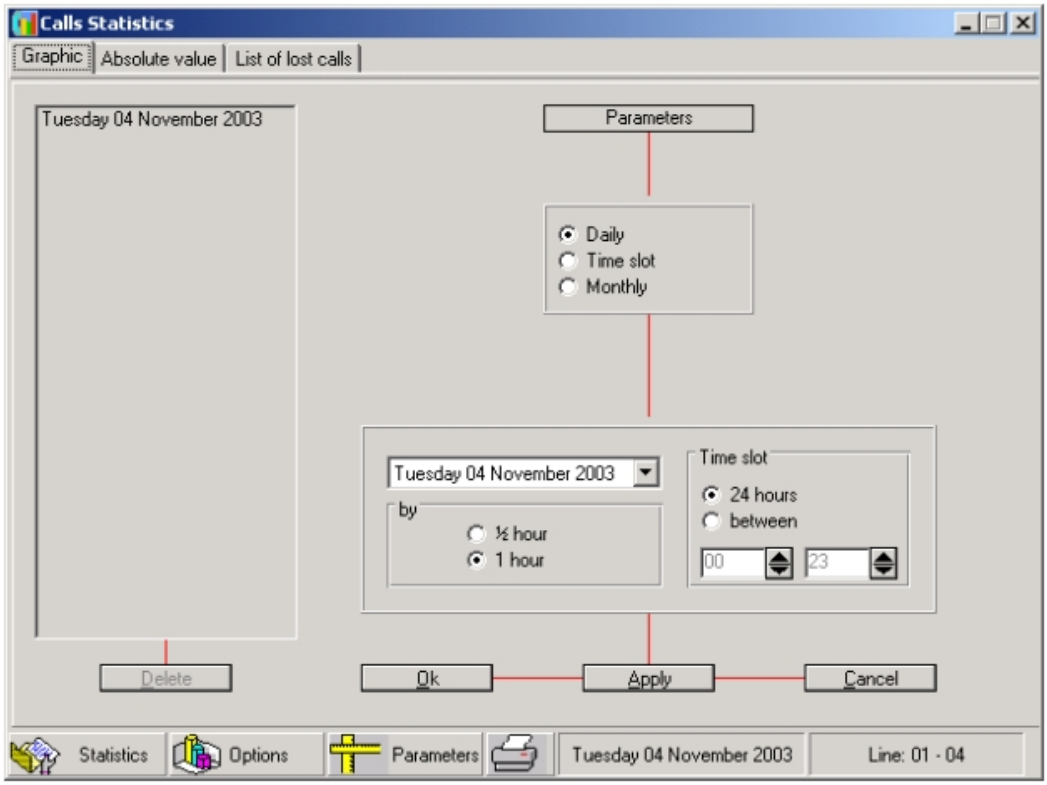
The window includes the tabs **Graphic**, **Absolute Value** and **List of Lost Calls** which are used to select the elements you want statistics on. The **Statistics**, **Options**, **Parameters** and **Print** buttons at the bottom of the screen are used to display various options. These options are displayed to the right of the tab you are in.

The **Graphic** tab is used to display the call statistics. Click the **Options** button to select:

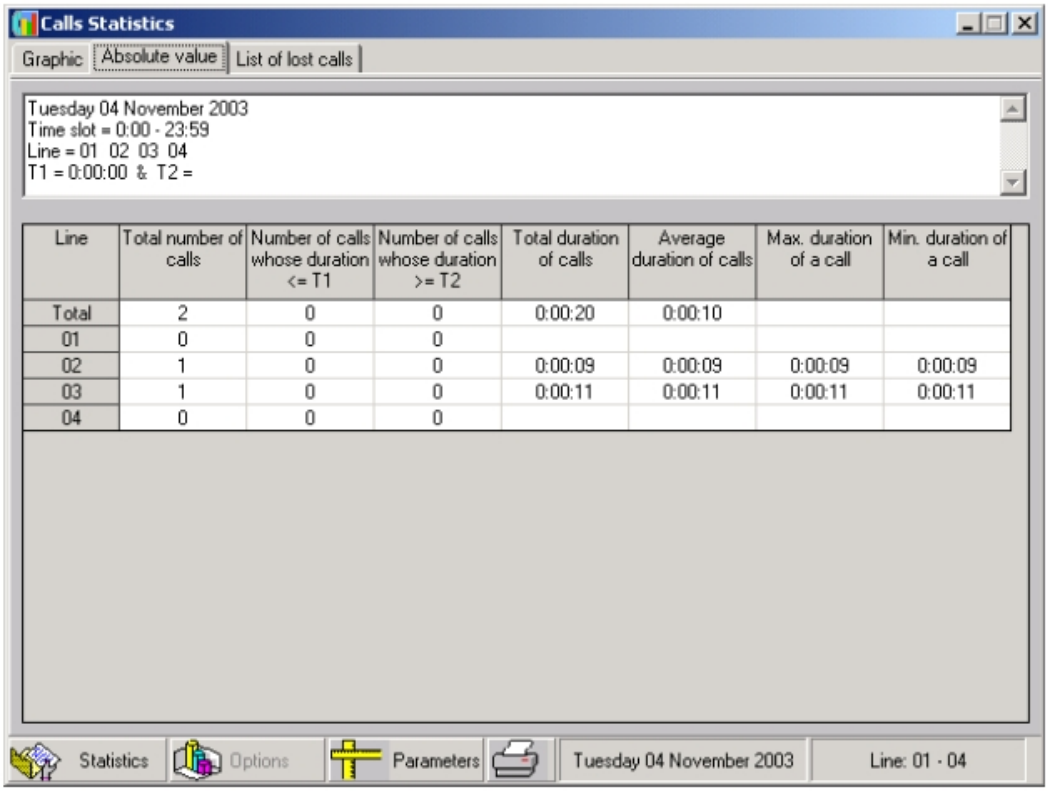
- **Appearance**: select the colour of the graph (Colour, Pastel or Greyed).
- **With lines**: select the type of gridline for the graphs (None, Horizontal, Vertical, Both).
- **Graph**: choose the type of graph by selecting: 2D Pie, 3D Pie, 2D Bar or 3D Bar.
- **Option**: select the type of calls that you want to see displayed. This information will be displayed in the **Absolute Value** tab.

To confirm the selection, click **OK**.

You can request statistics over a day, a period of several days or a month. To do this, click the **Statistics** button at the bottom of the screen. Select the period, full day or time slot of a day and select whether the statistics are presented every half-hour or hour.



The **Absolute Value** tab allows you to obtain information on the lines (as an absolute value).



Line	Total number of calls	Number of calls whose duration <= T1	Number of calls whose duration >= T2	Total duration of calls	Average duration of calls	Max. duration of a call	Min. duration of a call
Total	2	0	0	0:00:20	0:00:10		
01	0	0	0				
02	1	0	0	0:00:09	0:00:09	0:00:09	0:00:09
03	1	0	0	0:00:11	0:00:11	0:00:11	0:00:11
04	0	0	0				

Information is provided on the following:

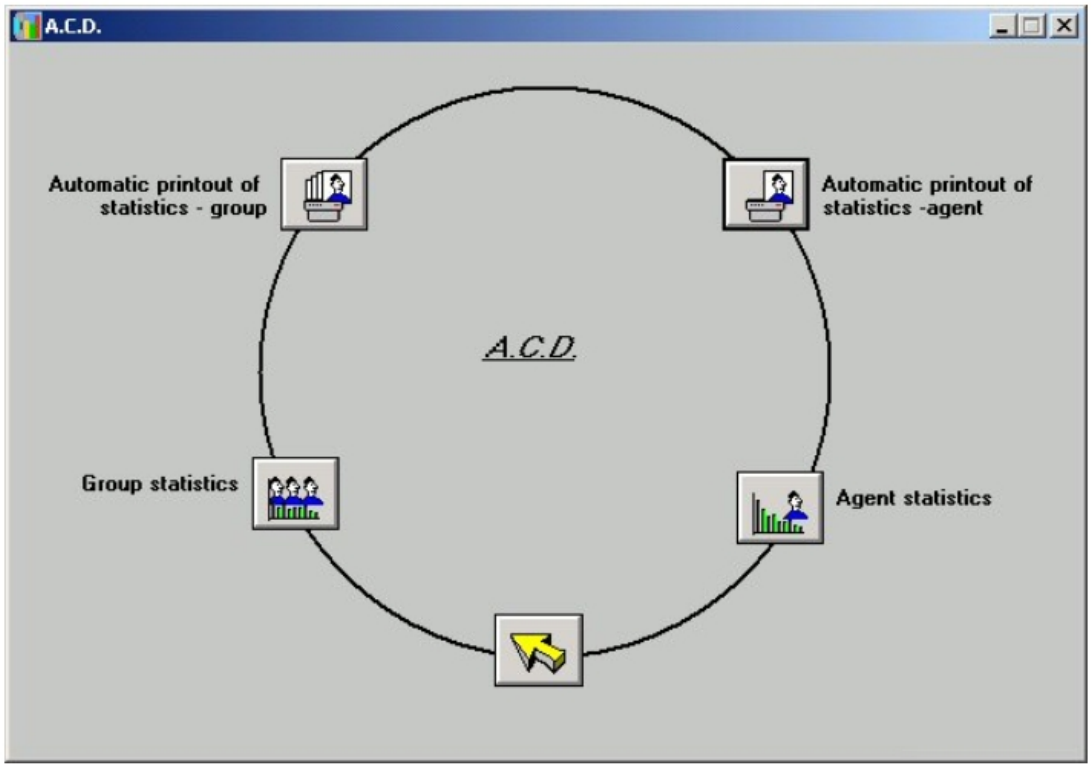
- Total number of calls.
- Number of calls which are shorter than T1; this parameter is defined by the manager.
- Number of calls which are longer than T2; this parameter is defined by the manager.
- Total call time.
- Average call time = total call time / total number of calls.
- Maximum time of a call.
- Minimum time of a call.

The **List of Lost Calls** tab provides information on lost calls.

10.7.5 ACD Statistics

In the **Statistic Manager** window, click the **ACD** icon: 

The following window opens:

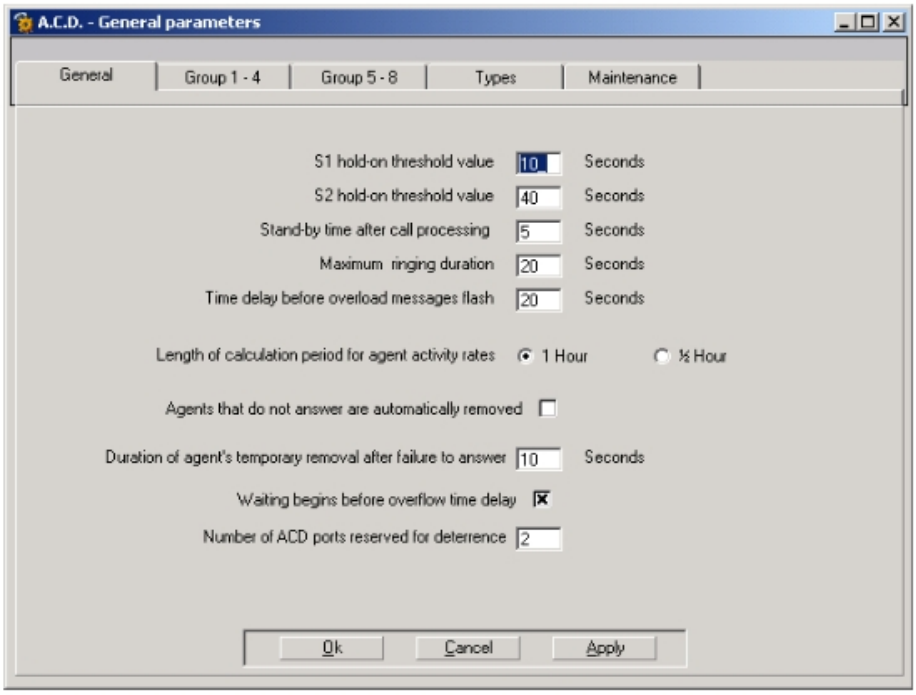


The **A.C.D.** window contains the following icons:

- **Group Statistics**, for obtaining statistics on groups.
- **Agent Statistics**, for obtaining statistics on agents.
- **Automatic Printing of Group Statistics**.
- **Automatic Printing of Agent Statistics.**
- **Arrow**, for closing the window

10.7.5.1 DEFINING THE PARAMETERS OF GROUP STATISTICS

The statistics parameters are defined using the menu **OMC / Automatic Call Distribution / ACD Services/ General Parameters / General**.



When configuring the general parameters of the call center, you have the option of checking or unchecking the box **Waiting Begins Before Overflow Time Delay**.

If the box is checked:

- The **Waiting Time** counter is incremented as soon as a call enters the queue and therefore groups all waiting calls together.
- The **Calls in Queue > S1** counter is incremented for all calls answered which have stayed in the queue for longer than period S1.
- The **Calls in Queue** > S2 counter is incremented for all calls answered which have stayed in the queue for longer than period S2.

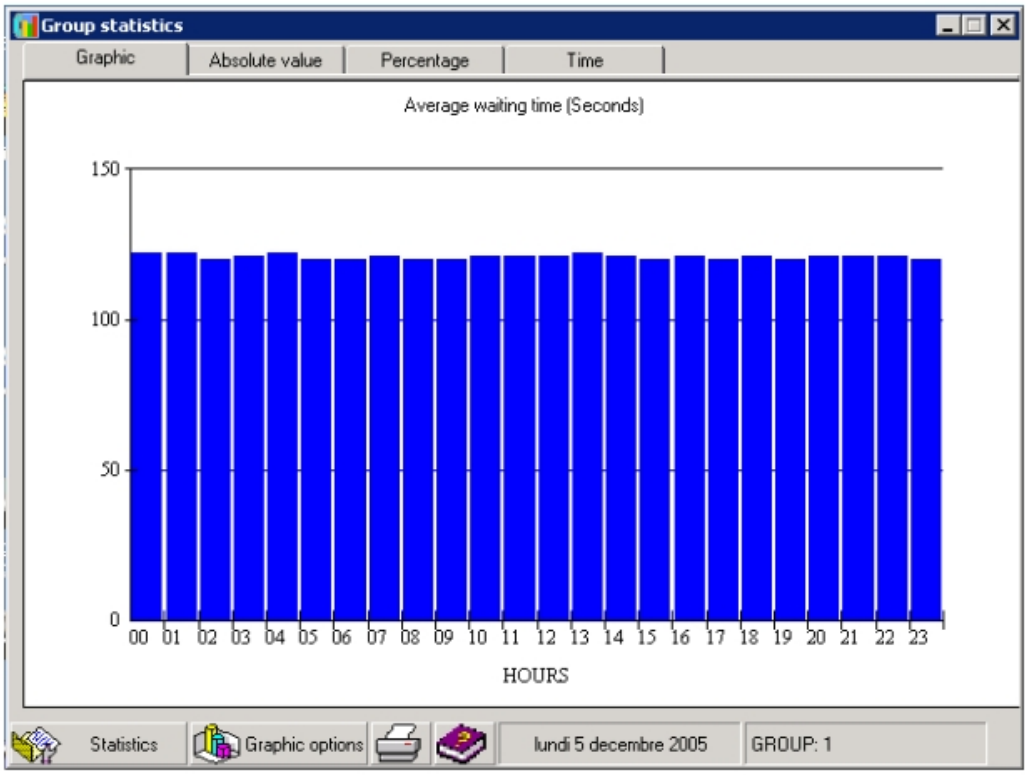
If the box is not checked:

- The **Waiting Time** counter only groups together those calls placed in the queue after overflow to another group has been implemented. It is possible to set the parameters of an overflow time delay independently for each of the groups 1-4 and 5-8 in the **Overflow Grouping** field.
- The **Calls in Queue** > S1 counter is incremented for all calls answered which have stayed in the queue for longer than (S1+ overflow time delay).
- The **Calls in Queue** > S2 counter is incremented for all calls answered which have stayed in the queue for longer than (S2+ overflow time delay).

10.7.5.2 GROUP STATISTICS

10.7.5.2.1 Overview

The group statistics window appears.



The window includes the tabs **Graphic**, **Absolute Value**, **Percentage** and **Time** which are used to select the elements you want statistics on. The **Statistics**, **Graphic options** and **Printing** buttons at the bottom of the screen are respectively used to display options on how often statistics are printed, how they are displayed, and printing of the statistical information selected. These options are displayed to the right of the tab you are in.

1. Click **Statistics** to:
   - Select the group for which you want statistics in the **Group** area.
   - Choose the period for which information will be displayed, in the **Statistics** area. The following periods can be defined:
     - **daily**: select a day from the drop-down menu. The selected day appears in the list to the left of the window. Select **Full Day** per 1 hour or 1/2 hour or define a time slot.
     - **period**: select the start day and end day of the period. The selected days in this period are displayed in the list to the left of the window.

       Remark 1:
       you can delete a day by double-clicking on it.

- **monthly**: select a month from the drop-down menu. The days considered in this month are displayed in the list to the left of the window.

  Remark 2:
  you can delete a day by double-clicking on it.
  The time slot is only accessible in the **Daily** mode.
  Click **Apply** to apply the changes without closing the window, **OK** to close the window and apply the changes, or **Cancel** to close the window without implementing the changes.

2. Click **Graphic options** to define the format the graphs are displayed in.
3. Click the **Printing** icon to select the print options and start printing the screen.

10.7.5.2.2 STATISTICS AS A PERCENTAGE OR AS AN ABSOLUTE VALUE

Click the **Absolute Value** tab or the **Percentage** tab.

Selecting elements to produce statistics

You can request statistics on the following elements:

- **Incoming Calls**: total number of calls arriving in the call distribution chain.
- **Calls Answered**: number of ACD calls transferred to an agent and connected, regardless of the group (called or through overflow).
- **Calls Waiting**
  - **Calls in Queue**: number of calls placed in the queue before being answered (connected to the customer), with:
    Calls in Queue > S1: number of calls for which the wait period is longer than threshold S1*. This counter is a subset of the "Calls in Queue" counter.
    Calls in Queue > S2: number of calls for which the wait period is longer than threshold S2*. This counter is a subset of the "Calls in Queue > S1" counter.
    * S1 and S2 are two threshold values which can be defined in OMC/ACD Service/General Parameters/General tab.
- **Calls Deterred**: number of calls routed to the deterrence announcement following saturation of the queue, or if no agent is defined for a given group.
- **Calls Abandoned**: number of calls which have left the ACD; the caller hangs up before being connected to an agent, regardless of the routing phase of the call.
- **Calls Service Closed**: number of calls while the group is closed.
- **Calls Overflow**: number of calls answered by an agent belonging to the group taking the overflow from the group requested. This counter is a subset of the **Calls Answered** counter.

Summary

Number of calls Waiting for **less than S1**= (Number of calls **Waiting**) - (Number of calls in **Queue > S1**)

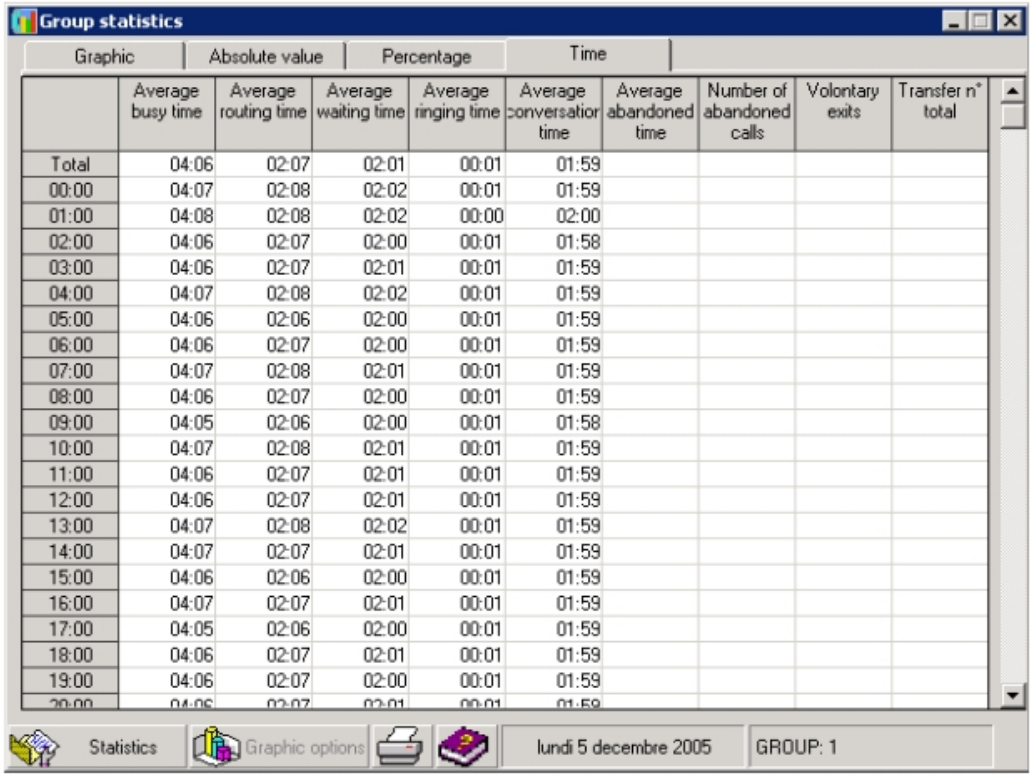
Number of calls Waiting **between S1 and S2**= (Number of calls in **Queue > S1**) - (Number of calls in **Queue > S2**)

Remark:

all the percentages in the table are calculated in relation to incoming calls.

10.7.5.2.3 TIME STATISTICS

In the **Group Statistics** window, click the **Time** tab.



	Average busy time	Average routing time	Average waiting time	Average ringing time	Average conversation time	Average abandoned time	Number of abandoned calls	Volontary exits	Transfer n° total
Total	04:06	02:07	02:01	00:01	01:59				
00:00	04:07	02:08	02:02	00:01	01:59				
01:00	04:08	02:08	02:02	00:00	02:00				
02:00	04:06	02:07	02:00	00:01	01:58				
03:00	04:06	02:07	02:01	00:01	01:59				
04:00	04:07	02:08	02:02	00:01	01:59				
05:00	04:06	02:06	02:00	00:01	01:59				
06:00	04:06	02:07	02:00	00:01	01:59				
07:00	04:07	02:08	02:01	00:01	01:59				
08:00	04:06	02:07	02:00	00:01	01:59				
09:00	04:05	02:06	02:00	00:01	01:58				
10:00	04:07	02:08	02:01	00:01	01:59				
11:00	04:06	02:07	02:01	00:01	01:59				
12:00	04:06	02:07	02:01	00:01	01:59				
13:00	04:07	02:08	02:02	00:01	01:59				
14:00	04:07	02:07	02:01	00:01	01:59				
15:00	04:06	02:06	02:00	00:01	01:59				
16:00	04:07	02:07	02:01	00:01	01:59				
17:00	04:05	02:06	02:00	00:01	01:59				
18:00	04:06	02:07	02:01	00:01	01:59				
19:00	04:06	02:07	02:00	00:01	01:59				

The following statistics are available as periods of time:

- **Average Busy Time**: total time of calls answered (time measured between the welcome announcement and the end of the call), divided by the number of calls answered.
- **Average Routing Time**: total routing time of calls answered, divided by the number of calls answered. The announcement time is counted in the routing time.
- **Average Waiting Time**: total time of calls in the queue, divided by the number of calls answered which have been waiting.
- **Average Ringing Time**: total ringing time of calls answered, divided by the number of calls answered.
- **Average Conversation Time**: total conversation time of calls answered, divided by the number of calls answered.
- **Average Abandoned Time**: total time of calls in the queue before the caller abandons the call (the caller hangs up before being connected to an agent), divided by the number of abandoned calls.
- **Number of Abandoned Calls**: total time of abandoned calls following a caller hanging up when they were in the queue, or while being transferred after leaving the queue. These

calls have gone through the queue. They are a subset of the counter.

- **Voluntary Exits**: number of calls which have voluntarily left the queue (by pressing the * key) without hanging up, to leave a message in the group mailbox.
- **Total of Transfer Numbers**: number of calls routed to the transfer number (programmed in **OMC / Automatic Call Distribution / ACD Services /General Parameters / Group 1-4 or Group 5-8**) following an abnormal situation (group open with no agents assigned, or call waiting when the last agent has gone off duty from the service, for example). The first call is routed to the transfer number and the following ones to the queue.

Summary

For a given time slot:

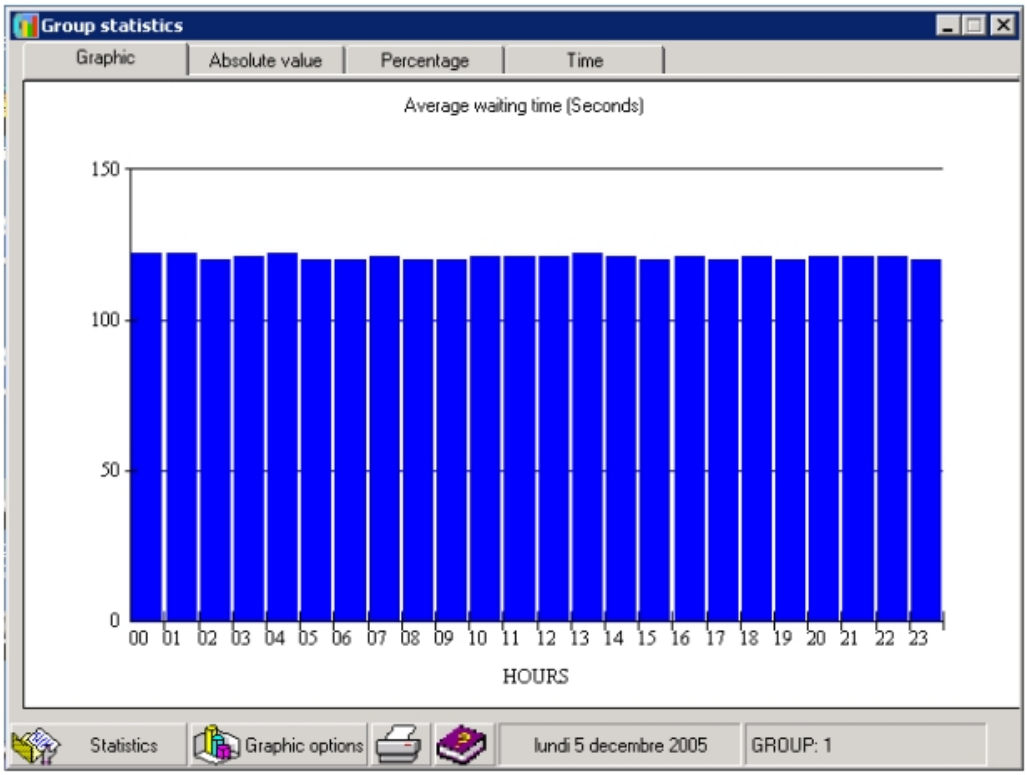
Average busy time = (Average routing time) + (Average conversation time)

Average routing time = (Average waiting time) + (Average ringing time)

Number of incoming calls = (Number of calls **Answered**) + (Number of calls **Abandoned**) + (Number of calls with **Voluntary Exit**) + (Number of calls **Deterred**) + (Number of calls **Closed**) + (Number of calls **Transferred**)

10.7.5.2.4 GRAPHS

In the **Group Statistics** window, click the **Graphic** tab to obtain summary information.



The **Graphic Options** button can be used to choose how the graphs are displayed (colors, shapes and units).

- Choose the graph color by selecting **Color**, **Pastel** or **Grayed** in the upper area.
- Choose the graph type by selecting **2D Pie**, **3D Pie**, **2D Bar** or **3D Bar** in the lower area.
- Choose how the graph is displayed by selecting **Absolute Value** or **Time** in the **Number** area. Depending on the choice made, the window listing statistical information on groups is displayed as an absolute value or in terms of time. Select the elements of your choice and click **OK** to return to the previous window.
- To define what type of call the statistics are produced from, select **Incoming Calls** or **Calls Answered** from the **Synthesis** area.
- The **Incoming Calls** synthesis graph shows the calls answered, deterred, abandoned and closed, for the day and the groups selected.

  Remark:
  incoming calls are selected by default.
- The **Calls Answered** synthesis graph shows the ACD calls (direct, in queue, in queue longer than S1 and in queue longer than S2) answered by an agent, for the day and the groups selected.

Summary

Definition of summaries for incoming calls:

Number of calls **Answered** = (Number of calls **In Queue**) + (Number of calls waiting **Longer than S1**) + (Number of calls waiting **Longer than S2**) + (Number of **Direct** calls)

This synthesis graph shows the calls answered, deterred, abandoned and closed, for the day and the groups selected.

Definition of summaries for calls answered:

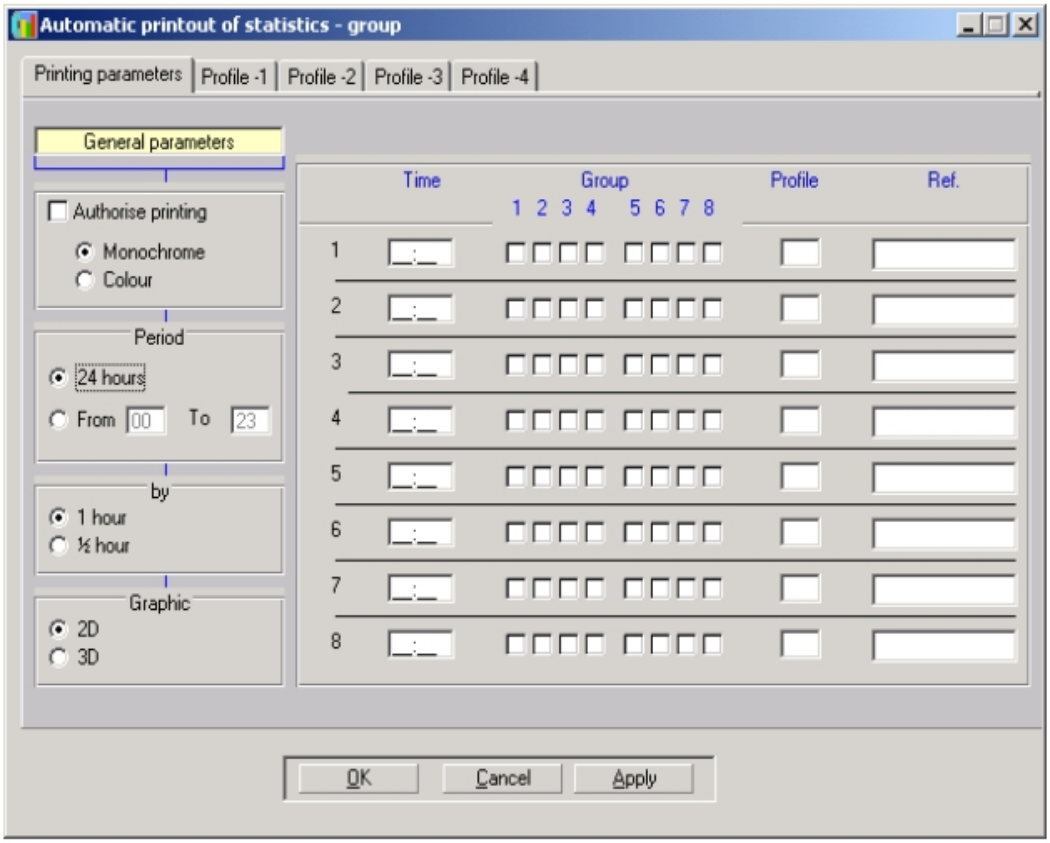
Number of calls **Answered** = (Number of calls **In Queue**) + (Number of calls waiting **Longer than S1**) + (Number of calls waiting **Longer than S2**) + (Number of **Direct** calls)

This synthesis graph shows direct calls, calls in queue, calls in queue longer than S1 and in queue longer than S2, for the day and the groups selected.

10.7.5.3 AUTOMATIC PRINTING GROUP STATISTICS

To access automatic printing options, open the ACD application from the **Statistic Manager** screen. Click the icon **Automatic Statistic Printing - Groups**. 

The following print window is displayed.



You can program automatic printing so that daily statistics are printed at certain times of day for the groups concerned.

1. Click the **Printing parameters** tab to print group statistics at a set time.

   a. *Remark 1:*
   up to 8 printing operations can be programmed per day.

   b. In the **General Parameters** area, define the type of printing (color or monochrome), the time slot, scale and graph type.

      i. In the right-hand area, define:
         - the automatic printing time,
         - the number(s) of the group(s) concerned by the printing operation,
         - the print profile(s) relating to profiles 1, 2, 3 or 4 defined by the supervisor.

      ii. Click **OK** or **Apply** to confirm your choices.

   c. Click the **Profile 1, 2**, **3** or **4** tab to define the print profiles.

   Remark 2:
   the supervisor can print four types of print profile, depending on the analysis required.
   For each profile, select the different statistics screens of the groups that you want to print by checking the corresponding boxes, then click **OK** or **Apply** to confirm your choices.

   d. Click **OK** to confirm.

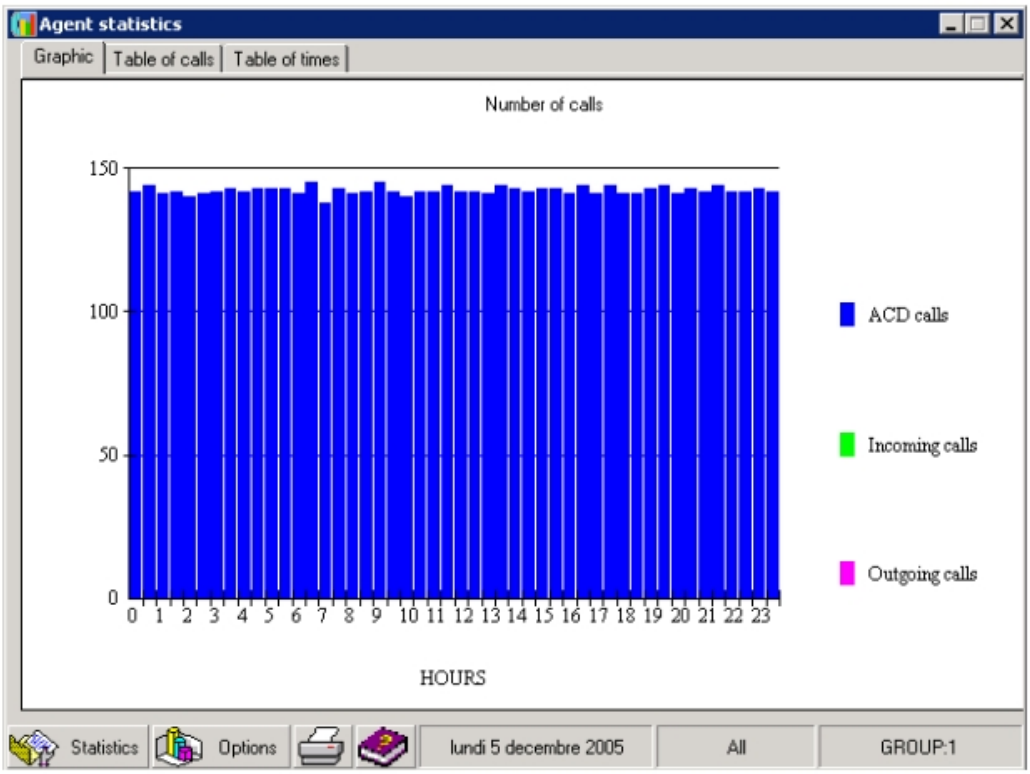
Remark 3:
*statistics can be printed manually from the **Group Statistics** screen.*

10.7.5.4 AGENT STATISTICS

10.7.5.4.1 Overview

To access agent statistics, open the ACD application from the **Statistic Manager** screen and click the **Agent Statistics** icon:

The agent statistics window appears.



The **Agent Statistics** window includes the tabs **Graphic, Table of Calls**, **Table of Times** and **Time** which are used to select the elements you want statistics on. The **Statistics**, **Options** and **Print** buttons at the bottom of the screen are respectively used to display options on how often statistics are printed, how they are displayed, and printing of the statistical information selected. These options are displayed to the right of the tab you are in.

10.7.5.4.2 Description of options

1. Click the **Table of Calls** tab. This tab shows statistical information on calls as an absolute value, in the form of a table.
   a. Click the **Statistics** button to display the window for selecting agent statistics.
      - **Agent**: used to select the number of the agent to be included in the statistics or to select all agents (**All** option).
      - **Group**: used to select the group(s) which the agent belongs to; check groups **1** to **8**.
      - **Statistics**: used to select the display period (**Daily**, **Period** or **Monthly**).
      - Click **Apply** to apply the changes without closing the window, **OK** to close the window and apply the changes, or **Cancel** to close the window without implementing the changes.

   b. Click the **Options** button.
      - **General**: select to display all calls.
      - **Call Number/Type**: used to display calls according to their type.

      The table is automatically updated after this selection.
2. Click the **Table of Times** tab. This tab shows statistical information on calls as a time value, in the form of a table.
   a. Click the **Statistics** button to display the window for selecting agent time statistics.
   b. Click the **Options** button to define the parameters of the type of information required.
   c. Select
      - **General** to display the time of all calls,
      - **Total Time/Type** to display the total time of calls according to their type,
      - **Average Time/Type** to display the average time of calls according to their type.

      The table is automatically updated as soon as one of these 3 options is selected.
3. Click the **Graphic** tab. This tab is used to view the statistics in the form of a graphic.
   a. Click the **Options** button to access the window allowing you to select how the graphs will be presented.
      i. Choose the graph color by selecting **Color**, **Pastel** or **Grayed** in the upper area.
      ii. Choose the graph type by selecting **2D Pie**, **3D Pie**, **2D Bar** or **3D Bar** in the lower area.
      iii. Choose how the graph is displayed by selecting **Number of Calls/Type** or **Total Time/Type**. Depending on the choice made, the window listing the statistical information produced on the groups in terms of time is displayed. Select the elements of your choice and click **OK** to return to the previous window.
      iv. To define from what type of calls the graph statistics are produced, select **Number of Calls** or **Average Time** or **Total Time** in the **Synthesis** area.
         - The **Number of Calls** synthesis graph shows ACD, "Other", "Incoming" and "Outgoing" calls, for the day, for agents, and their selected groups.
         - The **Average Time** synthesis graph shows ACD conversations, ACD rings and other conversations, for the day, the agent(s) and their selected groups.
         - The **Total Time** synthesis graph shows total ACD conversations, ACD ringing and other conversations, for the day, the agent(s) and their selected groups.
      v. To define graphs related to specific statuses, select **Number of Calls** or **Time** from the **Detail** area.
4. Click the **Print** button to open a screen with the print parameters.

10.7.5.4.3 Table of calls

Click the **Table of Calls** tab. The following call statistics are available:

- **ACD Calls**: number of ACD calls answered by the agent.
- **"Incoming" Calls"**: number of non-ACD calls arriving on the agent's set (external calls (DDI) or internal calls to the set).
- **"Outgoing" calls**: number of non-ACD calls initiated by the agent (internal or external calls and picking up the call).

  Remark 1:
  this is only possible if the protocol allows the information to be obtained; otherwise all "non-ACD" (or "Other") calls are placed in the "Incoming" Calls column.
- **No Answer**: number of calls of ACD origin that the agent does not answer.

  Remark 2:
  there may be several no answers for the same incoming call number.
- **Temporary Absence**: number of times the agent switches to "Temporary Absence" status.
- **Clerical Work**: number of times the agent switches to "Clerical Work" status.
- **On Duty**: number of times the agent comes "on duty".
- **Off Duty**: number of times the agent goes "off duty".

Summary

Synthesis for absolute value statistics

Total number of **Calls** = (number of **ACD** calls) + (number of **Incoming** calls) + (number of **Outgoing** calls)

10.7.5.4.4 Table of times

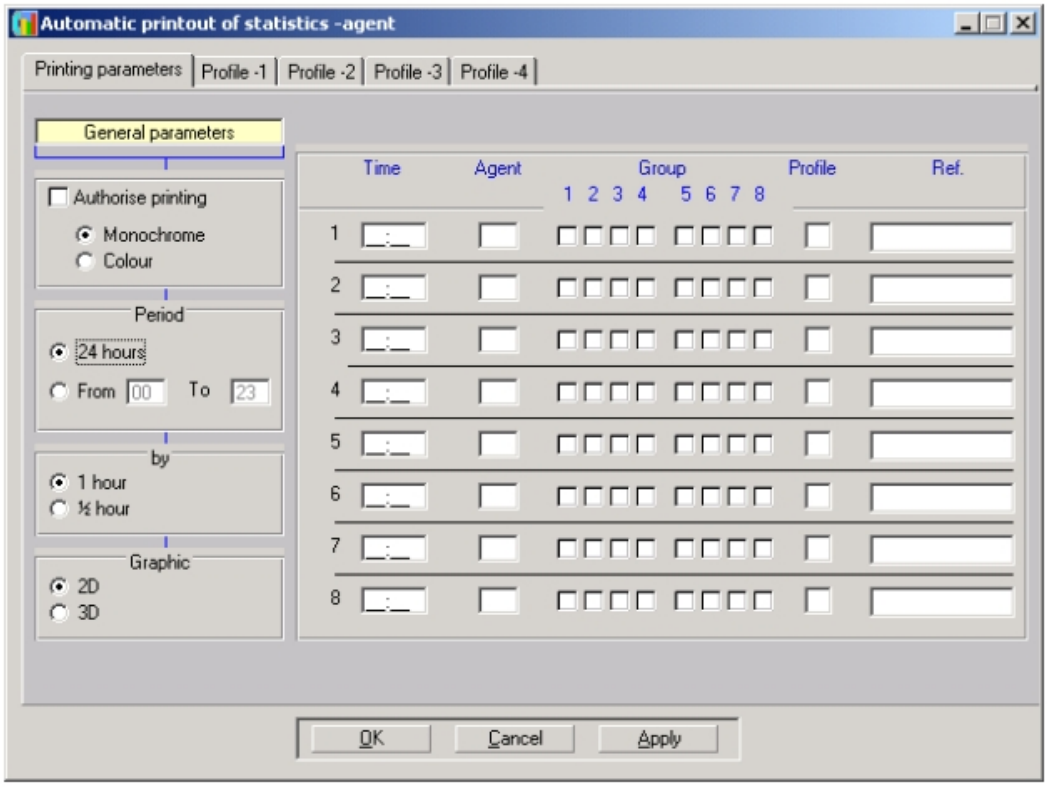
Click the **Table of Times** tab. The following call statistics are available:

- **ACD Com. Average**: total ACD conversation time/number of ACD calls answered by the agent.
- **ACD Ring Average Time**: total ring time of ACD calls arriving on the agent set (ring phase)/number of ACD calls answered by the agent.
- **Other Com. Average Time**: time during which the line of the "agent" set is busy ("Incoming" and "Outgoing") excluding calls originating from the ACD server/number of times this set is busy, excluding ACD calls.
- **Total Fully Busy**: total ringing time of calls from the ACD server + time of ACD conversations + time of Other calls ("Incoming" and "Outgoing").
- **Total ACD Com.**: total conversation time of ACD calls processed by the agent.
- **Total Other Com.**: time during which the line of the "agent" set is busy ("Incoming" and "Outgoing") excluding calls of ACD origin.
- **Total Temporary Absence**: total time the agent spends in "Temporary Absence" status.
- **Total Clerical Work:** : total time the agent spends in "Clerical Work" status.
- **Total On Duty**: total time the agent is connected (on duty).

10.7.5.5 AUTOMATIC PRINTING AGENT STATISTICS

To access automatic printing options, open the ACD application from the **Statistic Manager** screen. Click the icon **Automatic Statistic Printing - Agents**. 

The following print window is displayed.



You can program automatic printing so that the daily statistics are printed at certain times of day for the agents concerned.

1. Click the **Print Parameters** tab to print agent statistics at a set time.

   Remark 1:
   up to 8 printing operations can be programmed per day.

   a. In the **General parameters** area, define the type of printing (color or monochrome), the time slot, scale and graph type.

   b. In the right-hand area, define:

   - the automatic printing time
   - the number(s) of the group(s)
   - the print profile(s) relating to profiles 1, 2, 3 or 4 defined by the supervisor
   - the agent number when printing agent statistics only.

     Remark 2:
     *to select all agents, enter 99 in the **Agent** column.*

c. Click **OK** or **Apply** to confirm your choices.

2. Click the **Profile 1, 2**, **3** or **4** tab to define the print profiles.

   Remark 3:
   the supervisor can print four types of print profile, depending on the analysis required.
   For each profile, select the different statistics screens of the agents that you want to print by checking the corresponding boxes, then click **OK** or **Apply** to confirm your choices.

3. Click **OK** to confirm.

Remark 4:

*statistics can be printed manually from the **Agent Statistics** screen.*

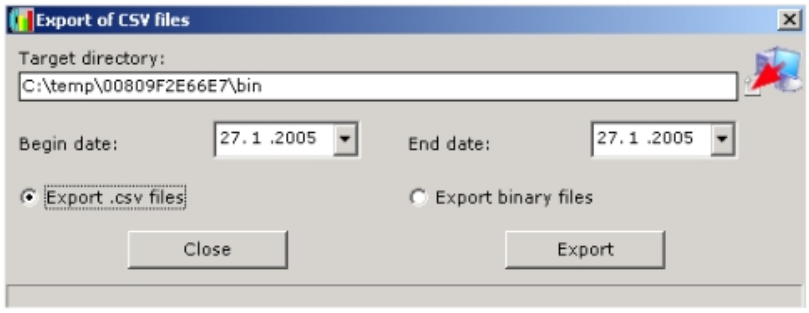
10.7.6 Exporting statistics files

10.7.6.1 PROCEDURE

A specific window is used to export statistics files. This window allows you to define the start and end of the export. It also allows you to specify whether the export is to produce .csv format files for external use or binary files for off-line use with the statistics application.

To access the statistics files export, open the ACD application from the **Statistic Manager** screen and click the **Export statistics files** icon.

The following window opens:



1. Adjust the **Begin date** and **End date** parameters for the export.
2. Select **Export .CSV files** or **Export binary files**.
3. Click **Export**. The export is launched.

10.7.6.2 STATISTICS FILES FORMAT

You can export the statistics files corresponding to a specified time period (there is one file per day), in a specified file format. As soon as it is connected to a system, the statistics application automatically converts files to binary format, but you can manually request the export of statistics files in one of two file formats: CSV format files (for external use) and binary files (for

use by the statistics application in local mode).

The files are transferred to a directory which is specific to the connected system. This directory is created from the MAC address of OmniPCX Office.

When viewing (binary format) files or exporting (binary or CSV format) files, only files not already present in the target directory are transferred.

10.7.6.2.1 Statistics files in .CSV format

Statistics files in the CSV format contain information concerning agents' actions, ACD calls, and calls received on the ACD ports.

Types of ticket

Once a statistics file has been created, these tickets are generated for all logged agents at each change of state of an agent.

Examples:

2004/01/30;10:10:08;F;01;101;S;1;2;3;4; ; ; ; ;

2004/01/30;10:10:08;F;02;102;S;1;2;3;4; ; ; ; ;

2004/01/30;10:10:08;F;03;103;S;1; ; ; ; ; ; ; ;

2004/01/30;10:10:08;F;04;104;S;1;2; ; ; ; ; ; ;

2004/01/30;10:10:08;F;08;108;H;1;2; ; ; ; ; ; ;

2004/01/30;10:10:08;F;09;101;H; ; ; ;4;5;6;7; ;

2004/01/30;10:10:08;F;10;110;H; ; ; ;4;5;6;7; ;

2004/01/30;10:10:08;F;11;111;T;1; ; ; ; ; ; ; ;

2004/01/30;10:10:08;F;12;112;A; ;2; ; ; ; ; ; ;

Explanation of elements:

Element	Format	Description
Element 1	yyyy/mm/dd	Date of ticket
Element 2	hh:mm:ss	Time of ticket
Element 3	F	Letter indicating format of ticket
Element 4	xx	Physical number of agent (from 01 to 32)
Element 5	qmcdu	Telephone number of agent
Element 6	x	Code indicating operation performed: S – Put into service H – Withdrawn from service T – Other task A – Temporary absence G – Change of group
Element 7	x	1 if the agent belongs to group 1
Element 8	x	2 if the agent belongs to group 2
Element 9	x	3 if the agent belongs to group 3
Element 10	x	4 if the agent belongs to group 4

Element 11	x	5 if the agent belongs to group 5
Element 12	x	6 if the agent belongs to group 6
Element 13	x	7 if the agent belongs to group 7
Element 14	x	8 if the agent belongs to group 8

State of agent telephone ticket

These tickets are generated for all logged agents at each change of state of an agent's telephone.

Examples:

2004/01/30;10:10:08;P;01;101;P;

2004/01/30;10:10:08;P;02;102;N;

2004/01/30;10:10:08;P;01;101;D;

Explanation of elements:

Element	Format	Description
Element 1	yyyy/mm/dd	Date of ticket
Element 2	hh:mm:ss	Time of ticket
Element 3	P	Letter indicating format of ticket
Element 4	xx	Physical number of agent (from 01 to 32)
Element 5	qmcdu	Telephone number of agent
Element 6	x	Code indicating operation performed: P – Line is no longer occupied D – Line is available again N – No answer (ACD call) B – Double call F – Call to non-existent number X – Anomaly (telephone not connected)

State of group ticket

These tickets are generated at each change of state of an ACD group.

Examples:

2004/01/30;10:10:08;G;01;a;

2004/01/30;10:10:08;G;02;b;

Explanation of elements:

Element	Format	Description
Element 1	yyyy/mm/dd	Date of ticket
Element 2	hh:mm:ss	Time of ticket
Element 3	G	Letter indicating format of ticket
Element 4	xx	Physical number of agent (from 01 to 08)

Element 5	x	Code indicating type of event: a – Group manually opened b – Automatic group opening/closing selected* c – Group manually closed * According to specified opening/closing times

ACD call ticket

These tickets are generated after every ACD call.

Examples:

2004/04/30;10:15:23;A;3;1;1;01;101;262;32;0;22;230;S;3;0323456789;9876;

2004/04/30;10:15:23;A;3;1;1;01;101;32;0;28;22;0;N; 0;0323456789;9876;

2004/04/30;10:15:23;A; 3; 1; 1; ; ;12;0;0;0;0;D;0;0323456789;9876;

2004/04/30;10:15:23;A; 3; ; ; ; ;0;0;0;0;0;P;0;0323456789;9876;

Explanation of elements:

Element	Format	Description
Element 1	yyyy/mm/dd	Date of ticket
Element 2	hh:mm:ss	Time of ticket
Element 3	A	Letter indicating format of ticket
Element 4	xx	Physical number of route that processed the call (from 01 to 14)
Element 5	xx	Number of requested ACD group (from 01 to 08)
Element 6	xx	Number of allocated ACD group (from 01 to 08)
Element 7	xx	Physical number of last agent called (from 01 to 32)
Element 8	qmcdu	Telephone number of last agent called
Element 9	xxxx	Duration for which ACD function was occupied (from call arrival until call termination by agent or caller).
Element 10	xxx	Duration of call routing (from call arrival until communication with agent began).
Element 11	xxx	Duration of call waiting (time spent in queue).
Element 12	xxx	Duration for which telephone was ringing.
Element 13	xxxx	Duration of conversation (from call answering by agent until call termination by agent or caller).

Element 14	x	Letter indicating the call outcome: S – Call successfully handled D – Call deterred A – Call abandoned F – Call received for closed group (outside group opening hours) f – Call received for closed group (manually closed) R – Call redirected to forwarding number Q – Caller voluntarily left queue (key *) P – Call lost (saturation of incoming call capacity) X – Anomaly (ACD engine not synchronized with PBX, and CSTA event sent)
Element 15	xx	Qualification code for the call (from 00 to 10) provided by the application agent.
Element 16	n	Caller's number.
Element 17	n	Number called.

10.8 Supervisor Console

10.8.1 Overview

The supervisor application is used to view real-time information on call center activity. This information is presented in the form of tables and charts on supervisor PCs.

The supervisor application can be used to perform the following operations:

- Supervise traffic and agent workloads in real-time: real-time display of the number of calls waiting, the number of agents connected, the number of calls deterred, the number of calls lost etc. The queue indicators are of course specific to each team or each group.
- Place agents on duty or take them off duty.
- Oblige an agent to move from one group to another, depending on the call load in the queue, the duration of calls or the workload observed.
- Simultaneously observe:
  - several groups or teams,
  - several call numbers,
  - several queues.

  The supervisor is provided with a tool which can be used to immediately check the status of his/her team. It can be used to see:
  - the number of calls waiting,
  - the number of calls received and processed,
  - the number of transactions made,
  - the number of calls abandoned or deterred,
  - the number of agents active, busy or free,

- the status of the agents assigned to sets: free, idle, post-processing or busy (conversation time, answer time, idle time, etc.).

Using the supervisor application, the supervisor manages:

- agent status,
- group status,
- agent activity rates,
- line (ACD port) status.

Note:

The supervisor can also act as an agent.

10.8.1.1 INTERFACE DESCRIPTION

The supervisor application contains three types of screen:

1. **A screen for observing agents or groups**
   It provides real-time information specific to:
   - agent sets
   - groups,
   - activity rates (with screen refreshing every second).

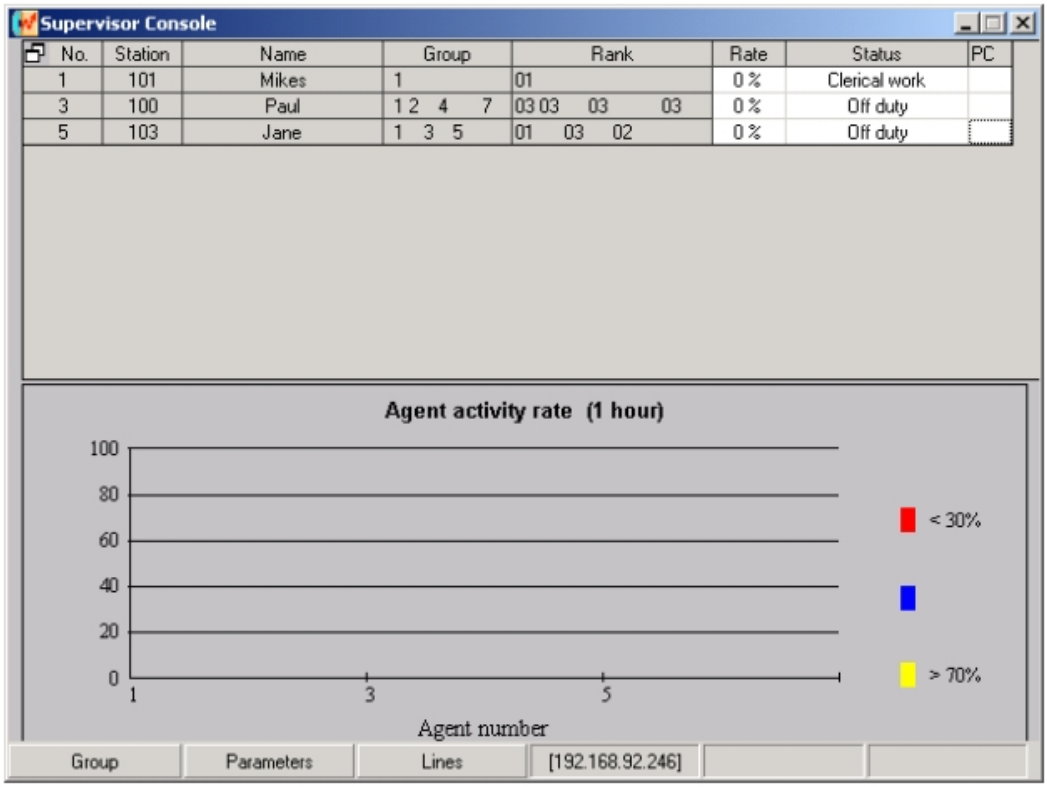
   To switch from the agent screen to the group screen, click the **Group** or **Agent** button at the bottom of the observation screen.
2. **A screen for defining the parameters used to display the results of the observation requested.**
3. **A screen for observing line (ACD port) status.**
   It provides real-time information on the status of lines (with screen refreshing every second).
   To switch from the agent screen to the group screen, click the **Lines** or **Supervisor Console** button at the bottom of the observation screen.

10.8.2 Observation of Agents and Group Activity

10.8.2.1 Operation

10.8.2.1.1 Observation of agent activity

When the Supervisor Console is opened, the agent status window appears.



This window contains two areas:

- An upper area listing agent parameters.
- The **Agent Activity Rate (%)** area.

Upper area listing agent parameters

The upper area lists the agent parameters in a table.

A set can have the following statuses:

- On duty,
- Temporary absence,
- Clerical work,
- Off duty.
- **On duty**
  A set can have the following statuses:
  - ***Awaiting Call***
    The agent assigned to an ACD group is likely to answer the next ACD call.
  - ***No Answer***
    A call has been sent to an agent who does not answer.

Remark 1:
when configuring the general parameters, if the heading ***Agents that do not answer are automatically withdrawn*** *is checked, the supervisor must put the set back on duty for it to be operational again; if the heading is not checked, the status No Answer is displayed for 10 seconds and the set then switches to Awaiting Call.*

- ***Being Routed***
  The agent's set is reserved for a call currently being transferred to it (the set is not yet ringing).
- ***Ringing***
  The agent's set rings after transfer of the ACD call.
- ***ACD Busy***
  The agent is holding an ACD conversation.
- ***Idle***
  The agent has just hung up after an ACD call. He/she is then given an idle period (General Parameters/General tab) before another call is sent.
- ***Not Available***
  The agent's set is busy with non-ACD calls.
- ***Faulty***
  The agent has dialed incorrectly.
- ***Busy, Outgoing Call***
  The agent's set is off the hook without any dialing taking place or the agent is making a non-ACD call.

- **Temporary Absence**
  The agent has temporarily gone off duty for a break.
- **Clerical Work**
  Following an ACD conversation, the agent may, for example, need to assess the call (fill out a customer information screen etc.); he/she temporarily withdraws from the call distribution chain.
- **Off Duty**
  The agent has withdrawn from all ACD groups or the agent has no associated terminal.

  Remark 2:
  an agent observed as off duty on an isolated basis can very easily have an activity rate of 80% for the hour currently being observed.

Agent Activity Rate (%) area

The agent activity rate is represented as a bar chart or graph. The agent activity rate is the ratio between the time spent on ACD calls for each agent in the selected time slot, and the period of time used to calculate activity rates (1 hour or 1/2 hour).

Changing agent parameters

Using the **Supervisor Console** window, the supervisor can change:

- The priority rank of the agent in the groups he/she belongs to.
- The agent status in real-time.
- The group the agent belongs to.

1. In the **Status** column of the table, click the cell corresponding to the agent whose parameters you want to change. The **Agent X Parameters** window appears.

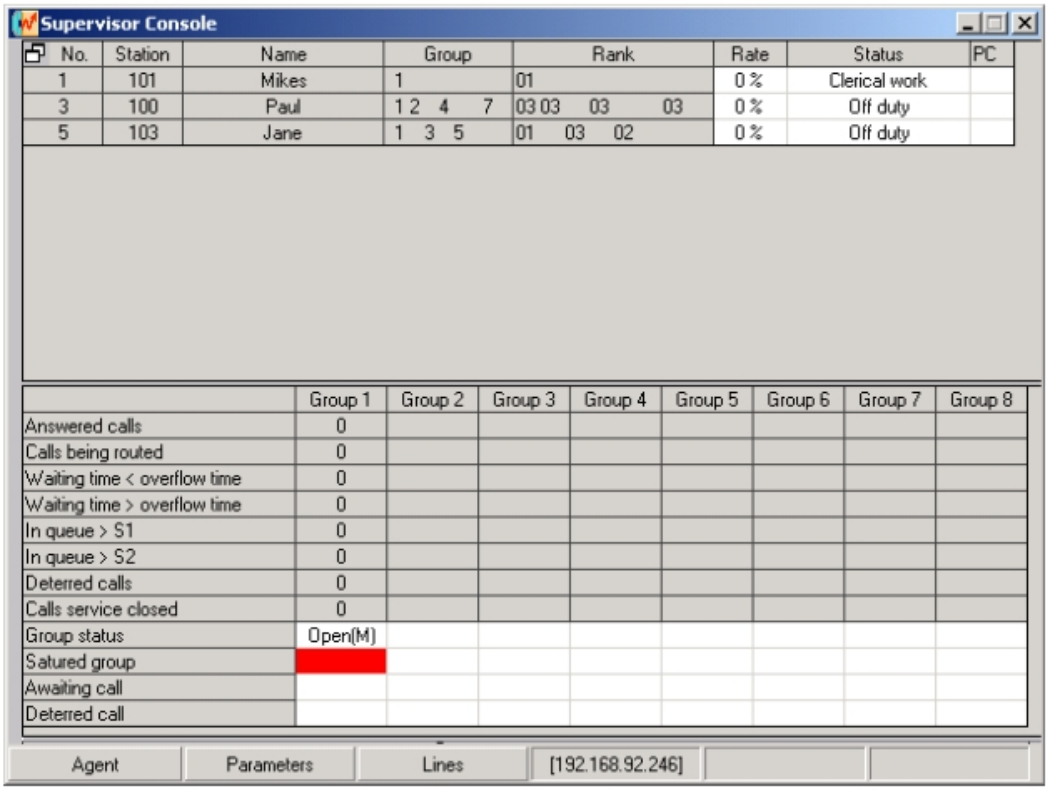
2. Change the parameters as required.

   Remark:
   The name and set number of the agent cannot be changed by the supervisor.

3. Click **Apply** to confirm the data, then **OK** to close the window. The changes are implemented by the system and the new parameters of the agent are shown in the table.

10.8.2.1.2 Observation of group activity

To access the window for observing the status of agent groups, click the **Groups** button. The groups observation window is displayed.



It contains two areas:

- An upper area listing the agent parameters in a table, as described in the previous paragraph.
- A lower area listing the parameters of calls and groups in a table:
  - **Calls Answered**: the number of ACD calls transferred to an agent, and resulting in a conversation being started (even if the conversation time is 0 seconds), regardless of the group (called or through overflow).
  - **Calls Being Routed**: the number of calls in the process of being connected to an agent, but not yet put through.
  - **Waiting Time < Overflow Time**: the number of calls which have been waiting less time than the overflow time delay (search for agent only in the group requested)

- **Waiting Time > Overflow Time**: the number of calls which have been waiting longer than the overflow time delay (search for agent only in the group requested and possibly in the overflow group if the latter is entered).
- **Calls in Queue > S1**: number of calls waiting for longer than threshold S1*. This counter is a subset of the "Calls in Queue" counter.
- **Calls in Queue > S2**: number of calls waiting for longer than threshold S2*. This counter is a subset of the "Calls in Queue > S1" counter.

  Note:
  ** S1 and S2 are two threshold values which can be defined in OMC/General Parameters/General tab.*
- **Deterred Calls**: the number of calls routed to the dissuasion announcement following saturation of the queue, or if no agent is defined in a given group.
- **Calls Service Closed**: the number of calls taking place while the group is closed.
- **Group Status**:
  Forcing to open or closed status is indicated on the Observation screens by the letter M for Manual. To view these statuses, click on the **Group Status** field, selecting the group required.
  The group statuses are:
  - OPEN M : group forced open.
  - CLOSED M : group forced closed.
  - OPEN : group open (depending on time slot or contact).
  - CLOSED : group closed (depending on time slot or contact).
- **Saturated Group**: there are too many calls and the group is overloaded.
  A group x is shown as overloaded as follows:
  - Group x saturated (orange): no agents are free in the group, the next call will be placed in the queue.
  - Group x saturated (red): the time elapsed since group x was saturated is longer than the value **Time Delay Before Gradation of Overload Announcements** defined when the groups are configured.
- **Calls in Queue**: there is at least one call in the queue.
- **Deterred Calls**: at least one call is being deterred.

Remark:
all the percentages in the table are calculated in relation to calls coming into the ACD.

Example 1: default scenario

The parameter **Waiting Begins Before Overflow Time Delay**(*)is checked:

- Calls in queue > threshold S1: number of calls in queue for longer than S1

- Calls in queue > threshold S2: number of calls in queue for longer than S2

In this case, counting of the queue time for the statistics starts as soon as the call enters the queue.

Example 2: specific scenario

The parameter **Waiting Begins Before Overflow Time Delay**(*)is not checked:

- Calls in queue > threshold S1: number of calls in queue for longer than (S1 + overflow time)

- Calls in queue > threshold S2: number of calls in queue for longer than (S2 + overflow time)

where **overflow time** is a value programmed independently for each of the groups 1-4 and 5-8

in the **Overflow Grouping** field.

In this case, counting of the queue time for the statistics starts on termination of the overflow time delay, the wait before this threshold being ignored.

(*) this screen can be accessed via OMC/ACD Services/General Parameters/General tab.

Changing the parameters of agent groups

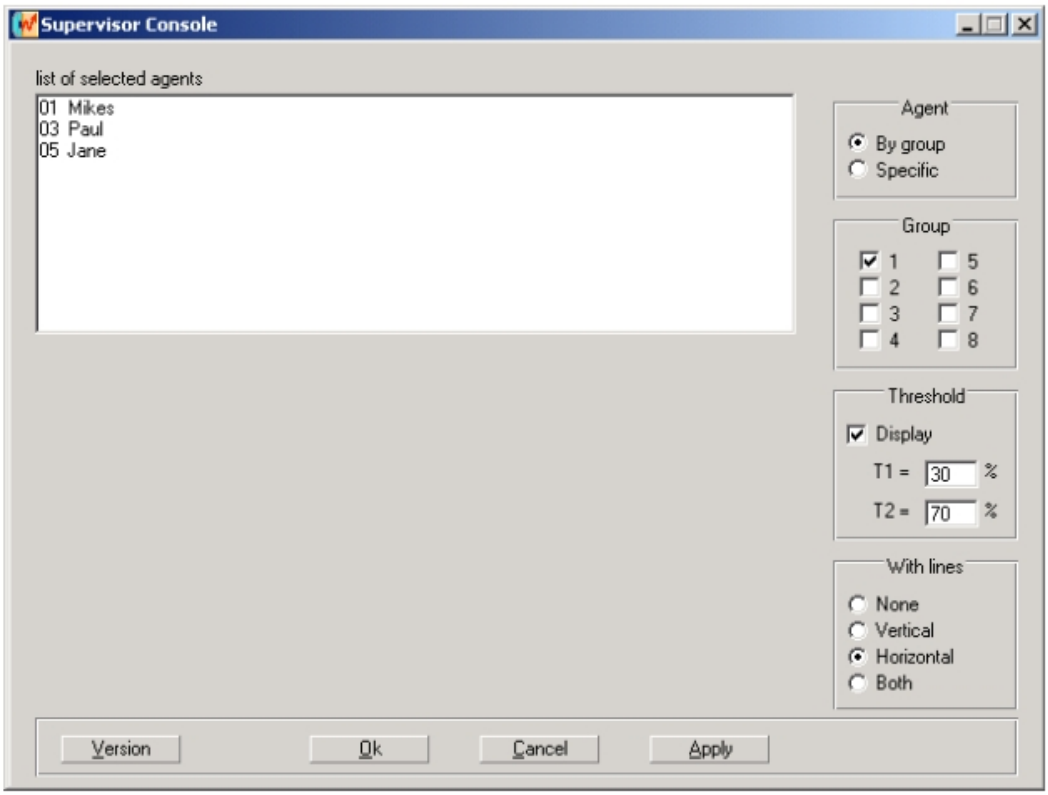
The only parameter which can be changed in real-time is the status of a group.

1. Click the cell corresponding to the group whose status you want to change. The window **Status of Group N° X** is displayed.
2. Select one of the following statuses:
   - Open (Manual): group forced open
   - Closed (Manual): group forced closed
   - Automatic (On Time Slot): group open in accordance with time slots
3. Click **OK** to confirm the data. The status of the group is simultaneously changed.

10.8.3 Displaying observation Windows Parameters

10.8.3.1 Operation

To customize how the observation window is displayed, click the **Parameters** button. The customization window appears.



The following operations can be performed using this window:

- Customizing the table:
  The table can be customized by:
  - Selecting agents by group (**Agent** area, **By Group** option).
  - Select agents in a specific way (**Agent area, Specific** option):
    - Selecting agents on an agent by agent basis, regardless of the group they belong to.
    - Deleting an agent from the list of agents in the table.
- Customizing the **Agent Activity Rate (%)** graph.
  The Agent Activity Rate (%) graph can be customized by:
  - Changing the display percentage of thresholds T1 and T2.
  - Changing the gridlines of the graph.

10.8.3.1.1 Selecting agents by group

1. To select agents by group, select the **By Group** option in the **Agent** area, then select the groups that you want to observe by checking the relevant box in the **Group** area.
2. Click **Apply**. The agents belonging to the group selected are displayed in the area **List of Selected Agents**.
3. Click **OK** to confirm the data and close the customization window. The observation window of the supervision console is displayed. The table shows how it has been customized.

10.8.3.1.2 Selecting agents on an agent by agent basis

Agents are selected on an agent by agent basis, regardless of the group they belong to.

1. Select the **Specific** option in the **Agent** area. All agents configured are displayed in the **List of All Agents** area, in the lower part of the window.
2. To select the agents you want to appear in the observation window, select an agent in the **List of All Agents** area, then click the **Add Agent** button, or double-click on the agent in the **List of All Agents** area. The agent is displayed in the **List of Selected Agents** area.

   Remark:
   each agent must be selected individually.
3. Click **OK** to confirm the data and close the customization window. The observation window of the supervision console is displayed. The table shows how it has been customized.

10.8.3.1.3 Deleting one or all agents from the list of agents in the table

To delete an agent, select that agent from the **List of Selected Agents** area, then click the **Delete Agent** button, or double-click on the agent in the **List of Selected Agents** area. The agent disappears from the **List of Selected Agents** area.

To delete all agents from the **List of Selected Agents** area, click on the **Delete All Agents** button. All agents disappear from the **List of Selected Agents** area.

Click **OK** to confirm the data and close the customization window. The observation window of the supervision console is displayed. The table shows how it has been customized.

10.8.3.1.4 Customizing the Agent Activity Rate (%) graph

1. To customize the **Agent Activity Rate** graph, click the **Parameters** button. The

customization window appears.

2. In the **Threshold** area,
   a. Check the **View** box to display thresholds T1 and T2 on the activity rate graph.
   b. In the fields **T1 =** and **T2 =**, enter the required value. T1 and T2 indicate quality of service, allowing rapid analysis of activity rates.

   Remark:
   T1 and T2 can be used to change the view thresholds of the agent activity rate.

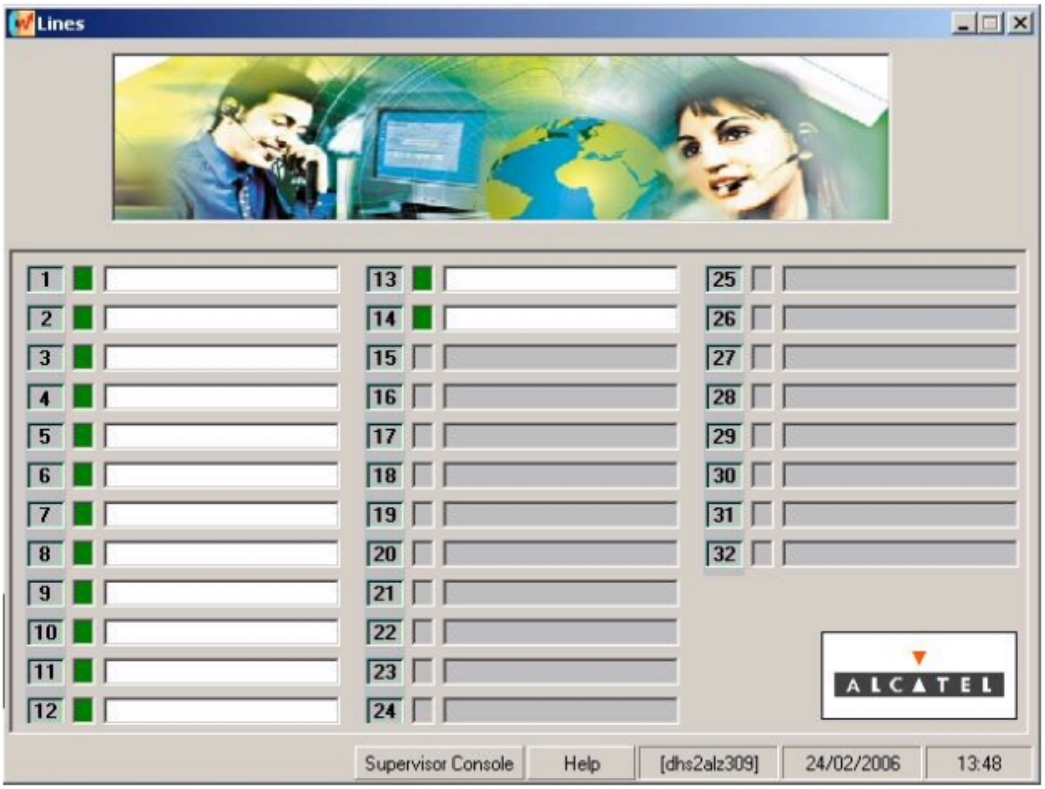
3. In the **Gridlines** area, select the type of gridline required by checking the boxes **None**, **Vertical**, **Horizontal** or **Both**.
4. Click **OK** to confirm the data and close the customization window. The observation window of the supervision console is displayed. The graph is displayed with the new customization.

10.8.4 Line Observations

10.8.4.1 Operation

The **Supervisor** application allows supervisors to access real-time information on lines (ACD ports).

To access the observation screen, click **Lines**.



This screen shows activation of the server lines in real-time (with screen refreshing every second). The screen shows:

- The line number.
- The line status.
  Lines can have one of the following 4 statuses: free (green), incoming (yellow), outgoing, faulty (red).
- A description of the line.
  The heading of the application assigned to the lines is displayed for ACD calls.

10.9 Traceability

10.9.1 Overview

Trace files can be used to obtain information on agent activity or calls.

This information is provided to assist the installer in setting up the ACD. In particular, it provides a list of the latest events related to agents and the ACD calls received.

Trace files are continuously activated, and their size is limited to approximately 100 kbytes. The files are regularly emptied of their content. The traces are in the form of letters and headings, in French only.

Important:
the format of trace files can be changed at any time by the manufacturer, without notice or guarantees in terms of syntax and/or content.

10.9.1.1 DISPLAYING ACD AGENT TRACE MESSAGES

To access the trace file of ACD agents, select the path **OMC / Automatic Call Distribution / ACD Services** and click the **File of ACD Agents** icon. 

Each line displayed represents an action related to an agent or group. Information is provided on the following:

- **yyyy/mm/dd**: the message date
- **hh:mm:ss**: the message time
- **P** or **G**: **P** for Agent Set and **G** for ACD Group

  Note:
  If P is used, the syntax is shifted to the right.
- **AG:**: Agent xx-yyy where xx is the agent identifier (1 to 32) and yyy is the agent set number.
- The letters S, H, A, O, D, N, X, P, B, F and G represent one of the statuses an agent can have. The possible statuses are as follows:
  - S: start of service
  - H: end of service
  - A: temporary absence
  - O: busy, out of ACD service

- D: agent available again
- N: no answer
- X: anomaly
- P: busy with outgoing call
- B: double call
- F: false call
- G: agent re-assigned(G). G is followed by the group number (0 to 7)

- **a**, **b**, **c** : show the group status: forced opening of the group (a), end of status forcing (b), forced closure of the group (c).

The figure below shows an example of an ACD Agents trace file.

10.9.1.2 DISPLAYING ACD CALL TRACE MESSAGES

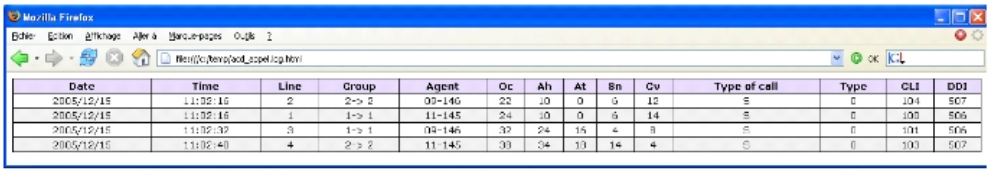
To access the trace file of ACD calls, select the path **OMC / Automatic Call Distribution / ACD Services** and click the **File of ACD Calls** icon. 

Each line displayed represents a call. Information is provided on the following:

- **yyyy/mm/dd**: the call date
- **hh:mm:ss**: the call time
- **A**: ACD
- **V**: the ACD port number
- **G**: the number of the group called (1 to 8); the number of the assigned group which answered the call
- **Ag**: the number of the assigned group which answered the call, followed by the set number of the agent who answered the call
- **Oc**: the total busy time from the agent picking up the call to the end of the communication in seconds (busy time = routing time + queuing time + ringing time + conversation time)
- **Ah**: the routing time in seconds (routing time = busy time - conversation time)
- **At**: the queuing time

- **Sn**: the ringing time of the agent set included in the routing time, in seconds
- **Cv**: the conversation time in seconds
- **S**, **D**, **A**, **F**, **f**, **R**, **Q** and **X** show one of the statuses that a call can have. The possible statuses are as follows:
  - S: answered
  - D: deterred
  - A: abandoned by the caller
  - F: closure on time slot
  - f: forced closure
  - R: routed to the transfer number
  - Q: the caller voluntarily left the queue
  - X: anomaly in routing the call
- **Ia**: the agent identifier (1 to 32)
- **Qlf**: definition of call types

The figure below shows an example of an ACD Calls trace file.



Chapter 11

Management Tools

11.1 OMC

11.1.1 Installation and Start-Up

11.1.1.1 Overview

OMC is the unified administration and configuration tool for Alcatel-Lucent OmniPCX Office Communication Server; running on a PC, it can be used for example to program the system's voice functionality, voice mail, the network, Internet access, downloading, even printing of mailing labels.

11.1.1.1.1 MINIMAL PC CONFIGURATION

- Pentium 166 MHz processor
- RAM: 128 MB
- Windows 2000 (with SP4 or above and Windows Installer 3.0), Windows 2003 (with SP1 or above), Windows 2003 R2, Windows XP (with SP2 or above and framework .Net 2.0) or Windows Vista
- Hard disk: 60 MB120 MB (recommended for installation and operation)
- Screen: 800 x 600 pixels
- 1 mouse
- 1 serial port (optional, only required for console traces see module Start and Stop of a System - Maintenance § Console port)
- 1 Ethernet board
- 64K (1 B-channel) or 128K (2 B-channels) PPP-compatible ISDN modem or V34 modem for remote access

11.1.1.1.2 INSTALLING THE OMC SOFTWARE

The OMC software is installed from a CD-ROM.

The application is installed by making selections from the options proposed in the various windows.

When installation is finished, you access the application either:

- by double-clicking the new icon created on the Windows desktop
- by selecting **Start** -> **Program** -> **Alcatel-Lucent OmniPCX Office Communication Server** -> **OMC** (in the case of an English-language operating system, this path can be customized). The OMC welcome dialogueue box appears

11.1.1.1.3 OMC REMOTE ACCESS

With remote access, you can use OMC to configure or download an Alcatel-Lucent OmniPCX Office Communication Server system. This access can be managed using:

- an ISDN modem able to use ISDN PPP (point to point) protocol at 64K (1 B-channel) or 128K (2 B-channels)

- a V34 analog modem in Hayes protocol at 33600 bds

The management of these two modems is integrated into Alcatel-Lucent OmniPCX Office Communication Server.

Important:
The OMC software must be installed on the remote maintenance PC, if Windows Terminal Server is not being used.

11.1.1.1.4 REMOTE ACCESS BY ISDN MODEM

ISDN modem recommended

Alcatel-Lucent OmniPCX Office Communication Server is equipped with a 64K (1 B-channel)/128K (2 B-channels) ISDN modem using PPP protocol for remote access through the public network. It provides a point-to-point link accessible via standard LINUX procedures (PPP, etc.).

For a 64K (1 B-channel) connection, the following modems are validated:

- KORTEX NOVAFAX ISDN 128000/33600 with PPP protocol
- FRITZ ¡X CAPI 2.0 or any standard "FRITZ" modem
- Multitech I Way Hopper MTA 128 ST 128 KBPS ISDN (see note below)

For a 128K (2 B-channels) connection, the following modems are validated:

- OLITEC USB ISDN 128K
- Multitech MTA128ST-RC ML-PPP (see note below)
- Eicon Diva 852 ISDN T/A USB - ISDN BRI ST - 128 Kbits/s

ISDN 64 to 128 KPBS modems handling the PPP protocol are generally compatible and support CHAP authentication.

Note:
When using the Multitech modem, the authentication method must be set to CHAP. This is the default method for current firmware versions. For modems with older firmware, you must either update the firmware or activate CHAP with the AT command ***AT S58=3****.*

RAS installation process

In Windows 2000/XP/Vista, you do not need to install new operating system components before configuring a new access method; the Remote Access Services (RAS) component is installed by default on these systems.

The sub-sections below describe how to set up the following remote access methods:

- Direct V24 Connection (OmniPCX Office Direct V24)
- Remote connection via ISDN modem (an example is provided for driver installation)

V24 driver installation procedure

1. Open the **Control panel**.
2. Select **Phone and Modem Options**.
3. Select the **Modems** tab.

4. Click **Add**.
5. Check **Don't detect my modem; I will select it from the list**.
6. Follow the Wizard instructions to install the modem. You will need to choose the COM port that will be associated with the modem.
7. You may need to reboot the PC to complete the installation.

Installing the driver for an ISDN modem (example)

The following procedure describes how to install a FRITZ modem.

1. Insert the modem installation CD-ROM.
2. Click the **FRITZ ¡X PC Capi driver** installer icon The wizard is displayed.
   a. Indicate the serial port where the modem will be connected.
   b. When the install process is complete, reboot the PC.
3. Insert the modem installation CD-ROM. The wizard is displayed
   a. Click the **FRITZ ¡32 Communication Software** installer icon.
   b. Select **Install and configure**.
   c. Use the default installation (click **Next** in each Wizard screen).
   d. At the end of the Wizard mode, check the **Install Capi-port driver** box.
4. Select **AVM ISDN1 Internet (PPP over ISDN)**.
5. Reboot the PC.

Using remote access with OMC

1. Launch **OMC**. The OMC Welcome page is displayed.
2. Select the appropriate menu, as follows:
   - the **Expert** menu, if you are logging in as "installer"
   - the **EasyPlus** menu, if you are logging in as "administrator"
   - the **Easy** menu, if you are logging in as "operator" or "attendant"
3. In the toolbar menu, click **Comm**.
4. Select **Connect**. The **Communication Path** window is displayed.
5. Click **Modem direct**, then **OK**.
6. Click **Dialling** and select **AWM ISDN1 Internet (PPP over ISDN)**.
7. Dial the customer phone number and click **OK**.
8. Type in the appropriate password according to your user mode, as follows:
   - **Expert**: pbxk1064
   - **EasyPlus**: kilo1987
   - **Easy**: help1954

Note:
The PC and B1 lights on the modem should light up when the connection is established.

The configuration session is open.

Remote access to the ISDN modem

When an ISDN modem is used, it is necessary to reserve a DDI number in the public numbering plan to be able to establish remote access.

If no DDI number is available, check whether the system's ISDN modem access is in the default attendant group (default group). In this case it is not necessary to keep a DDI number.

Remark:

If the modem is not currently in the attendant group, it is useful to set the Reroutdata flag to the value 01H. The system then automatically recognises the ISDN service corresponding to the incoming call and looks in the default attendant group for a data terminal.

11.1.1.1.5 REMOTE ACCESS BY THE ANALOG MODEM

Analog modem (recommended)

Alcatel-Lucent OmniPCX Office Communication Server is equipped with an analog V34 modem for remote access through the public network. This modem provides a point-to-point communication link accessible via standard LINUX protocols (PPP, etc.).

Its main characteristics are:

- V34 Modem
- Maximum transmission speed: 33600 bds
- Hayes protocol

In the current version of the system, the V34 "US Robotic" modem has been validated. The other types of modems were not validated.

Installation process of the remote access by analog modem

Follow the procedures described in the previous paragraphs, but replace the **FRITZ** modem with the **US Robotics** analog modem.

Remote access to the analog modem

When the analog modem is used, it is necessary to hold a DDI number in the public numbering plan in order to be able to carry out remote maintenance.

In the case of no DDI number is available, the access to the modem will be possible only via the operator transfer.

11.1.1.1.6 OPERATING MODE

1. Open **OMC** on the remote access PC.
2. Select the **Expert** menu.
3. Click **Comm**.
4. Select **Connect**. The **Communication Path** window is displayed.
5. Click **Modem direct**, then **OK**.
6. There are two ways of establishing a remote connection:
   - Select a modem phone book entry in the **Used Entry** field of the **Modem Connection** window.
   - Click **Dialling**, select the modem to use ("used modem"), then dial the customer remote access number in the **Number** field.

7. Enter the system's default password **pbxk1064**. It will take a few seconds for the connection to be established.

11.1.1.1.7 SECURITY

In the remote access, the protocol used in the "data link" OSI layer is PPP (Point-to-Point Protocol). The TCP/IP protocols are used respectively in the "transport" and "network" layers. For each layer, Alcatel-Lucent OmniPCX Office Communication Server carries out an access control.

Authentication

At the start of the connection (PPP), an account name (system masked) and password (pbxk1064) are required. This account name is automatically generated by OMC. The password is required by OMC to establish a direct connection (LAN) with Alcatel-Lucent OmniPCX Office Communication Server. Any other authentication will be rejected.

Firewall

If the system accepts the authentication, the PPP connection will be established, and all the data packets received on this interface will be filtered according to the following rules:

All the packets are refused except:

- packets bound for Alcatel-Lucent OmniPCX Office Communication Server FTP server via two TCP ports preset for the PBX configuration by OMC.
- packages bound for Alcatel-Lucent OmniPCX Office Communication Server HTTP server via the HTTP port preset for the Internet access configuration by WBM (Web Based Management).
- control packets using the ICMP protocol (Internet Control Message Protocol).

11.1.1.1.8 LOCAL V24 ACCESS FOR OMC

It is possible to use OMC software to dialogue with OmniPCX Office using a V24 connection. In this case the network connection is not necessary.

A specific reinforced cable must link the "Config" RJ45 connector on the system CPU to the Com port of the PC using OMC.

Wiring of the connection cable

RJ45	SUB D 9-point (F)
1	7
2	4
3	3
4	NC
5	5
6	2
7	6
8	8

Installation procedure

1. Open the **OMC** software on the PC.
2. Select the **Expert** mode.

3. Select **Comm** from the menu toolbar.
4. Select **Connect** from the dropdown menu. The **Communication Path** window is displayed.
5. Select **Local V24**.
6. The system proposes installation of **Alcatel-Lucent OmniPCX Direct V24**. Click **Yes**. The **Modem options** window is displayed.
7. Click **Add**. The **Installation** window is displayed.
8. In the **Installation** window, check **Don't detect my modem. Propose the option in a list** and click **Next**.
9. Select the manufacturer.
10. Select **Alcatel-Lucent OmniPCX Direct V24** (for Windows XP/2003/2000).
11. Select the Com port used.
12. Click **Next**.
13. Click **Finish**.
14. Click **Close**.
15. Back in OMC, click **Comm**. The **Local V24** box is now enabled and the Com port is displayed.
16. Click **Ok** and enter the password. It will take a few seconds for the OMC to connect to the system.

11.1.1.1.9 LOCAL ACCESS BY LAN

The default IP address for the main CPU board is 192.168.92.246 for:

- A connection to the LAN port on the main CPU board via a UTP Category 5 5-100 Ohm crossover cable.
- A connection to the switch to which the main CPU board is connected by a direct cable.

The PC IP address and network mask must be compatible with the address of Alcatel-Lucent OmniPCX Office Communication Server. For example 192.168.92.1 and 255.255.255.0.

For security reasons, the OmniPCX Office can be configured with an additional IP address, which is used only for management of OmniPCX Office.

11.1.1.1.10 DOWNLOADING THE SOFTWARE

To download the software, use the following procedure.

1. Open OMC.
2. Open the **Tools** folder.
3. Open the **OMC-Software Download** application.
4. In the **Communication Mode** window, select the type of download:
   - Local
   - Modem Direct
   - Modem Call Back
   - LAN

5. Enter the password **pbxk1064**.
6. The **OMC-Software Download** window opens. This window has several areas:
   - One parameter setting area to:
     - Select the directory containing the sub-directory **DownloadingItems**.
       Use the **Delivery file** drop-down menu.
     - Select the country for the new software release.
       Use the **...Delivery** drop-down menu in the **Country & Supplier...** area. The field **... In the PCX** shows for information the country of the software release currently used.
     - Save the data.
       If the **Data saving** box is checked: the system automatically saves and restores the data after having swapped over to the new software release.
       If the **Data saving** box is not checked, you must use the new OMC to: save the data to a file, download/swap to the new software version and then restore the data from the file to the PBX.
     - Download all the files required for Automatic Call Distribution (ACD) by checking **ACD Service**.
     - Download the files needed for voice features on IP.
       According to customer needs, check **Voice Over IP**.
     - Download the files required for remote access.
       Depending on customer needs, check **Remote Access Service**.
     - Download the files required for Internet services.
       According to customer needs, check **Internet Services**.
     - Select the language of the voice guides to download.
       Click the **Languages** button to access the **Languages to Download** window.
     - Define a time zone by selecting a city and country.
       Click the **Time Zone** button to access the **Time Zone to Download** window.
     - Define the software swap mode.
       In the **Software Exchange** area, there are two possible choices:
       Click the **After OMC disconnect** button to swap immediately. The swap starts when you quit the downloading application.
       Click the **Date** button and indicate the required date and time for a delayed swap.

       Remark:
       If you select immediate switching, it will take effect as soon as you quit the download application.
   - A read only zone
     - The **Downloadable Item** area allows you to see the different versions of the applications constituting Alcatel-Lucent OmniPCX Office Communication Server.
     - The **Action** column lists the files to download.
     - The bottom part of the window allows you to follow downloading progress precisely. Each downloading and acknowledgement action produces a message.
7. Click **Start** to start downloading.

11.1.1.1.11 IMPORTING/EXPORTING FILES

This function is used to import into Alcatel-Lucent OmniPCX Office Communication Server a data file sent by a customer (or a file previously exported from an Alcatel-Lucent OmniPCX Office Communication Server system; for example, a file of collective speed dial numbers with

the extension .CRP).

Importing data

To import Excel data into OMC, follow the procedure below.

1. Edit the file in Excel.
2. Check the syntax. The name must contain no punctuation, spaces, digits in the first 2 characters or more than 15 characters.
3. Copy all the Excel data.
4. In OMC (connected beforehand), select **Collective Speed Dial**.
5. Copy the file's data into this directory. The system checks the syntax.
6. Click **OK** to confirm copying of the data.

Exporting data

To export Excel data from OMC, follow the procedure below.

1. In OMC (connected beforehand), select **Collective Speed Dial**.
2. Copy the OMC data (to put it onto the clipboard) using the contextual menu.
3. Paste the OMC data (from the clipboard) to an Excel document.

11.1.1.1.12 Access with Proxy

A proxy server can be added to improve security.

To connect a remote OmniPCX Office via a proxy server, the login dialogue box can request a user account and password to connect to the proxy server.

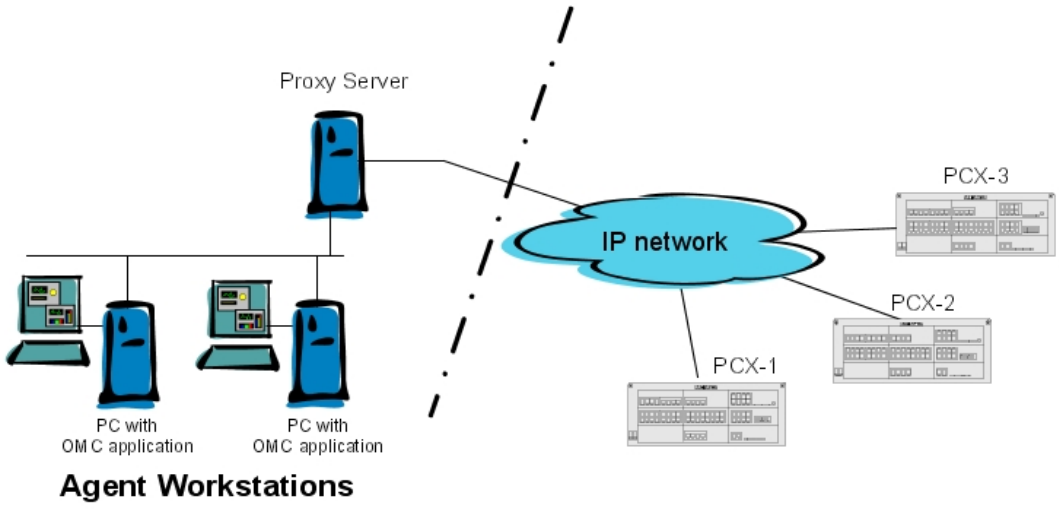


Figure 11.1 : Configuration Example with a Proxy Server

To configure a proxy server:

1. In OMC, select **Options > Proxy Parameters** from the menu toolbar
   The **Privileged User Login** window opens
2. Enter the **Privileged User Password** and validate
   The **Proxy Parameters** window opens
3. Enter Proxy parameters:
   - **No Proxy Used**: when this radio button is selected, the proxy server is not used. In this case, all other fields are disabled
   - **Use Proxy Server**: when this radio button is selected, requests from and to OMC are sent via a proxy server
     - **Name/IP Address**: enter the name or IP address of the proxy server
     - **Port**: enter the port number used by the proxy server
     - **Do not use proxy for local address**: when this checkbox is validated, requests are not sent via the proxy server when destination addresses are in the same subnetwork
     - **User account in Proxy server**: enter the user account for the proxy server
     - **Password**: enter the associated password

   If the proxy account and password are incorrect in the above parameters, each login dialogue box, to connect a remote OmniPCX Office, requests the proxy account and the associated password,

To modify the privileged user password:

- In OMC, select **Options > Change Privileged User Password** from the menu toolbar
  The **Change Privileged User Password** window opens.
- Enter the **Old Password**(after installation, the initial password is OMCAdmin)
- Enter the **New Password**
- Confirm the **New Password**

Note 1:

If you forget the privileged user password, the only solution is to uninstall and reinstall the OMC.

Note 2:

When OMC is launched from 4760 in online mode, the above mentioned configuration is not applicable.

11.1.2 Services provided

OMC provides a complete set of configuration tools for Alcatel-Lucent OmniPCX Office Communication Server systems.

Three packages are available:

Package	Corresponding views	Levels of use (passwords)
OMC Expert	Expert View, EasyPlus View, Easy View	Manufacturer Installer (pbxk1064)
OMC EasyPlus	EasyPlus View, Easy View	Administrator (kilo1987)
OMC Easy	Easy View	Attendant (help1954)

Expert View offers Wizard-type configuration and Easy/EasyPlus View also offers some Wizard-type configuration.

The Wizard (or configuration assistant) serves to configure the most commonly used system parameters; OMC helps configure these parameters using a series of simple questions, with plenty of guidance and explanation. Indeed, using the default configuration avoids having to program a lot of the parameters.

For customised installation, there are links to Expert View menus from the pages of the Wizard, flagged by the "Advanced" and "Details" buttons in EasyPlus View. The configuration assistant is available on installation and throughout the life of the system.

Expert View gives you unrestricted access to all the configuration possibilities.

Features included		**Easy**	**EasyPlus**	**Expert**
Tools				
.	Software download			Yes
.	Batch software distribution			Yes
.	Data collection	Yes	Yes	Yes
.	Database transformation			Yes
.	Batch data distribution			Yes
.	Lola	Yes	Yes	Yes
.	Labelset	Yes	Yes	Yes
Client/supplier info		**Yes**	**Yes**	**Yes**
Typical installation				
.	Business Initial Installation Wizard	Yes	Yes	Yes
.	Hotel Initial Installation Wizard	Yes	Yes	Yes
.	Data loading Wizard	Yes	Yes	Yes
.	DECT/PWT on-air registration	Yes	Yes	Yes
Typical modification				
.	Subscribers	Yes	Yes	Yes
.	Groups	Yes	Yes	Yes
.	System	Yes	Yes	Yes
.	Collective Speed Dialling	Yes	Yes	Yes
.	External Accesses	Yes	Yes	Yes
.	Export System overview	Yes	Yes	
Numbering				
.	Installation numbers			Yes
.	Default configuration			Yes
.	Numbering plans			Yes
.	Features in conversation			Yes
.	DDI number modification table			Yes
.	Number modification table			Yes
.	Splitting table			Yes
.	End of dialling table			Yes

Features included		**Easy**	**EasyPlus**	**Expert**
.	Automatic Routing Selection (Automatic routing: Prefixes, Trunk groups list, Hours, Day groups, Providers/destinations, Authorisation codes, Tone/Pause-MF, ARS Miscellaneous)			Yes
.	PTN conversion			Yes
Collective Speed Dialling		**Yes**	**Yes**	**Yes**
Directory				Yes
Subscribers/Basestations List				**Yes**
Voice Processing				
.	Voice processing activation			Yes
.	Automated attendant			Yes
.	Mailboxes			Yes
.	Information messages			Yes
.	General parameters			Yes
.	Statistics			Yes
Time Ranges				**Yes**
Attendant groups				**Yes**
Hunting groups				**Yes**
Broadcast groups				**Yes**
Pick-up groups				**Yes**
Manager/secretary relationship				**Yes**
Subscribers Misc.				
.	Pre-announcement (Overview, Messages)			Yes
.	Permanent Logical Links (PLLs)			Yes
.	Fax notification for subscribers			Yes
External Lines				
.	List of accesses			Yes
.	List of trunk groups			Yes
.	Remote substitution			Yes
.	Traffic counters (number of outside calls)			Yes
.	Protocols (analogue protocols, private and public ISDN access at levels 2 and 3, ISVPN protocols)			Yes
.	Analogue Protocols Selection			Yes
.	Incoming call handling			Yes
Hardware and Limits				
.	Main cabinet	Yes	Yes	Yes
.	Extension cabinet	Yes	Yes	Yes
.	Auxiliary interfaces			Yes

Features included			Easy	EasyPlus	Expert
.	IP addresses				Yes
.	Software key features				Yes
.	Fan Management				Yes
.	System's Limits				Yes
Metering					
.	Metering				Yes
.	Metering transmission characteristics				Yes
.	Currency conversion				Yes
.	Metering counters				Yes
Traffic Sharing and Barring					
.	Traffic sharing matrix				Yes
.	Barring matrix				Yes
.	Barring tables				Yes
.	Joining				Yes
.	Account code table				Yes
Network Management Control					
.	Callback/Authorised callers				Yes
.	Centralised management				Yes
.	Select Urgent Alarms				Yes
.	SNMP (Simple Network Management Protocol)				Yes
Voice over IP					
.	VoIP: Parameters				Yes
.	VoIP: Traffic counters				Yes
Internet Access Configuration					**Yes**
System Miscellaneous					
.	Feature design				Yes
.	Set PCX date and time adjustment				Yes
.	Password				Yes
.	System Reset				Yes
.	DECT/PWT ARI/GAP				Yes
.	DECT/PWT Frequencies				Yes
.	UTAM Licence				Yes
.	**Memory Read/Write**				
.		Timer Labels			Yes
.		Debug Labels			Yes
.		Other Labels			Yes
.		Numeric Addresses			Yes

Features included			Easy	EasyPlus	Expert
.	**Messages and Music**				
.		Music on Hold			Yes
.		Mailing messages			Yes
.	Doorphone signals				Yes
.	Manual normal/restricted mode				Yes
	Software versions				
Import/Export					
.	Import/Export Data				Yes
.	Exporting Labels				Yes
History & Anomalies					
.	History table				Yes
.	HW Anomaly Table				Yes
Data Saving & Swapping					
.	Commands				Yes
.	Date & Time Data Saving				Yes
.	SW-Downloading				Yes
.	Terminals Downloading				Yes
Automatic Call Distribution					
.	ACD setup			Yes	Yes
.	ACD services			Yes	Yes
.	ACD voice messages			Yes	Yes
.	ACD statistic manager			Yes	Yes
Central Services Global Info					**Yes**

11.1.3 Managing Voice Prompts

11.1.3.1 Operation

11.1.3.1.1 Introduction

OMC offers the facility to import, export and save audio files containing on-hold music, automated attendant voice prompts, pre-announcement messages and Automatic Call Distribution voice messages. This chapter describes audio file management.

Note:
In this chapter and in the OMC tool, the phrase "voice prompts" is sometimes used to refer to all kinds of audio files.

11.1.3.1.2 Individual types of audio file

The following categories of audio files are used by the Alcatel-Lucent OmniPCX Office Communication Server system:

- On-hold music
- Automated attendant voice prompts
- Pre-announcement messages
- Automatic Call Distribution voice messages

Externally recorded, custom audio files can be used for all of the above. The import and export of these audio files are described in the sub-sections below.

On-hold music

On-hold music is the music played to an external phone set which has been put on hold during a call.

Three options are available:

- **Default Music:** This is the standard music provided by the system.
- **Tape:** This is music from an audio source (such as a cassette tape player) connected to the audio-in connection of the system's CPU board.
- **Recorded Music:** This is music from a custom audio file (with .wav extension) stored in the system.

With regard to the last option, the OMC tool allows you to transfer a custom audio file containing on-hold music to or from the system. You can therefore import an audio file to the system from your PC, or export an audio file from the system to your PC. The path to the required screen within OMC is:

System Miscellaneous > Messages & Music > Music on Hold

For information on how to use this screen, refer to the OMC Help.

Note:

In order to transfer audio files, OMC must be in online mode (connected to the system) - the transfer option is not available in offline mode. Also, this option is only available when using OMC in Expert mode.

The duration of the musical sequence in an audio file can be up to 10 minutes (the actual maximum duration depends on your licence). A request to transfer to the system an audio file that exceeds this duration will be refused.

A custom audio file for on-hold music must be a .wav file. No other audio file format is accepted. The file must also satisfy one of the following audio encoding requirements:

Encoding Type	Bits Per Sample	Sample Frequency	Channels
ADPCM (G726)	4	8 kHz	Single (mono)
CCITT A-law encoded PCM	8	8 kHz	Single (mono)
CCITT µ-law encoded PCM	8	8 kHz	Single (mono)
Linear PCM	16	8 kHz	Single (mono)

In fact, the system stores the recording as 4-bit ADPCM (G726). If you provide the audio file in any of the other encodings listed above, OMC converts the file to the ADPCM encoding before passing it to the system. When an audio file is transferred from the system to a PC, OMC converts this file from 4-bit ADPCM to 16-bit linear PCM, since ADPCM cannot be played by standard desktop media players.

Automated attendant

An audio file can be provided for each menu and sub-menu of the automated attendant, as well as for an automated attendant welcome message and goodbye message. All these messages, except the goodbye message, can exist in two different versions for use during opening hours and closing hours.

The OMC tool allows you to transfer custom audio files containing automated attendant voice prompts to or from the system. You can therefore import audio files to the system from your PC, or export audio files from the system to your PC. The path to the required screen within OMC is:

Voice processing > Automated attendant

For information on how to use this screen, refer to the OMC Help.

Note:
In order to transfer audio files, OMC must be in online mode (connected to the system) - the transfer option is not available in offline mode. Also, this option is only available when using OMC in Expert mode.

A custom audio file for an automated attendant voice prompt must be .wav audio files (no other audio file format is accepted). The file for must also satisfy one of the following audio encoding requirements:

Encoding Type	Bits Per Sample	Sample Frequency	Channels
ADPCM (G726)	4	8 kHz	Single (mono)
CCITT A-law encoded PCM	8	8 kHz	Single (mono)
CCITT µ-law encoded PCM	8	8 kHz	Single (mono)
Linear PCM	16	8 kHz	Single (mono)

In fact, the system stores the recording as 4-bit ADPCM (G726). If you provide the audio file in any of the other encodings listed above, OMC converts the file to the ADPCM encoding before passing it to the system. When an audio file is transferred from the system to a PC, OMC converts this file from 4-bit ADPCM to 16-bit linear PCM, since ADPCM cannot be played by standard desktop media players.

Pre-announcement messages

A pre-announcement message can be played to an external caller before their call is answered (either before the phone starts ringing or while it is ringing), as a company welcome message, for example. The system can store up to 8 pre-announcement messages (the maximum number depending on your license). The durations of the messages are pooled and the total length of all the messages must not exceed a certain limit (which depends on your license).

The OMC tool allows you to transfer custom audio files containing pre-announcement messages to or from the system. You can therefore import audio files to the system from your PC, or export audio files from the system to your PC. The path to the required screen within OMC is:

Subcribers Misc > Preannouncement Messages

For information on how to use this screen, refer to the OMC Help.

Note:
In order to transfer audio files, OMC must be in online mode (connected to the system) - the transfer option is not available in offline mode. Also, this option is only available when using OMC in Expert mode.

A custom audio file for a pre-announcement message must be a .wav audio file (no other

audio file format is accepted). The file must also satisfy one of the following audio encoding requirements:

Encoding Type	Bits Per Sample	Sample Frequency	Channels
CCITT A-law encoded PCM	8	8 kHz	Single (mono)
CCITT µ-law encoded PCM	8	8 kHz	Single (mono)
Linear PCM	16	8 kHz	Single (mono)

In fact, the system stores the recording as 8-bit CCITT A-law or µ-law encoded PCM, depending on the country. If you provide a 16-bit linear PCM audio file, OMC converts the file to the relevant 8-bit encoding before passing it to the system. However, you must provide either 16-bit linear PCM or the required CCITT law encoding, as OMC will not convert between the A-law and µ-law encodings.

Automatic Call Distribution voice messages

There are six Automatic Call Distribution voice messages, one for each call center action. The six messages (with their maximum durations) are:

Voice Message	Description	Maximum Duration
Welcome	Broadcast when the caller arrives in the group.	60 seconds
Waiting 1	Broadcast once, when the caller joins the queue.	60 seconds
Waiting 2	Continuously broadcast after the first waiting message.	300 seconds
Deterrence	Broadcast when the queue is full.	60 seconds
Closing	Broadcast when the caller arrives in the group, to indicate the group is closed.	60 seconds
Estimated waiting time	Broadcast to indicate to the caller that they are likely to have a certain minimum waiting time before the call is answered (for example, 'You may have more than 5 minutes to wait before your call is answered').	60 seconds

In fact, you can store up to 8 such sets in the system, referred to as Automatic Call Distribution groups 1 to 8.

You can create your own voice mail messages using recording software available on your PC. It is also possible to record voice messages from one of the installed telephone handsets, e.g. by recording Information Messages (**MMC handset/Instal/VMU/List/Select messages 1 to 50/record**).

The OMC tool allows you to transfer custom audio files containing Automatic Call Distribution messages to or from the system. You can therefore import audio files to the system from your PC, or export audio files from the system to your PC. The path to the required screen within OMC is:

Automatic Call Distribution > Automatic Call Distribution Voice messages

For information on how to use this screen, refer to the OMC Help.

Note:

In order to transfer audio files, OMC must be in online mode (connected to the system) - the transfer option is not available in offline mode. Also, this option is only available when using OMC in Expert mode.

A custom audio file for an Automatic Call Distribution voice message must be a .wav audio file (no other audio file format is accepted). The file must also satisfy one of the following audio encoding requirements:

Encoding Type	Bits Per Sample	Sample Frequency	Channels
CCITT A-law encoded PCM	8	8 kHz	Single (mono)
CCITT µ-law encoded PCM	8	8 kHz	Single (mono)
Linear PCM	16	8 kHz	Single (mono)

In fact, the system stores the recording as 8-bit CCITT A-law or µ-law encoded PCM, depending on the country. If you provide a 16-bit linear PCM audio file, OMC converts the file to the relevant 8-bit encodings before passing it to the system. However, you must provide either 16-bit linear PCM or the required CCITT law encoding, as OMC will not convert between the A-law and µ-law encodings.

11.1.3.1.3 Global management of audio files

This section describes a general method for managing (exporting, importing and saving) audio files (voice prompts) of all kinds. Therefore, the actions described here apply to all audio file types (on-hold music, automated attendant voice prompts, pre-announcement messages and Automatic Call Distribution voice messages).

Note:

Alternatively, the different audio file types can be individually managed as described in § Individual types of audio file .

General export procedure

In order to export audio files, it is necessary to open the Alcatel-Lucent OMC software in direct connection and Expert mode. The following procedure is the same for all kinds of audio file, but here we take the example of a mailbox greeting.

1. Select the **Subscribers/Base stations list**.
2. Select a subscriber of your choice which already has a personalised mailbox.
3. Click **Details**.
4. Click **Mailbox**.
5. Select **Option** in the **Subscriber mailbox** window and then select the box **Voice prompt - Personal greeting Transfer and save as**. At this stage, it is possible to:
   - export the voice prompt
   - listen directly to the message (click **Play**)
   - delete it (click **Erase**)
6. Specify the destination path for the export on your main hard drive (for example, **C:/Temp/Prompts**) and the file name.
7. Click **Export**; at this stage, the system will suggest a file format, either the standard .wav PC format or the regular Alcatel-Lucent ADPCM format.

8. The voice prompt is then transferred from the system to the PC; this operation may take few seconds according the size of the file. The voice prompt will be stored on your drive in one of the formats Alcatel-Lucent ADPCM G726 or PCM 16 bit 8 kHz mono, according to your choice.

   Note:
   *If no greeting has been pre-recorded (no customisation), the **Personal greeting** box is greyed out.*

General import procedure

The import procedure is the same as the export procedure described above.

You must specify the exact path on your PC where the file to be imported is located. You must then click on **Import**. The transfer duration depends on the file size.

Note:
At any time, it is also possible to listen to or erase the audio file (the file present in the system).

Complete save of audio files

All audio files can be globally saved using the following save procedure:

1. Start the Alcatel-Lucent OMC software with a direct or remote connection.
2. Select the menu **Comm -> Read from PBX -> Voice Prompts**.
3. Click **OK**.
4. Wait until the end of the transfer.
5. Save the file selecting **File -> Save as**.
6. Enter a file name and click **OK**.

The audio files stored this way are available under:

C:\Program Files\PCXTools\OMC\R400_12.1b\targprod\afr100\customer.dbs

Note:
*Directory **R400_12.1b** corresponds to the OMC version used during the save procedure; directory **afr100** corresponds to the "Target" system used during OMC installation*

The .wav files stored following this procedure are in the format Alcatel-Lucent ADPCM G726 and can be listened to or modified only using specific software and Codec.

11.1.3.1.4 System language modification

The languages present in the Alcatel-Lucent OmniPCX Office Communication Server system are installed during manufacture. They depend on the hardware and key (licence) ordered. Four languages are available when there is an XMEM (memory expansion) or hard disk present, otherwise only two languages are available.

It is possible to modify the number and range of languages using the software downloading mechanism in OMC.

Note:
Language modification can also be performed during software downloading for migration to a new software version.

Procedure

To modify the range of languages available in the system, follow the procedure below:

1. Start the OMC software.
2. Select the **Tools** menu.
3. Select **Software Download**.
4. In the **Software Download** window, choose the desired version in **Delivery file** (V19_09, for example). You must choose a software version to be downloaded, usually the current software version already installed in the system so that only the languages will be loaded during the downloading.
5. Click **OK**.
6. Press the **Languages** button to display the **Languages** dialogue box, and then modify the order and/or choice of languages.
7. Click **OK**.
8. Select the **Data saving** box (if data saving is not performed, all customer data will be lost after the swap).
9. Click **Start**.
   The system downloads the different languages and corresponding voice prompts. The new languages will be available following the download, swap and system reset. All other configuration parameters will remain unchanged.

Note the following:

- The list of available language can be easily checked using customization mode ondedicated sets (menu Custom, option, language).
- The default language is always the first one in the list.
- During language downloading, the system does not check if the memory capacity is sufficient for the number of languages loaded; it is the responsibility of the installer to make sure the system configuration is appropriate for 4 languages (maximum).
- If the language selected for a particular subscriber is no longer present after downloading, silence will replace the missing language for that subscriber.

11.2 MMC Station

11.2.1 Accessing MMC

11.2.1.1 Overview

The Man-Machine Conversation (MMC) by 4034/Advanced station enables modifying parameters of the different system elements.

Note:

- Only a single 4034/Advanced station can be in MMC at a given moment
- Simultaneous access to the MMC by station and PC is impossible

Modifications are made in 2 ways:

- By introducing a numeric value (number of the station for example) or an alphanumeric value

- By choosing one of the predefined values presented on the display using the soft keys

11.2.1.1.1 ACCESS TO THE MMC

Access to the MMC is enabled by:

- Entering the code 70 (by default), or by using a key programmed with this code, or by pressing the SYSTEM key (Advanced station)
- Selecting one session among the following three sessions: INSTALLER (INSTAL key), ADMINISTRATOR (ADMIN key), or OPERATOR* (OPERAT key). These different levels of access to the configurable features enable modification to be authorized to specific individuals
- Entering the password corresponding to the selected session

Note:

** Only Installer and Administrator sessions are presented in this notice; for the Operator session, refer to the Installation guide.*

Password default values

INSTALLER session	pbxk1064
ADMINISTRATOR session	kilo1987

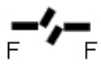
11.2.1.1.2 CONFIGURABLE FEATURES

All the configurable features in the Installer session are described in the different files contained in the current guide. The features and sub-features available in the Administrator session are indicated by the symbol  positioned beside the titles of the configurable elements.

Each feature has a diagram describing the entry procedure (in Installer session). The features which are accessible by soft keys are indicated by:

- SUBSCR: for moving through the MMC tree or for choosing a feature
- CHOICE: gives access to the drop down menu

Quitting the session

To quit the MMC session press the  key (4034 station) or the  key (Advanced station). You will quit the session automatically, after a time delay when the last key is pressed.

11.2.1.1.3 GENERAL COMMANDS

Soft keys

- ADD: adds an item to a list
- GOTO: moves quickly through a list
- READ+: displays the next page

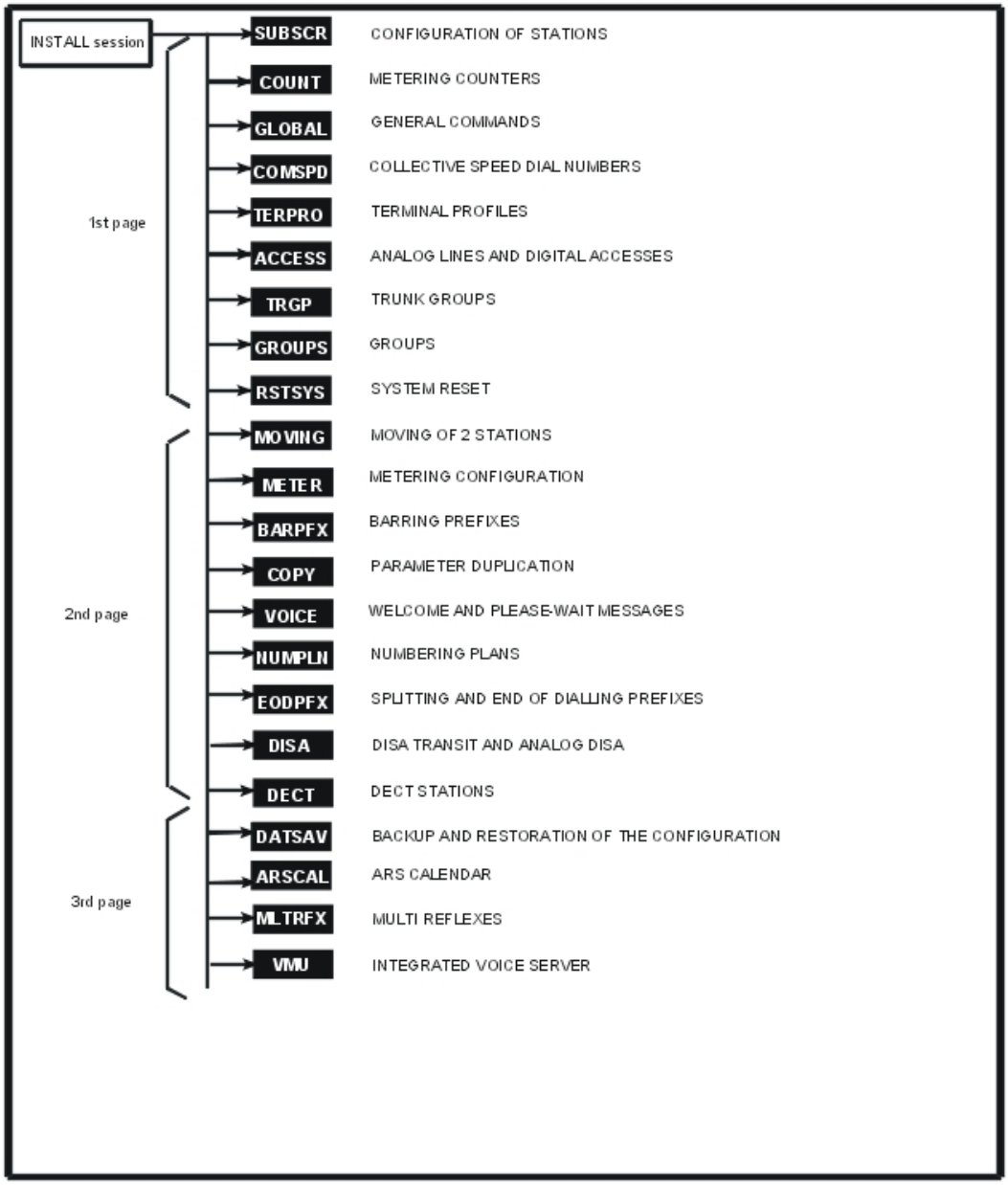
- CLEAR: cancels
- RUBOUT: corrects the last character
- MODIFY: modifies an item in a list
- NEXT: next entry in a list
- PREV: previous entry in a list
- BACK: returns to previous menu
- Valide: validates an entry
- -> : forward cursor movement
- <- : backward cursor movement

Using the alphabetic keypad

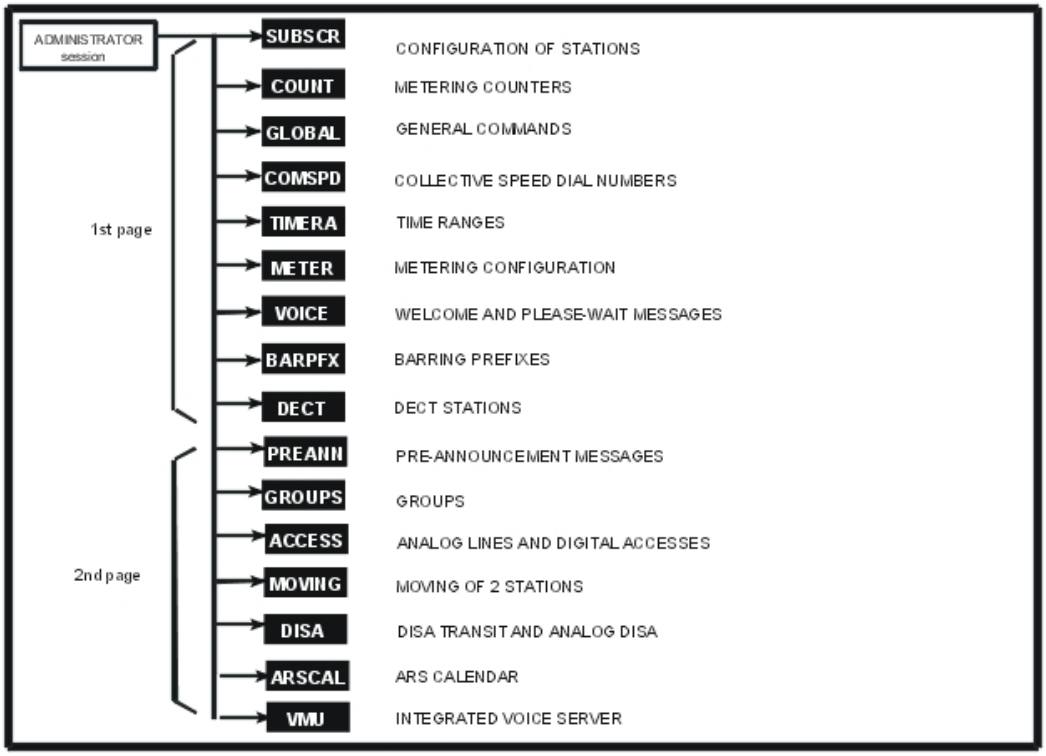
Each time you need to enter a name or a label associated to a key or a feature, use the alphabetic keypad. If the station does not have an alphabetic keypad, use the dialing keypad. To enter a letter, press the key which has the required letter on it: once for the first letter, twice for the second and three times for the third. To enter two consecutive letters on the same dialing key, press -> before entering the second letter. Entering special characters:

- "space': press **1**
- "-" : press **1** twice
- "." : press **1** three times
- "#' : press #
- ":" : press # twice
- "=" : press # three times
- "*" : press *****
- "+' : press ***** twice
- "/' : press ***** three times
- "0" to "9": press #**0** or #**9**

11.2.1.1.4 CONFIGURABLE FEATURES IN INSTALLER SESSION



11.2.1.1.5 CONFIGURABLE FEATURES IN ADMINISTRATOR SESSION

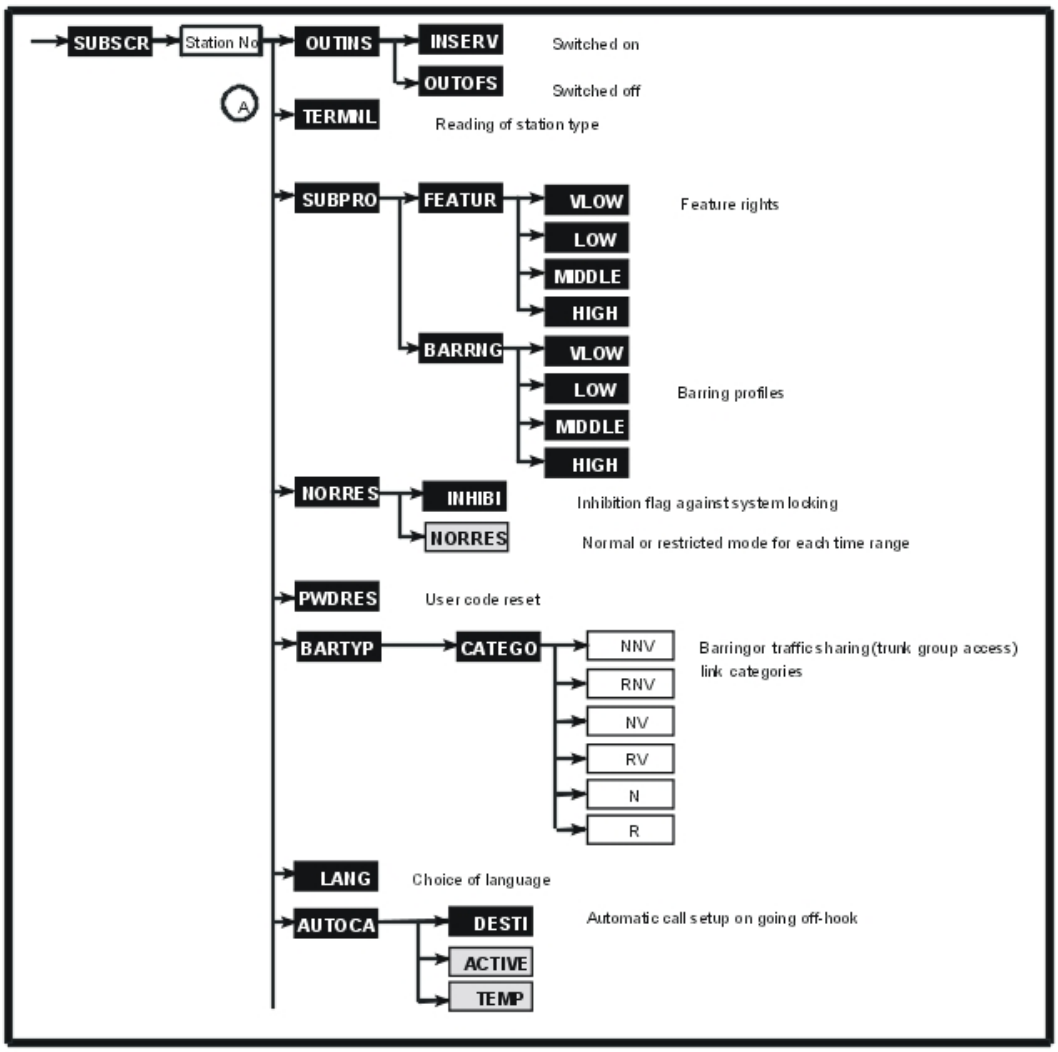


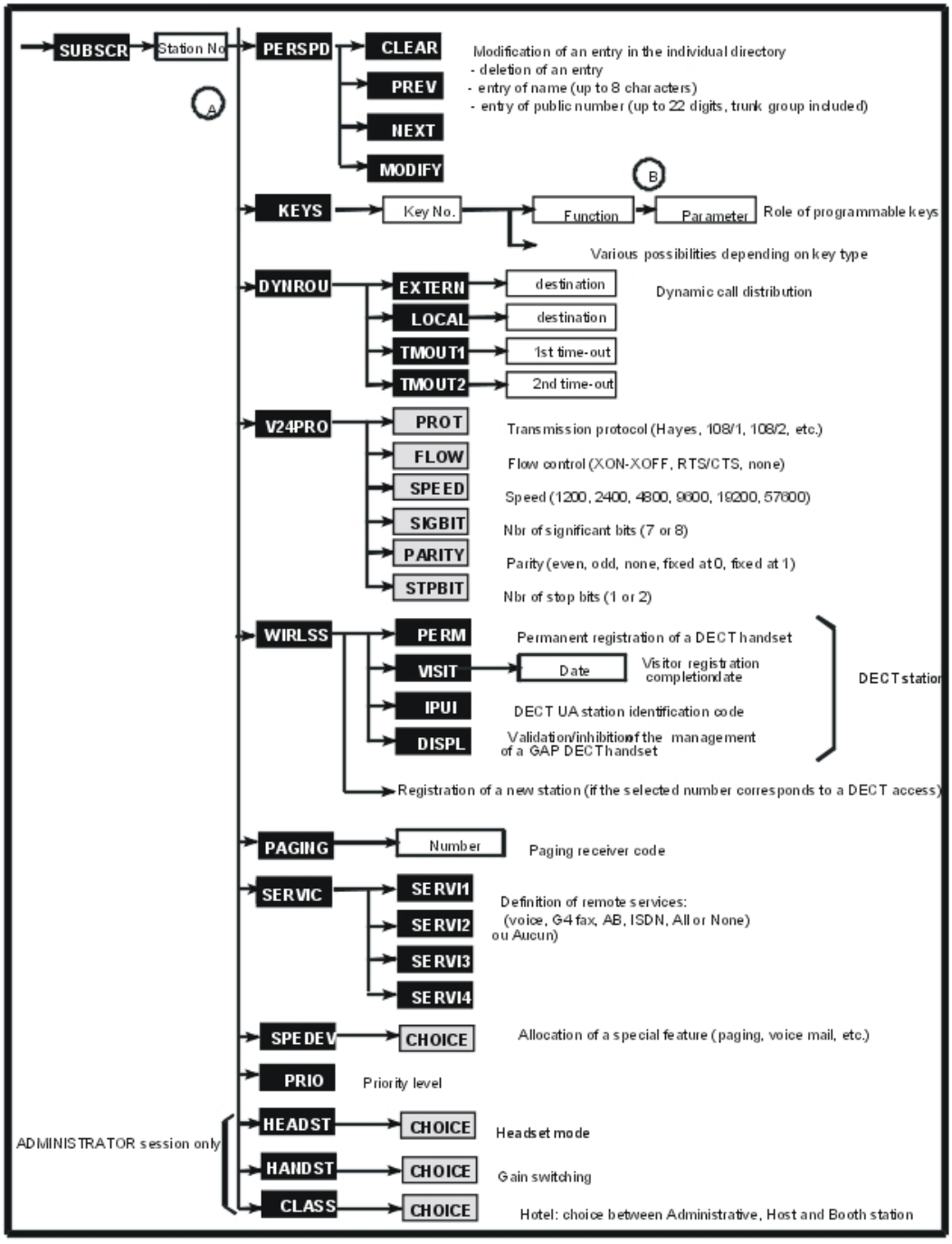
Note:
The TIMERA and PREANN features are no longer offered on a R2.0 system's MMC station.

11.2.2 Configuring Stations

11.2.2.1 Configuration procedure

This feature makes it possible to define particular characteristics for each station.


SUBSCR
Station No
A
OUTINS
INSERV
Switched on
OUTOFS
Switched off
TERMNL
Reading of station type
SUBPRO
FEATUR
VLOW
LOW
MIDDLE
HIGH
Feature rights
BARRNG
VLOW
LOW
MIDDLE
HIGH
Barring profiles
NORRES
INHIBI
Inhibition flag against system locking
NORRES
Normal or restricted mode for each time range
PWDRES
User code reset
BARTYP
CATEGO
NNV
RNV
NV
RV
N
R
Barring or traffic sharing (trunk group access) link categories
LANG
Choice of language
AUTOCA
DESTI
ACTIVE
TEMP
Automatic call setup on going off-hook



Press SUBSCR.

Enter the directory number of the station concerned.

11.2.2.1.1 STATUS OF THE STATION - OUTINS A

Before allocating a terminal profile or carrying out a remote customisation of a station, this station must be switched off by pressing OUTINS Ⓐ . After assignment, the station can be switched on again.

The station can be:

- In Service
- Logical OOS
- Physical OOS/Logical OOS: station not operational
- Physical OOS/Logical OOS: station not regarded by the system (not declared or disconnected) and switched on by the installer

Choosing INSERV + validation switches the station ON (IN SERVICE). Choosing OUTOFS + validation switches the station OFF (OUT OF SERVICE).

Note:

The Administrator session only allows the status of the station to be read.

11.2.2.1.2 TYPE OF STATION USED - TERMNL Ⓐ

Press TERMNL Ⓐ .

The station directory number, type and software version are displayed.

11.2.2.1.3 SUBSCRIBER PROFILE - SUBPRO Ⓐ

Feature rights profile - FEATUR Ⓐ

Press SUBPRO then FEATUR.

Choose the feature rights to be assigned to the station.

FEATURE RIGHTS	**VERY LOW**	**LOW (default)**	**MIDDLE**	**HIGH**
Authorised camp-on		YES	YES	YES
Protection against camp-on	--	--	--	--
Authorised barge-in (intrusion)	--	--	YES	YES
Protection against barge-in (station busy) and protection against interphone (station free)	--	--	YES	YES
Protection against camp-on tone	--	--	--	YES
Conference	--	YES	YES	YES
Automatic callback	YES	YES	YES	YES
Call pickup authorised	--	YES	YES	YES
Paging	--	--	YES	YES
Calling line identity masked	--	--	--	YES
UUS reception authorised	--	--	YES	YES

Restricted mode inhibited (no longer exists in R2.0)	--	--	--	--
Private station	--	--	--	--
VM = automated attendant dyn. forward level 1	--	--	--	--
VM = automated attendant dyn. forward level 2	--	--	--	--
Name display	YES	YES	YES	YES
External accesses joining by transfer	--	--	--	--
Trunk access by transfer	YES	YES	YES	YES
Selective forwarding	--	YES	YES	YES
External forwarding	--	--	--	--
Trunk line assignment	--	--	--	--
DISA Transit	--	--	--	--
Protection against DDC calls	--	--	--	--
Automatic call set-up on going off hook (immediate or after time-out)	--	--	--	--
DND override authorised	--	--	--	YES
Protection against DND override	--	--	YES	YES
Assign authorisation for cost (hotel: possibility of charging costs to a room telephone)	--	--	--	--

Barring profile - BARRNG Ⓐ

Press SUBPRO Ⓐ then BARRNG.

Choose the restriction profile to be assigned to the station.

CONTENT		**VERY LOW**	**LOW (default)**	**MIDDLE**	**HIGH**
Traffic sharing (access to trunk groups)	Normal mode	No trunk group	Main trunk group	Main and even trunk groups	All trunk groups
	Restricted mode	No trunk group	No trunk group	Main trunk group	All trunk groups
Station traffic sharing	Normal mode (N)	16	12	8	4
	Restricted mode (R)	16	16	12	4

Restriction level of trunk groups (result from the barring matrix with station restriction below and trunk group restriction by default)	Trunk groups 1 to 9, 50 to 57 and 98 to 105	1	2	3	4
	Trunk groups 10 to 17, 58 to 65 and 106 to 113	2	3	4	5
	Trunk groups 18 to 25, 66 to 73 and 114 to 120	3	4	5	6
	Trunk groups 26 to 33 and 74 to 81	4	5	6	1
	Trunk groups 34 to 41 and 82 to 89	5	6	1	2
	Trunk groups 42 to 49 and 90 to 97	6	1	2	3
Station restriction (voice or data)	Normal mode (NV and NNV)	1	2	3	4
	Restricted mode (RV and RNV)	1	1	1	4
Station speed dial rights (voice or data)	Normal mode	10000000	11100000	11111000	11111111
	Restricted mode	10000000	11100000	11111000	11111111

11.2.2.1.4 NORMAL/RESTRICTED MODE FOR EACH STATION - NORRES A

Note:
This function is no longer offered on a R2.0 system's MMC station.

NORRES (A) is used to define the time range operating mode.

INHIBI makes it possible to inhibit the switch to restricted mode. By successively pressing on CHOICE key, you can define whether changing the operating mode by operator command, or by a key at central processing level, is taken into account for this station:

NORRES: by successively pressing this key, you can choose the operating mode for the time range concerned:

- inhibited: changing the operating mode is not possible for this station
- possible: changing the operating mode is possible

11.2.2.1.5 REINITIALIZATION OF THE USER CODE - PWDRES A

Press PWDRES (A). Validating makes it possible to return to the default value for the password of the station concerned: 1515

11.2.2.1.6 BARRING AND TRAFFIC SHARING CATEGORIES - BARTYP A

BARTYP (A) makes it possible to define barring and traffic sharing link categories for each station.

NNV : restriction link COS for data calls in normal mode

RNV : restriction link COS for data calls in restricted mode

NV : restriction link COS for voice calls in normal mode

RV : barring link category for voice communications in restricted mode

N: traffic sharing link COS in normal mode

R: traffic sharing link COS in restricted mode

Note:

Restriction link COS make it possible to define the controls carried out during a trunk seizure by a means other than the system speed dial numbers or during the seizure of a trunk group. Traffic sharing link COS define the controls for accessing the trunk groups (outgoing traffic sharing).

After pressing CATEGO, enter the value (from 1 to 16) to be allocated to the category concerned, then validate.

11.2.2.1.7 CHOICE OF LANGUAGE - LANG A

After pressing LANG (A), choose the display language for the station from the proposed languages.

11.2.2.1.8 AUTOMATIC CALL SET-UP ON GOING OFF-HOOK - AUTOCA A

AUTOCA (A) makes it possible to define:

- the destination of an automatic call set-up on going off-hook
- call type: immediate or after a timeout

DESTI: enter the destination of an automatic call (station's directory or hunting group number or external number using a speed dial number).

ACTIVE: by successively pressing this key, you can define whether the automatic call is active (YES) or inactive (NO) for the station concerned.

TEMP: by successively pressing this key, you can define whether the automatic call is after a timeout (YES) or not (NO).

11.2.2.1.9 PERSONAL SPEED DIAL NUMBERS - PERSPD

PERSPD (A) makes it possible to create/modify the name and number stored in an entry in the individual directory of the station concerned (the complete entry of an entry with the line or trunk group used and sub-address is only possible through OMC).

PREV and NEXT make it possible to select a personal directory entry (01 to 30 for a 4034/Advanced station, 01 to 15 for 4023 stations and 01 to 10 for other stations). If this entry is already configured, the name and associated public number (last 18 digits) are displayed.

MODIFY makes it possible to modify the data stored in a directory entry.

Enter the name (up to 8 characters) and press OK. Then enter the public number (up to 22 digits, including the trunk group number) and press OK.

NUMBER makes it possible to erase ALL the data of a directory entry (even those that cannot be configured in this session).

11.2.2.1.10 ROLE OF THE PROGRAMMABLE KEYS - KEYS (A)

KEYS (A) makes it possible to define the role of the programmable keys.

Note 1:

Before performing the remote customisation of a station, the station must be switched off. It is advisable to cancel a key's current configuration before beginning a new configuration.

The display may show:

- the number (for example 01/98)
- the type of key (for example RGM)
- the rights associated with it (INS = installer)
- the current feature
- possible parameter(s)

State the number of the key to be programmed (see location below) by pressing ALLERA (GOTO) or by selecting the next or previous key.

UPDATE makes it possible to show the display which groups together all the functions offered. (B) . Press the soft key corresponding to the list which contains the desired function.

Function list

Choosing CALL (B)

KEY	FUNCTION	PARAMETERS
?Cback	Automatic callback request	--
¦Cback	Cancellation of an automatic callback request	--
ProCom	Protection of a call against any barge-in (intrusion)	--
Barge-in or Intrusion	Barge-in	--
Pgpfix	Paging call by prefix	--
PgaGen	Paging call by suffix	--
CLIR	Calling Line Identification Restriction (CLIR)	--
BMdial	Block mode dialling	--
SubAdd	Sub-address (ISDN)	--
DNDovr	Override DND/Priority call	--

Choosing ABBNUM (B)

KEY	FUNCTION	PARAMETERS
Redial	Redial last number	--
TmpRep	Putting a number into a temporary memory	--
PerSpD	Access to personal speed dial numbers	--
Call	Direct internal or external call	Trunk number External number (22 digits maximum) Sub-address (4 digits maximum)
Dir	Directory access	--
Macro1	Internal call + interphone barge-in on free; equivalent to an incoming RSL	Station directory number Data for dynamic routing
Macro2	External call + business account code + business account code value	Trunk number External number (22 digits maximum) Sub-address (4 digits maximum) Business account code (16 digits maximum)
Macro3	Calibrated loopbreak + time-out + number	Number to be transmitted after the calibrated loop break
PrCall	Priority calls	--

Choosing ANSWER (B)

KEY	FUNCTION	PARAMETERS
IndPic	Individual call pickup	Station directory number
GrpPic	Pickup group	--
GenBel	Unassigned night answer	--
Track or Monit	Selective monitoring	Station directory number (internal or DID numbers) Type of calls tracked (internal, external, all)
SubMon	Subscriber monitoring	Station directory number (internal or DID numbers) Type of calls tracked (internal, external, all)
GrpSup	General tracking	Hunt group number
AutAns	Auto-answer mode (intercom mode)	--
Ring	Supervised call ringing	--
Pgasel	Paging call answer	--
PgaGen	General paging answer	--
GenMon	Group supervision	--
2ndCal	Consultation call (only for 4073 stations)	--

Choosing DIVERT (B)

KEY	FUNCTION	PARAMETERS
SelFwd	Selective forwarding	--
PCX?	PCX forwarding	--
IndFwd - Immed? - Busy? - Text? - Follo? - Page? - DND	Access to personal call forwarding Immediate call forwarding Forward on busy Forwarding to text mail Follow-me Forwarding to paging "Do Not Disturb"	Internal or external destination Internal or external destination -- Number of the station concerned -- --
GrpFwd - Immed? - GrpWd	Group forwarding Immediate group call forwarding Disconnect from group (unavailable)	-- -- Station number
MstFwd - M ImmD - M Busy - M Grp	Master forwarding keys Immediate call forwarding Forward on busy Immediate forwarding of group calls	Internal destination Number of the station or group Number of the station or group
ScrMgr	Screening	Directory number of the secretary station
ScrSec	Screening	Directory number of the manager station
DelAll	Cancel all forwardings	--

Choosing OPTION (B)

KEY	FUNCTION	PARAMETERS
?Conf	Conference	--
AccCom	Modification of the business account code during the call	Value of the code (16 digits maximum)
AccOut	Business account code entered before new outgoing call	Value of the code (16 digits maximum)
Mail K	Access to text mail	--
Read +	Display next screen	--
MV	Access voice mail	Number of the voice mailbox
?PBX	Calibrated loop	--
NRMode	Normal or restricted mode for attendant	--
Reserv	Trunk group reservation for attendant	--
Prog	Programming mode	--
Hold	Common hold for voice transfer	--
Transf	Transfer of a call	--
Digits	Putting dialling into a memory	--
Mail L	Access to mailing	--

?DTMF	Send MF code	Digits (22 max) to be sent in MF
Forced	Interphone barge-in (intrusion) on free	--
Lock	Station lock/unlock	--
Park	Call parking/retrieval	--
MTR	COUNT (METER) TOTAL RECALL	--
AssgnN or AllotN	Trunk line assignment	Barring level
AssgnM or AllotM	Allocation of a line with total meter recall	Barring level
AttDiv	External forwarding of attendant calls	Internal or external destination
BkgMus	To choose the emitting source of please wait message	--
Door	Door opener control	--
Broker	Broker call (only for 4073 station)	--
RecCal	Recording of conversations	--
MVScrn	Screening of vocal messages	--

Choosing RESOU (B)

KEY	FUNCTION	PARAMETERS
RGI	Handles internal incoming calls	Call type: internal, external, all Data for dynamic routing
RGO	Handles internal outgoing calls	Call type: internal, external, all
RGM	Handles mixed calls (incoming-outgoing)	Call type: internal, external, all Data for dynamic routing
RSL	Handles internal calls with a specific station	Station directory number (4 digits max) Sub-address (4 digits maximum) Data for dynamic routing
RSD	Reception of internal or external calls Outgoing seizure on a given trunk	Station directory number or hunt group directory number (internal call) or DID (external call) Trunk directory number or ARS for outgoing call (optional) Data for dynamic routing
RSB	Set-up of an external call on a specific trunk group and reception of external call	Trunk directory number or ARS Data for dynamic routing
RSP	Reception and transmission of calls on a specific external interface	Line number Data for dynamic routing
SUP	Station tracking	Tracked station directory number Tracked resource key address

PARAMETERS ASSOCIATED WITH RESOURCE KEYS

Note 2:

This paragraph only describes the main parameters which can be defined according to the role assigned to the key; other parameters are possible (trunk number if RSD or RSB, station sub-address if RSL, type of tracking key and number of the tracking key if RSP).

? Dynamic routing

This sub-function is only provided for the MACRO1, RGI, RGM, RSL, RSD, RSB and RSP keys. DYNDYN makes it possible to define the data necessary for the dynamic routing of calls managed by the key concerned. Press UPDATE:

- TP1: by successively pressing this key, you can define whether the timeout 1 is active (TP1) or inactive (tp1)
- TP2: by successively pressing this key, you can define whether the timeout 2 is active (TP2) or inactive (tp2)
- OPERAT or GENBELL : by successively pressing this key, define whether the system should route the call to the attendant and/or the general bell after the non-response time-out TP2 has lapsed (active = ATTD or GBEL; inactive = attd or gbel).
- DIVERT makes it possible to authorise (DIVE) or not (dive) forwarding for this key.
- NUMBER makes it possible to define a destination station (or group) for the dynamic routing in the case of no answer after a timeout TP1 (12 seconds by default).

? Type of call

This sub-function is only provided for the RGI, RGO and RGM keys.

CALLTYP makes it possible to determine the type of calls managed by the key concerned.

By successively pressing on the CALLTYP key, you can choose between Ext/Loc, External and Local.

? Number of the associated station

This sub-function is only provided for the RSL, RSD and SUP keys. NUMBER makes it possible to define the directory number of the associated station.

11.2.2.1.11 DYNAMIC ROUTING OF CALLS - DYNROU A

Dynamic routing of calls makes it impossible to have a call (internal, external, private, etc.) remaining unanswered.

Press DYNROU (A).

EXTERN and LOCAL make it possible to define whether the dynamic distribution (timeouts T1 and T2, destinations) criteria for each type of call (external or local) are active or not:

- NUMBER makes it possible to define a destination station (or group) for the dynamic routing in the case of no answer after a timeout TP1 (12 seconds by default).
- TP1: by successively pressing this key, you can define whether the timeout 1 is active (TP1) or inactive (tp1).
- TP2: by successively pressing this key, you can define whether the timeout 2 is active (TP2) or inactive (tp2).
- OPERAT or GENBELL : by successively pressing this key, define whether the system should route the call to the attendant and/or the general bell after the non-response

time-out TP2 has lapsed (active = ATTD or GBEL; inactive = attd or gbel).

- DIVERT makes it possible to authorise (DIVE) or not (dive) forwarding for this key.

TMOUT1 and TMOUT2 make it possible to define the timeouts in tenths of a second. The default value is 12 seconds.

11.2.2.1.12 CHARACTERISTICS OF THE V24 OUTPUT OF A DIGITAL STATION - V24PRO (A)

V24PRO (A) (when the selected station corresponds to a V24 interface) makes it possible to define the characteristics for the V24 option installed on a digital station.

PROT: by successively pressing this key, you can choose the transmission protocol: 108/1, 108/2, Hayes or Dec. auto (Hayes by default).

FLOW: by successively pressing this key, you can choose the type of flow control: XON/XOFF, RTS/CTS or without (XON/XOFF by default).

SPEED: by successively pressing this key, you can choose the transmission speed: 1200, 2400, 4800, 9600, 19200 or 57600 bits/s (9600 bits/s by default).

SIGBIT: by successively pressing this key, you can choose the number of significant bits: 7 or 8 (8 by default).

PARITY: by successively pressing this key, you can choose the parity: 0, 1, even, uneven or no parity (no parity by default).

SERVI4: by successively pressing this key, you can choose the number of stop bits: 1 or 2 (1 by default).

11.2.2.1.13 CORDLESS DECT STATIONS - WIRLSS (A)

WIRLSS (A) (when the selected station is a DECT) makes it possible to define the parameters for DECT stations.

PERM makes it possible to select a permanent association with the system.

VISIT makes it possible to select a temporary association with the system; enter the date on which the mobile is to be automatically disconnected from the system and validate.

IPUI makes it possible to modify the IPUI value of the DECT station; enter 14 octal digits and validate.

DISPL makes it possible to validate or inhibit a GAP DECT display.

WIRLSS SERVI4 (when the selected number is a DECT access) allows registering of a new DECT station (UA or GAP).

11.2.2.1.14 PAGING NUMBER - PAGING (A)

PAGING SERVI4 makes it possible to define the number of the paging receiver for the station concerned.

11.2.2.1.15 REMOTE SERVICES - SERVIC (A)

SERVIC (A) makes it possible to define the remote service(s) accessible for the station

concerned (4 services maximum).

By successively pressing on SERVI1 to SERVI4 keys, select the authorised remote service:

- VOICE (telephone services)
- ALLSVC (all remote services)
- ABS (analog data service)
- FAX2/3
- FAX4
- V24AE (asynchronous V24)
- TLTX64 (64 kbits/s teletext)
- DATA64 (64 kbits/s data transmission)
- VIDEO
- X21
- X25
- Bdx
- BdxNw
- MixMod
- NOSERV

Only calls compatible with the services programmed are accepted for both outgoing and incoming calls. All other types of call are rejected and not presented when incoming. For non S0 stations, only service 1 is to be defined.

11.2.2.1.16 SPECIAL FEATURES - SPEDEV (A)

After pressing SPEDEV (A), by pressing successively on CHOICE, you can select features from those offered:

- Normal
- Paging
- Voice mail unit
- Doorphone
- Bank Alarm (priority call)
- Fix DTMF

11.2.2.1.17 PRIORITY LEVEL - PRIO

PRIO (A) makes it possible to define the priority level (0 to 7, 7 = highest level) for external calls (priority call feature).

11.2.2.1.18 FEATURES ONLY PROVIDED IN AN ADMINISTRATOR SESSION - HEADST, HANDST AND CLASS

Headset mode - HEADST

After pressing HEADST (A), by pressing successively on CHOICE, you can tell whether or not the station operates with a headset. If it does, plug the headset into the handset slot.

Gain improvement - HANDST

After pressing HANDST (A), by pressing successively on CHOICE, you can activate or cancel gain improvement on a station (improves hearing in noisy surroundings).

Hotel type telephone set - CLASS

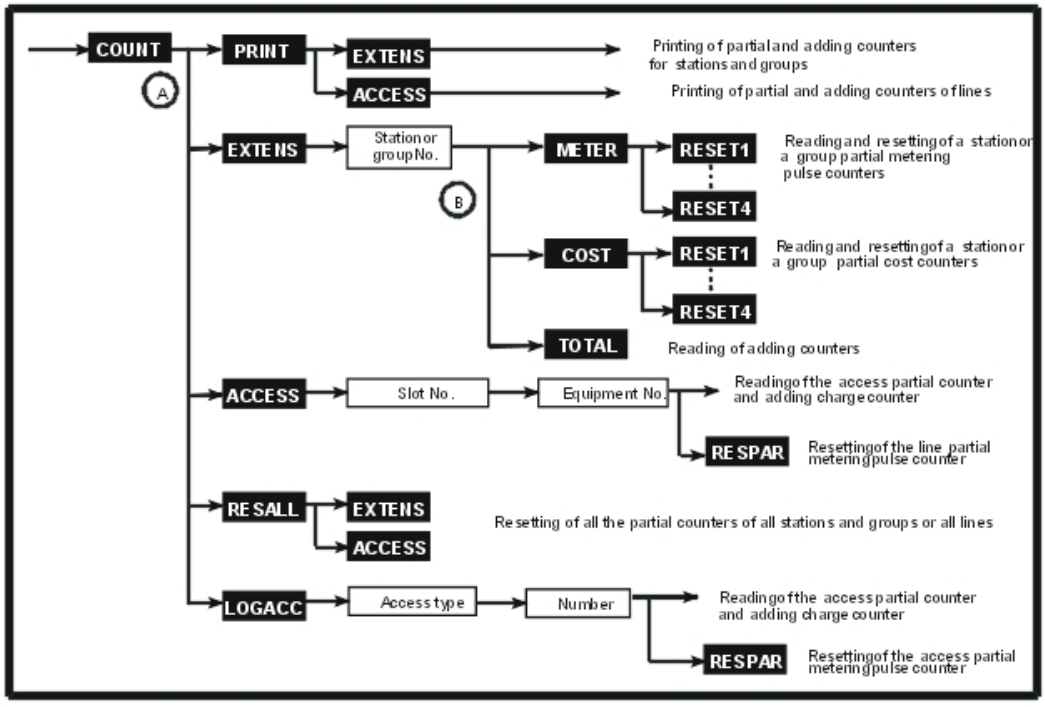
After pressing CLASS (A), by pressing successively on CHOICE, select between Administrative, Host and Booth station.

11.2.3 Metering Counters

11.2.3.1 Operation

The system sums up the following call detail information in the form of partial and total counters:

- For each station or group (stations or attendant stations):
  - 4 partial charge (signals) counters and 4 partial cost counters
  - 1 total charge (signals) counter and 1 total cost counter
- For each line:
  - 1 partial charge (signals) counter
  - 1 total cost counter



Press COUNT.

11.2.3.1.1 PRINTING OF STATION/GROUP AND LINE COUNTERS - PRINT (A)

Press PRINT (A).

EXTENS makes it possible to print the partial and adding counters for the stations and groups.

ACCESS makes it possible to print the partial and adding counters for the lines.

11.2.3.1.2 READING OF A STATION'S/GROUP'S COUNTERS - EXTENS (A)

After pressing EXTENS (A), enter the directory number of the station (or group) whose counter should be printed.

Reading and resetting of the meter pulse counters - METER (A)

METER (B) displays the contents of the 4 partial metering pulse counters for the station concerned.

RESET1 to RESET4 make it possible to reset the 4 counters individually.

Reading and resetting of the cost counters - COST (A)

COST (B) displays the contents of the 4 partial cost counters for the station (or group) concerned.

RESET1 to RESET4 make it possible to reset the 4 counters individually.

Readout of the adding counters - TOTAL (A)

TOTAL (B) displays the station adding and cost counter values.

11.2.3.1.3 READING AND RESETTING OF THE LINE COUNTERS (PHYSICAL ADDRESSES) - ACCESS

After pressing ACCESS (A), enter the data necessary for identification of the line whose partial and adding counters are to be displayed, validate.

Identification of interfaces:

- SLOT : slot number: 1 to 8 (basic module), 11 to 18 (extension module 1), 21 to 28 (extension module 2)
- EQUIP : equipment number: 1 to 8

The display then shows the values for the line counter signals and cost total counters.

RESPAR makes it possible to reset the line partial metering pulse counter.

11.2.3.1.4 RESETTING OF THE STATION/GROUP AND LINE PARTIAL COUNTERS - RESALL (A)

RESALL (A) makes it possible to reset all the partial counters for the stations or lines.

EXTENS makes it possible to reset all the station or group partial counters.

ACCESS makes it possible to reset all the line partial counters.

Note:

Only the station partial counters can be reset in Administrator session.

11.2.3.1.5 READING AND RESETTING OF THE LINE COUNTERS (LOGICAL ADDRESSES) - LOGACC

After pressing LOGACC (A), enter the data necessary for identification of the access (access number and type) for which the partial and adding counters are to be displayed and then validate.

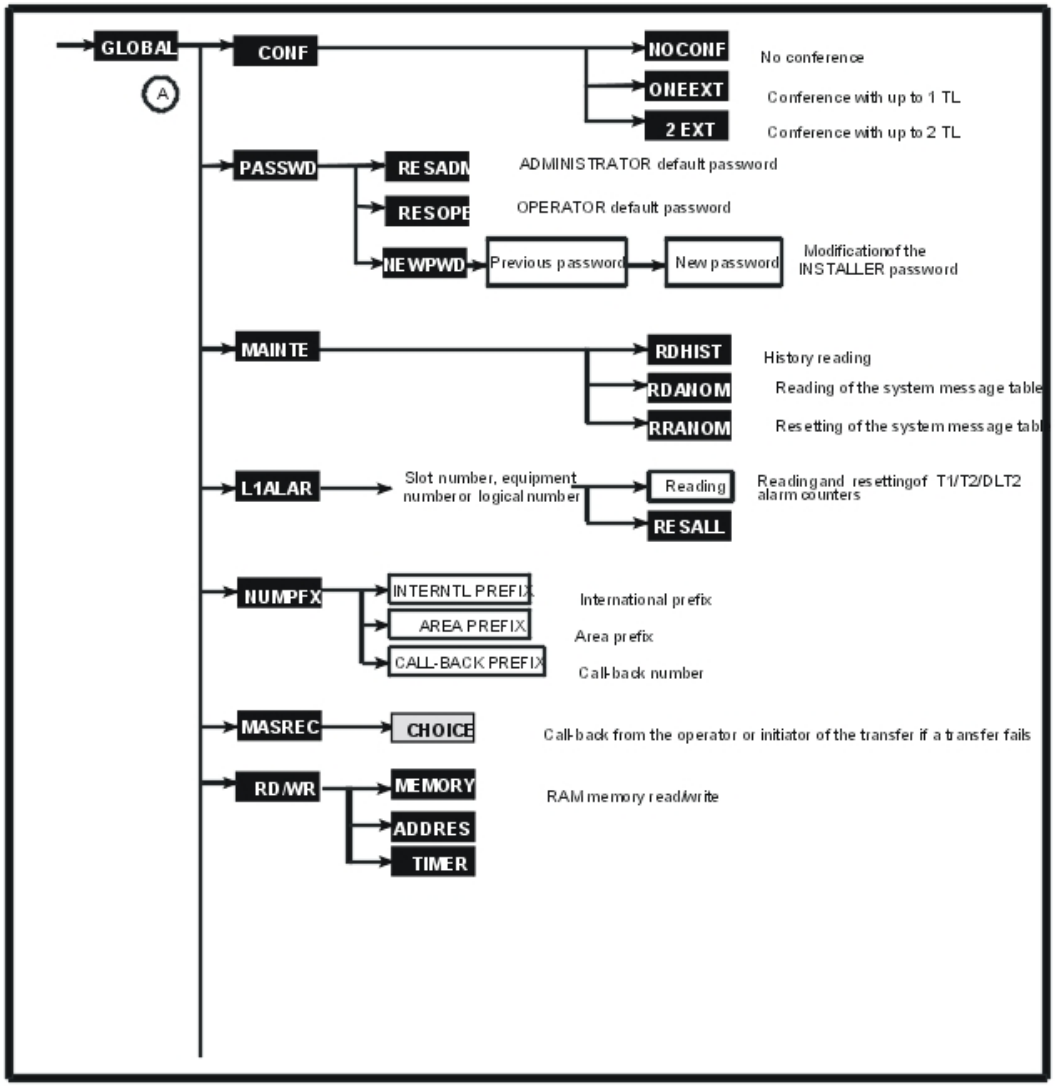
To enter the access type, press the L(AG) soft keys for a TL, N(T0) for a T0 access or P(T2) for a T2/DLT2 access. The display then shows the values for the line partial and total counters.

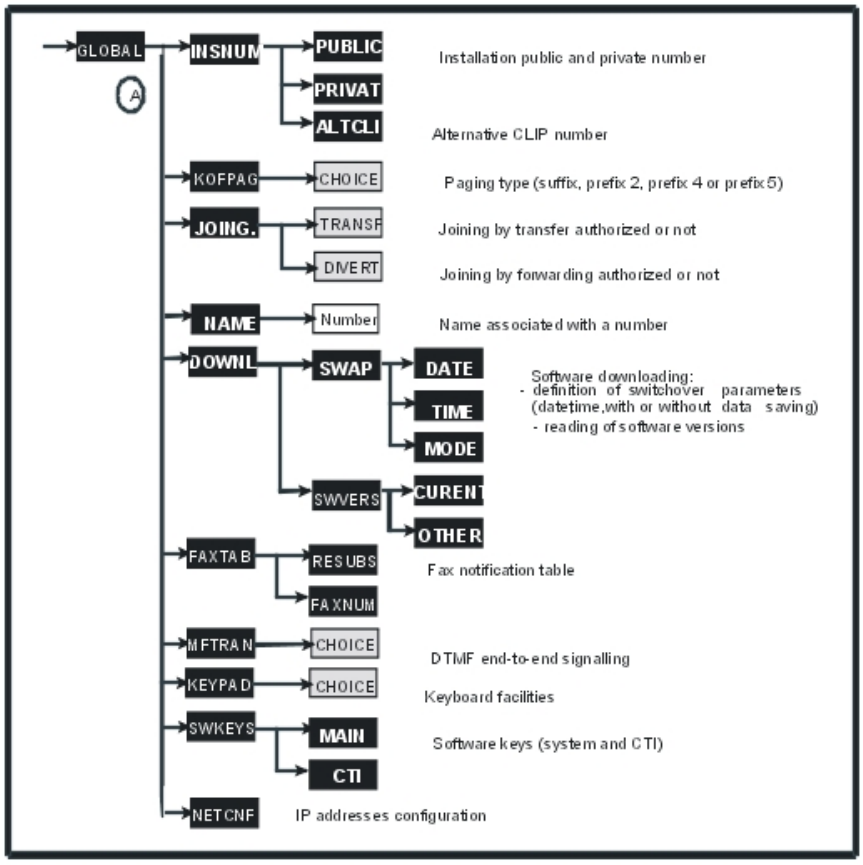
RESPAR makes it possible to reset the line partial metering pulse counter.

11.2.4 General Commands

11.2.4.1 Operation

This feature is used for defining general items which are common to the whole system.


GLOBAL
A
CONF
NOCONF
No conference
ONEEXT
Conference with up to 1 TL
2 EXT
Conference with up to 2 TL
PASSWD
RESADM
ADMINISTRATOR default password
RESOPE
OPERATOR default password
NEWPWD
Previous password
New password
Modificationof the INSTALLER password
MAINTE
RDHIST
History reading
RDANOM
Reading of the system message table
RRANOM
L1ALAR
Slot number, equipment numberor logical number
Reading
Readingand resettingof T1/T2/DLT2 alarm counters
RESALL
NUMPFX
INTERNTL PREFIX
International prefix
AREA PREFIX
Area prefix
CALL-BACK PREFIX
Call-back number
MASREC
CHOICE
Call-back from the operator or initiator of the transfer if a transfer fails
RD/WR
MEMORY
RAM memory read/write
ADDRES
TIMER



Press GLOBAL.

11.2.4.1.1 CHOICE OF THE TYPE OF CONFERENCE - CONF A

After pressing CONF (A), choose the conference operating mode (no conference, with one external line, with 2 external lines); by default: with one external line.

11.2.4.1.2 PASSWORDS - PASSWD A

Press PASSWD (A).

Reinitializations of the passwords - RESADM and RESOPE

The choices RESADM and RESOPE make it possible to return to the default password required for entering the ADMINISTRATOR and OPERATOR sessions.

Modification of the Installer password - NEWPWD

NEWPWD makes it possible to change the INSTALLER password.

Enter the current password (8 characters).

Enter the new password (8 characters).

Confirm the password by entering it a second time.

Note:

In the Administrator session, only the password of the current sessions can be modified, that of a lower level may be reinitialized.

11.2.4.1.3 HISTORY AND EQUIPMENT MESSAGES - MAINTE (A)

Press MAINTE (A).

RDHIST makes it possible to read the history message table.

RDANOM makes it possible to read the hardware messages.

RRANOM makes it possible to reset the system messages table.

Note:

For more details regarding the messages, refer to the Maintenance guide.

11.2.4.1.4 T1/T2/DLT2 ALARM COUNTERS- L1ALAR (A)

L1ALAR (A) makes it possible to read and reset the T1/T2/DLT2 alarm counters. Select the link (slot number + equipment number or logical number).

- MS : : No 2 Mbits Signal
- RRA: : Receive Remote Alarm
- AIS : Alarm Indication Signal
- PVT : Loss of Synchronization
- TE : Error rate
- LV1: : Level 1 unavailable
- LV2: : Level 2 unavailable

RESALL makes it possible to reset all the counters.

11.2.4.1.5 DIALING PREFIXES - NUMPFX

Press NUMPFX (A).

1st display: enter the international prefix, validate.

2nd display: enter the area prefix, validate.

3rd display: enter the callback prefix (4 digits max, number of trunk group used to make an outgoing call from the directory of callers), validate.

11.2.4.1.6 REACTION ON TRANSFER FAILURE - MASREC

Press MASREC (A).

By successively pressing on keys CHOICE, you can choose the destination set to which the call will be routed when a transfer fails: ATTENDANT RECALL or MASTER RECALL (initiator of the transfer).

11.2.4.1.7 READ/WRITE IN MEMORY - RD/WR

RD/WR (A) makes it possible to read and modify the contents of the labeled addresses in the system RAM memory. Modification of these contents makes it possible to configure some system operations.

Entering a value at the incorrect address may result in deterioration of the system operation.

Write in memory - MEMORY

MEMORY makes it possible to modify the value of a labeled address. Enter the address (8 characters maximum) then validate.

Softkeys A, B, C, D, E and F are used to enter the hexadecimal address.

Read memory (except timers and maintenance and debug addresses) - ADDRES

ADDRESS makes it possible to read the contents of the system's labeled addresses, except for addresses which concern timers and maintenance and debug features.

ALLERA makes it possible to go to any index.

Reading the timers - TIMER

TIMER makes it possible to read the contents of the labeled addresses concerning the system timers.

11.2.4.1.8 INSTALLATION NUMBERS - INSNUM

INSNUM (A) makes it possible to define the Alternative CLIP number and the installation's public and private numbers.

PUBLIC: number up to 20 digits max, separators * not included; the * character separates the different fields: country indication, area number (optional field depending on country), PCX number. The size of the field depends on the country.

PRIVAT: number up to 10 digits max. without separators.

ALTCLI: Alternative CLIP number (20 digits max.). This number, if configured, is sent to the ISDN correspondent on an outgoing call in place of the installation number + DDI number of the calling party.

11.2.4.1.9 TYPE OF PAGING - KOFPAG

Press KOFPAG (A).

CHOICE: by successively pressing this key, you can define the operating mode for paging:

- suffix: paging connected to a trunk line interface; selective paging.
- prefix 2
- prefix 4: paging connected to a Z station interface; general paging
- prefix 5

11.2.4.1.10 JOINING - JOING

Press JOING (A).

TRANSP: by successively pressing this key, you can authorize or inhibit joining by transfer (transfer ext -ext).

DIVERT: by successively pressing this key, you can define the type of external forwarding: Joining or Rerouting.

11.2.4.1.11 DIRECTORY - NAME (A)

NAME (A) makes it possible to display all the names corresponding to a given number in the numbering plan, with the possibility of modifying these names.

MODIFY and ADD make it possible to modify/add a name; enter the user name (16 characters maximum) as "surname-space-first name" using the alphabetic keypad or the station's dialing keypad which will have automatically switched to "letters" mode.

11.2.4.1.12 DOWNLOADING - DOWNLD

Press DOWNLD (A).

SWAP makes it possible to configure the date, time and mode of the software swap:

DATE: swap date

TIME: swap time

MODE: swap mode; by pressing successively on CHOICE, define the swap operating mode:

- normal with data saving
- normal without data saving
- forced with data saving (no restoration of the old version in the case of a transfer failure).

SWVERS makes it possible to read the software references of the CPU board:

CURRENT: current CPU software reference

OTHER: new CPU software reference

11.2.4.1.13 FAX NOTIFICATION TABLE - FAXTAB

This 30-entry table defines the relationships between the user numbers to be notified by a message in an incoming fax which is intended for them and the number of the receiving fax machine.

Press FAXTAB (A).

RESUBS makes it possible to define the number of the set to call (sending a message saying that a fax has arrived).

FAXNUM makes it possible to define the number of the fax machine concerned.

11.2.4.1.14 DTMF END-TO-END SIGNALING - MFTRAN

Press MFTRAN (A).

CHOICE: by successively pressing this key, you can define whether the DTMF end-to-end signaling is applied overall for all users, for no user or whether the passage in DTMF end-to-end signaling is carried out individually for the sets.

11.2.4.1.15 KEYPAD DIALING FEATURES - KEYPAD

Press KEYPAD (A) .

CHOICE: by successively pressing this key, define whether the “Keyboard facilities” feature is activated or not in the system. For further information, refer to the “ISDN Services” of the “Telephone services” section.

11.2.4.1.16 SOFTWARE KEYS - SWKEYS

Press SWKEYS (A) .

MAIN makes it possible to configure the system software license.

CTI makes it possible to configure the CTI software license.

11.2.4.1.17 IP ADDRESSES - NetCNF

Press NETCNF .

This function makes it possible to read and change the following system elements" IP addresses:

- IP@CPU: IP address of the main CPU.
- IP@Rtr: default IP address of the router.
- IP@Msk: IP address of the sub-system mask.
- VoIP@: VoIP master IP addresses (VoIPm) and slaves (VoIPs1 to VoIPs5).

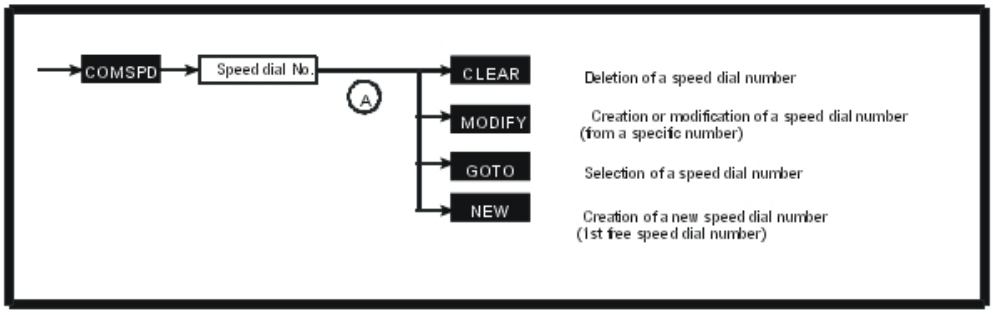
The system MUST be re booted for any IP address change to be incorporated.

11.2.5 Collective Speed Dial Numbers

11.2.5.1 Operation

The system makes it possible to create a general directory of 2000 numbers.

Each number can have 22 digits (trunk group number included).



Press COMSPD.

CLEAR makes it possible to delete the programming of a specific speed dial number.

MODIFY after pressing this key, enter the call recipient's name and validate; then enter the public number preceded by the trunk group number and validate.

Note:

*A "pause" (character **!**) or an "MF forcing" (character **/**) can be entered in the public number entry screen using the alphanumeric keyboard.*

GOTO provides direct access to a specific speed dial number; enter the call recipient's name or press the NUMBER key to provide access via the speed dial number, and then validate.

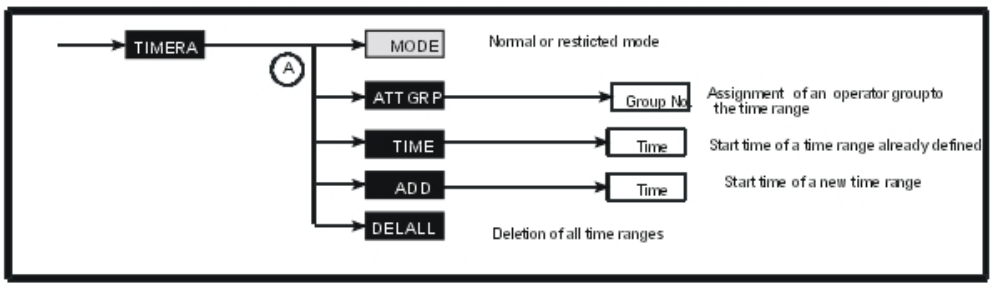
NEW: after this key is pressed, the first free entry in the directory is displayed; the procedure is then identical to the procedure provided by the MODIFY key.

11.2.6 Time Ranges

11.2.6.1 Operation

WARNING: This feature is no longer offered on a R2.0 system's MMC station.

This feature is used for dividing a day's 24 hours into a maximum of 7 time ranges defined by the starting time. Each range can be in normal or restricted mode. A group of a maximum of 8 attendant stations can be assigned to each time range. At least one time range must be defined in the system.



Press TIMERA.

MODE (A) : by successively pressing this key, you can choose the desired operating mode: normal or restricted.

ATTGRP (A) makes it possible to state the operator group number (1 to 8) assigned to the time range concerned.

TIME (A) makes it possible to enter the start time of the time range.

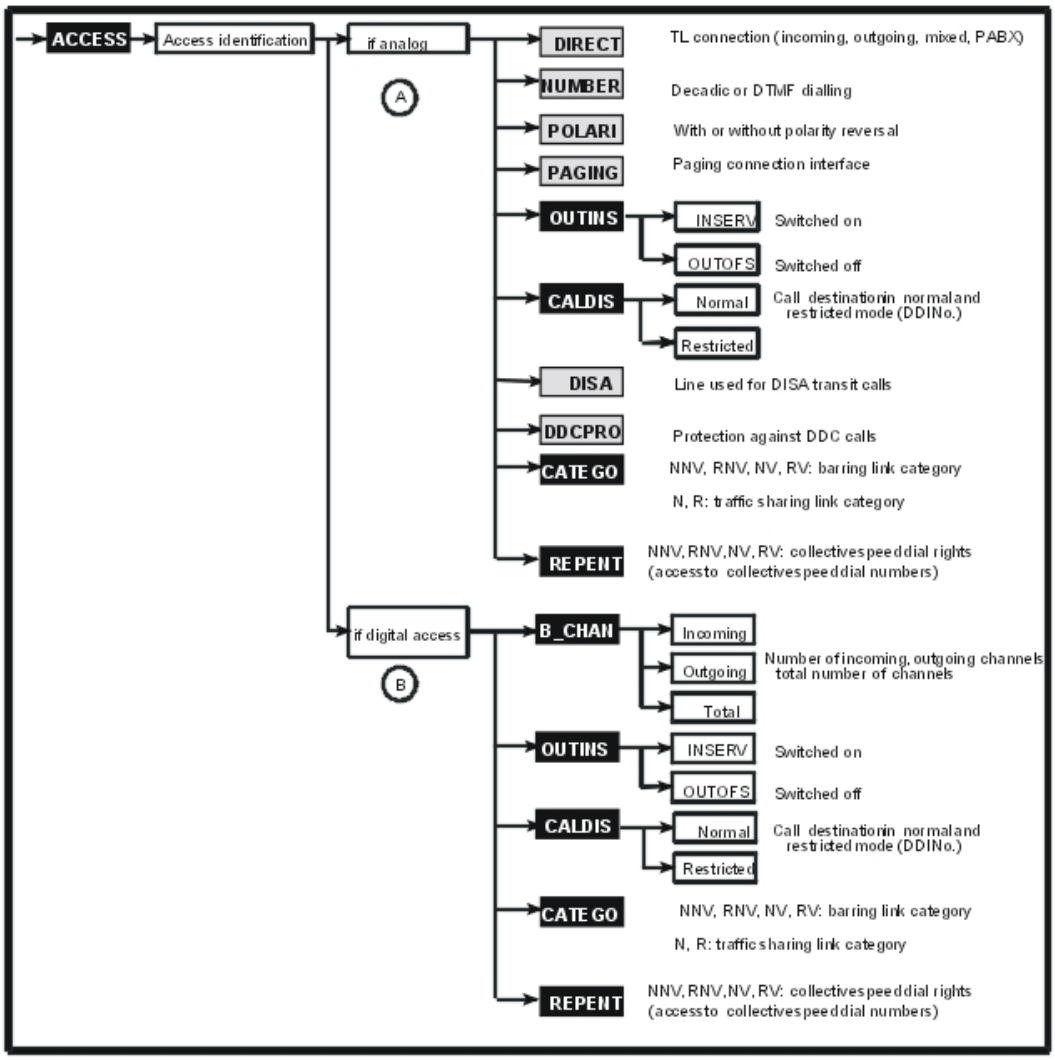
ADD (A) makes it possible to add a new time range (if less than 7).

DELALL (A) makes it possible to delete all time ranges.

11.2.7 Analog Lines and Digital Accesses

11.2.7.1 Operation

This function is used to define the properties of the analog lines (available from version R1.1 onwards) and T0/T2/DLT2 digital accesses.



Press ACCESS.

Enter the data necessary for identifying the access and validate:

Identification of interfaces:

- SLOT : slot number: 1 to 8 (basic module), 11 to 18 (extension module 1), 21 to 28 (extension module 2)
- EQUIP : equipment number: 1 to 8

11.2.7.1.1 ANALOG LINES (from version R1.1 onwards)

DIRECT (A) : by successively pressing this key, you can display the desired line connection mode:

- PBX: line behind PCX
- INC : incoming line
- OUT : outgoing line
- MIX : mixed line

NUMBER (A) : by successively pressing this key, you can display the desired dialing mode:

- DE : pulse dialing
- MF : MF dialing
- NO : no dialing

POLARI (A) : by successively pressing this key, you can display the desired characteristic:

- YES : with polarity reversal
- NO : without polarity reversal

PAGING (B) : by successively pressing this key, you can display the desired characteristic:

- YES : interface for connection of a paging device
- NO : TL interface

OUTINS (A) makes it possible to read the current access status: In Service, Out of Service, Physical OOS/Logical OOS or Physical OOS/Logical IS.

Choosing INSERV + OK sets the access to LOGICAL IN SERVICE.

Choosing OUTOFS + OK sets the access to PHYSICAL OUT OF SERVICE/LOGICAL OUT OF SERVICE.

(A) CALDIS (A) : enter the DDI number of the destination station or hunting group for calls in normal mode. A second similar display is presented indicating the destination for calls in restricted mode.

DISA (A) : by successively pressing this key, state whether the line can be used for DISA calls or not.

DDCPRO (A) : by successively pressing this key, it is possible to accept or refuse DDC calls when this line is used for a station external forwarding.

(A) CATEGO (A) makes it possible to define barring and traffic sharing link categories for each station.

NNV : restriction link COS for data calls in normal mode

RNV : restriction link COS for data calls in restricted mode

NV : restriction link COS for voice calls in normal mode

RV : barring link category for voice communications in restricted mode

N : traffic sharing link COS in normal mode

R : traffic sharing link COS in restricted mode

Enter a value from 1 to 16 to assign to the category concerned then validate.

A REPENT A makes it possible to define the collective speed dial numbers which can be transmitted on each trunk. For example, a trunk with category 10100000 may be used to transmit speed dial numbers in COS 1 and 3.

NV: speed dial rights link category for voice communications in normal mode

NNV: speed dial rights link category for data communications in normal mode

RV: speed dial rights link category for voice communications in restricted mode

RNV: speed dial rights link category for data communications in restricted mode

FEATUR: by successively pressing this key, you can define whether the station concerned has the right (1) or not (0) to access the chosen directory list (NV, NNV, RV, RNV), then validate.

11.2.7.1.2 DIGITAL ACCESSES

B_CHAN B : for T0/T2/DLT2 accesses, state the number of incoming (INC) or outgoing (OUT) channels as well as the total number of channels (value non modifiable for T0 access), then validate; the number of mixed (MIX) channels is deduced from the other data.

OUTINS A makes it possible to read the current access status: In Service, Out of Service, Physical OOS/Logical OOS or Physical OOS/Logical IS.

Choosing INSERV + OK sets the access to LOGICAL IN SERVICE.

Choosing OUTOFS + OK sets the access to PHYSICAL OUT OF SERVICE/LOGICAL OUT OF SERVICE.

A CALDIS A : enter the DDI number of the destination station or hunting group for calls in normal mode. A second similar display is presented indicating the destination for calls in restricted mode.

A CATEGO A makes it possible to define barring and traffic sharing link categories for each access.

NNV : restriction link COS for data calls in normal mode

RNV : restriction link COS for data calls in restricted mode

NV : restriction link COS for voice calls in normal mode

RV : barring link category for voice communications in restricted mode

N : traffic sharing link COS in normal mode

R : traffic sharing link COS in restricted mode

Enter a value from 1 to 16 to assign to the class of service concerned then validate.

A REPENT A makes it possible to define the collective speed dial numbers which can be

transmitted on each access. For example, an access with COS 10100000 may be used to transmit speed dial numbers in the speed dial rights and traffic sharing COS.

NV: speed dial rights link category for voice communications in normal mode

NNV: speed dial rights link category for data communications in normal mode

RV: speed dial rights link category for voice communications in restricted mode

RNV: speed dial rights link category for data communications in restricted mode

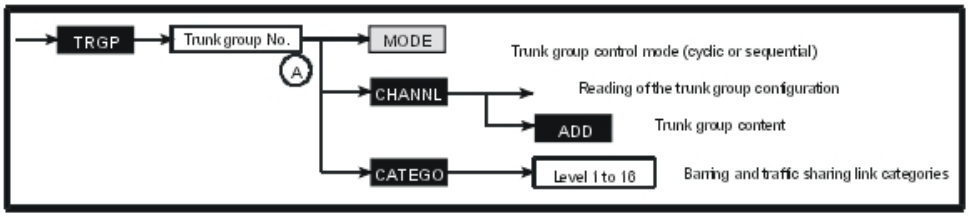
FEATUR: by successively pressing this key, you can define whether the station concerned has the right (1) or not (0) to access the chosen directory list (NV, NNV, RV, RNV), then validate.

11.2.8 Trunk Groups

11.2.8.1 Operation

It is possible to create 120 trunk groups with up to 120 lines in each trunk group.

Each trunk group is assigned restriction and traffic sharing link classes of service and a control mode (circular or serial).



Press TRGP.

Enter the trunk group number (1 to 120), and validate.

11.2.8.1.1 TRUNK GROUP CONTROL MODE - MODE

MODE (A) : by successively pressing on this key, you can choose the trunk group control mode: serial/sequential (SER/SEQ) or circular/cyclic (CIRCYC).

11.2.8.1.2 TRUNK GROUP CONFIGURATION - CHANNL

CHANNL (A) grants access to the trunk group configuration window.

ADD makes it possible to add a line (or an access) to the trunk group. Enter the data necessary for identification of the trunk group and validate:

Identification of interfaces:

- SLOT : slot number: 1 to 8 (basic module), 11 to 18 (extension module 1), 21 to 28 (extension module 2)
- EQUIP : equipment number: 1 to 8

11.2.8.1.3 RESTRICTION AND TRAFFIC SHARING CLASSES OF SERVICE - COS/CATEGO

CATEGO (A) makes it possible to define the barring and traffic sharing link categories for each trunk:

NNV : restriction link COS for data calls in normal mode

RNV : restriction link COS for data calls in restricted mode

NV : restriction link COS for voice calls in normal mode

RV : barring link category for voice communications in restricted mode

N : traffic sharing link COS in normal mode

R : traffic sharing link COS in restricted mode

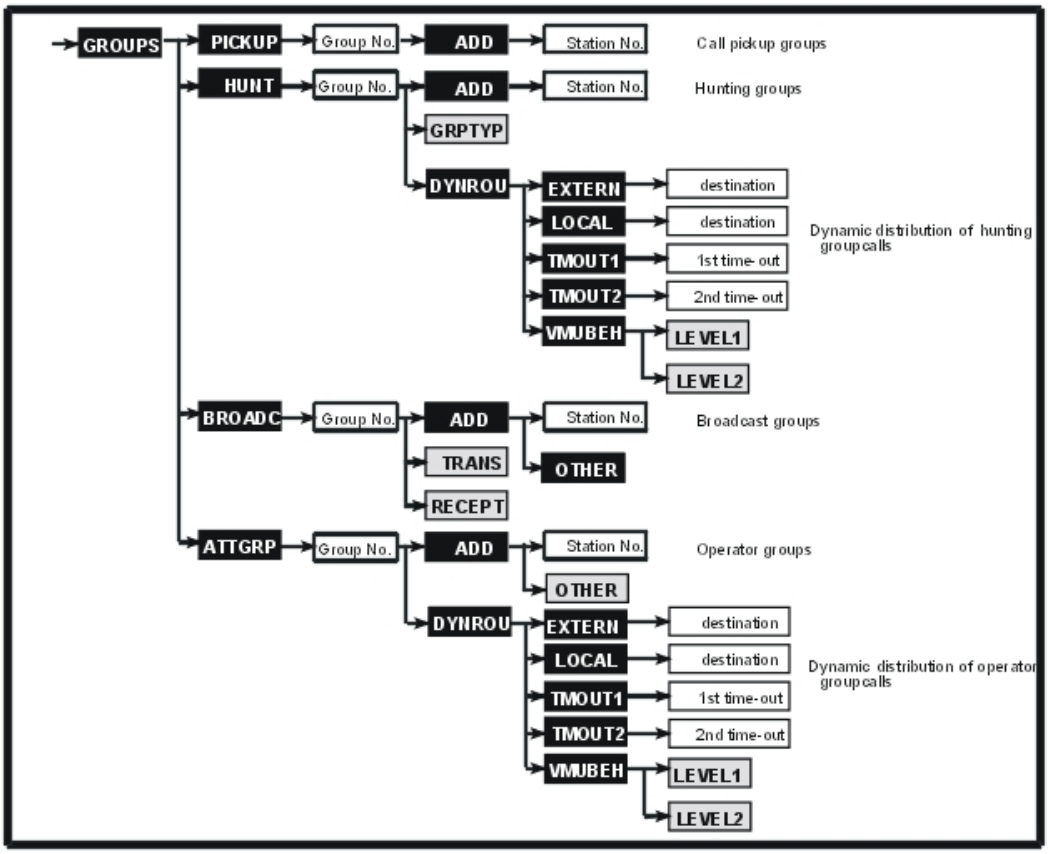
Enter a value from 1 to 16 to assign to the class of service concerned then validate.

11.2.9 Groups

11.2.9.1 Operation

This function is used to create:

- 50 hunt, call pickup or broadcast groups with up to 32 stations in each group.
- 8 groups of attendant stations with up to 8 stations in each group.



Press GROUPS.

11.2.9.1.1 CALL PICKUP GROUPS - PICKUP

After pressing PICKUP (A), enter the group index and validate. The directory number of the first station in the group is displayed.

ADD makes it possible to add a station directory number to the group. Enter the number of the station to be added to the group.

11.2.9.1.2 HUNT GROUPS - HUNT

After pressing HUNT (A), enter the hunting group directory number. The directory number of the first station in the group is displayed.

ADD makes it possible to add a station directory number to the group. Enter the number of the station to be added to the group.

GRPTYP: by successively pressing this key, you can choose the type of group: parallel, serial or circular then validate.

DYNROU makes it possible to define the dynamic routing mechanisms for hunting group calls:

- EXTERN and LOCAL make it possible to define whether the dynamic distribution (time-outs T1 and T2, destinations) criteria for each type of call (external or local) are active or not:
  - NUMBER makes it possible to define a destination station (or hunting group) or a collective speed dial number for the dynamic routing in the case where the call has not been answered after a time-out TP1 (12 seconds by default).
  - TP1: by successively pressing this key, you can define whether the time-out 1 is active (TP1) or inactive (tp1).
  - TP2: by successively pressing this key, you can define whether the time-out 2 is active (TP2) or inactive (tp2).
  - OPERAT or GENBELL : by successively pressing this key, define whether the system should route the call to the attendant and/or the general bell after the non-response time-out TP2 has lapsed (active = ATTD or GBEL; inactive = attd or gbel).
- TMOUT1 and TMOUT2 make it possible to define the time-outs in tenths of a second. The default value is 12 seconds.
- VMUBEH makes it possible to define the role of the office communicator when it is used in a level 1 or 2 dynamic routing; by successively pressing LEVEL1 or LEVEL2, you can choose between "Auto-sec" or "Mailbox".

11.2.9.1.3 BROADCAST GROUPS - BROADC

After pressing BROADC (A), enter the broadcast group directory number. The directory number of the first station in the group is displayed.

ADD makes it possible to add a station directory number to the group. Enter the number of the station to be added to the group; press OTHER to add the general bell to the group.

TRANS: by successively pressing this key, you can choose whether the station concerned can transmit a broadcast call.

RECEPT: by successively pressing this key, you can choose whether the station concerned is subjected to a broadcast call.

Note:

In a group with an external speaker, the following rights must be observed: for the stations: transmission = YES, reception = NO; for the speaker: transmission = NO, reception = YES

11.2.9.1.4 ATTENDANT STATION GROUP - ATTGRP

After pressing ATTRGRP (A), enter the group index and validate. The directory number of the first station in the group is displayed.

ADD makes it possible to add a station directory number to the group. Enter the number of the station to be added to the group.

OTHER proposes another destination; by successively pressing this key, you can choose the destination (General bell, Welcome 1 to 8) then validate.

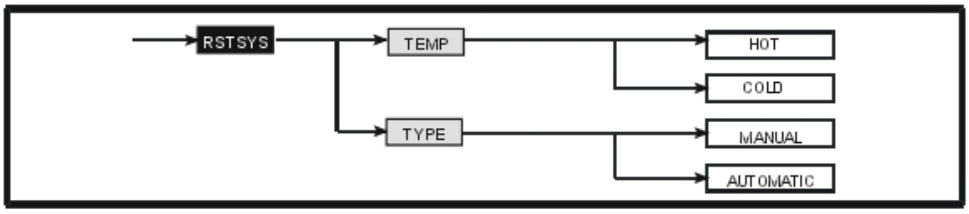
DYNROU makes it possible to define the dynamic routing mechanisms for operator station group calls:

- EXTERN and LOCAL make it possible to define whether the dynamic distribution (time-outs T1 and T2, destinations) criteria for each type of call (external or local) are active or not:
  - NUMBER makes it possible to define a destination station (or hunting group) or a collective speed dial number for the dynamic routing in the case where the call has not been answered after a time-out TP1 (12 seconds by default).
  - TP1: by successively pressing this key, you can define whether the time-out 1 is active (TP1) or inactive (tp1).
  - TP2 : by successively pressing this key, you can define whether the time-out 2 is active (TP2) or inactive (tp2).
  - OPERAT or GENBELL: by successively pressing this key, define whether the system should route the call to the attendant and/or the general bell after the non-response time-out TP2 has lapsed (active = ATTD or GBEL; inactive = attd or gbel).
- TMOUT1 and TMOUT2 make it possible to define the time-outs in tenths of a second. The default value is 12 seconds.
- VMUBEH makes it possible to define the role of the office communicator when it is used in a level 1 or 2 dynamic routing; by successively pressing LEVEL1 or LEVEL2, you can choose between "Auto-sec" or "Mailbox".

11.2.10 System Reset

11.2.10.1 Operation

This function is used for defining the conditions of the next system reset (hot, cold, manual, or automatic).



Press RSTSYS.

TEMP: by successively pressing this key, you can display the type of reset to be carried out:

- hot reset: simple reset.

  Note 1:
  It is recommended to perform a hot reset of the system when changing the external metering mode from IP to V24.

- cold reset: reset + loss of client configuration (return to default configuration).

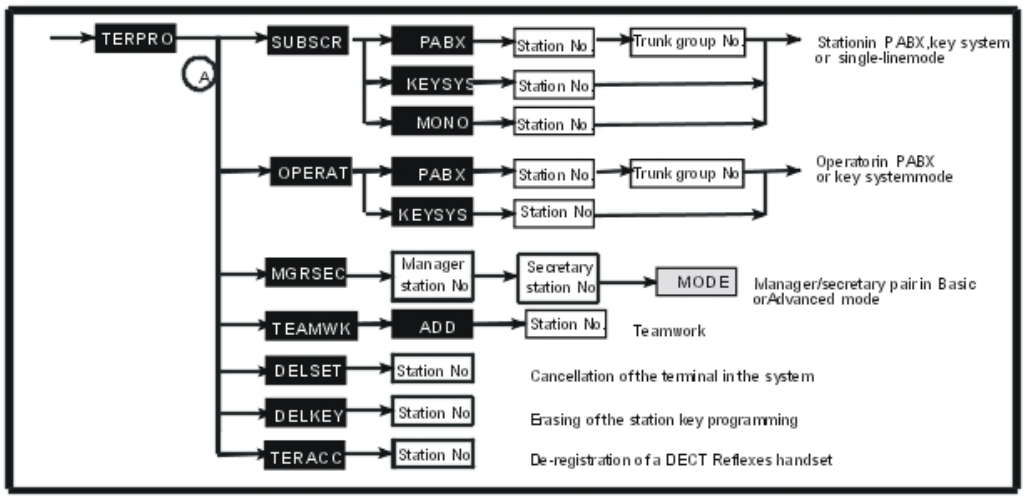
TYPE: by successively pressing this key, you can display the condition for the next reset: manual or automatic.

11.2.11 Terminal Profiles

11.2.11.1 Operation

This function is used for assigning a terminal profile to the stations, in the following order:

- assignment of a basic profile:
  - key system mode (attendant and stations)
  - PCX mode (attendant and stations)
  - single-line (stations only)
- assignment of an advanced profile:
  - manager/assistant
  - teamwork



11.2.11.1.1 TERMINAL PROFILES AVAILABLE ACCORDING TO THE TYPE OF STATION

Station type	BASIC PROFILE			Advanced PROFILE		
	Single-line	Multiline		Working group	Manager/Assistant couple	
		PCX	Key system		Manager	Secretary
Stations with display		YES	YES	YES	YES	YES
Multi-line stations without display	Except 4003	YES	YES	YES		YES
Singl-line stations	YES	Except 4003	Except 4003			
Z Option	YES					

Press TERPRO.

11.2.11.1.2 STATION PROFILE - SUBSCR

After pressing SUBSCR (A), choose the profile to be assigned: single line, key system or PCX.

Enter the station directory number; for the PCX mode, state the trunk group number associated with the RSB keys and validate. To load the selected profile, validate.

11.2.11.1.3 ATTENDANT PROFILE - ATTEND (OPERAT)

After pressing OPERAT (A), choose the profile to be assigned: key system or PCX.

Enter the attendant station directory number; for the PCX mode, state the trunk group number

associated to the RSB keys and validate. To load the selected profile, validate.

11.2.11.1.4 MANAGER-ASSIST PROFILES - MGRAST (MGRSEC)

After pressing MGRSEC (A), enter the manager station's directory number followed by that of the assistant station.

MODE: by successively pressing this key, define the mode for the assistant station: Advanced or BASIC, then validate. After choosing **Basic**, each station in the pair has:

- A **Filter** key for activating or deactivating the screening of manager station calls.
- An **RSL** key which allows both members of the couple to call the other member directly.

If the assistant station is to monitor the manager stations resources, choose **Advanced** mode instead of **Basic** mode.

To cancel the manager-assistant configuration, cancel the programmed **Filter** key and the **RSL** resource key on each station of the screening pair.

11.2.11.1.5 TEAMWORK PROFILE - TEAMWK

Press TEAMWK (A).

ADD makes it possible to add a member to the group. Enter the station directory number. Validate. The display then states the number of station resources.

11.2.11.1.6 CANCELLATION OF DATA - DELSET AND DELKEY

DELSET (A) after a logical switchoff, makes it possible to erase the data from the station (station type, appointment reminders, messages, forwardings, etc.). Enter the station directory number. Validating deletes the data from the station.

DELKEY (A) after a logical switchoff, makes it possible to cancel all programmings of the keys (MMC station or OMC) so that a new profile may be loaded. Enter the station directory number. Validating cancels all key programming.

11.2.11.1.7 REMINDER OF FUNCTIONS AVAILABLE WITH THE RESOURCE KEY

A resource key is a line key that manages only one incoming/outgoing, internal or external call. Resource keys can be specialized or not. If a resource key is not specialized, that key can handle all types of call:

- mixed resource key (RGM): handles internal and/or external calls, whether incoming or outgoing.
- outgoing resource key (RGO): handles internal and/or external outgoing calls.
- incoming resource key (RGI): handles internal and/or external incoming calls.

If the key is specialized, that key handles a particular type of call:

- resource key dedicated to external access (RSP): handles the calls coming from or going to that access.
- resource key specialized in destination (RSD):
  - dedicated to a directory number, handles internal calls for this number.
  - dedicated to a DID number, handles incoming calls for this number.

- associated to a trunk number, handles the outgoing calls on this trunk.

- resource key dedicated to a station (RSL): handles the calls coming from and going to a particular station
- resource key dedicated to a trunk (RSB): for making external outgoing calls via a particular trunk and receiving all network calls.

11.2.11.1.8 TERMINAL PROFILE IN KEY SYSTEM MODE

This profile consists of:

- 2 mixed resource keys (RGM) for internal and external calls
- as many network monitoring, physical resource keys (RSP) as trunks in the system.

11.2.11.1.9 TERMINAL PROFILE IN PCX MODE

This profile consists of:

- 2 mixed resource keys (RGM) for internal and external calls
- 2 RSB keys for external calls

11.2.11.1.10 TERMINAL PROFILE IN SINGLE-LINE MODE

This profile consists of 3 virtual keys (RGM) for internal and external calls.

11.2.11.1.11 TEAMWORK PROFILE

assigning this profile gives stations:

- n-1 RSL keys ("n" being the number of members in the group)
- a selective ringing monitoring key
- a group call pickup key

11.2.11.1.12 MANAGER/ASSISTANT TERMINAL PROFILES

Mode	MANAGER	SECRETARY
Basic	- key for direct call from the secretary station - FILTER key	- key for direct call from the secretary station - FILTER key
Advanced	- key for direct call from the secretary station - FILTER key	- key for direct call from the manager station - FILTER key - monitoring keys for all manager's resources

11.2.11.1.13 DE-RECORDING OF DECT Reflexes STATIONS - TERACC

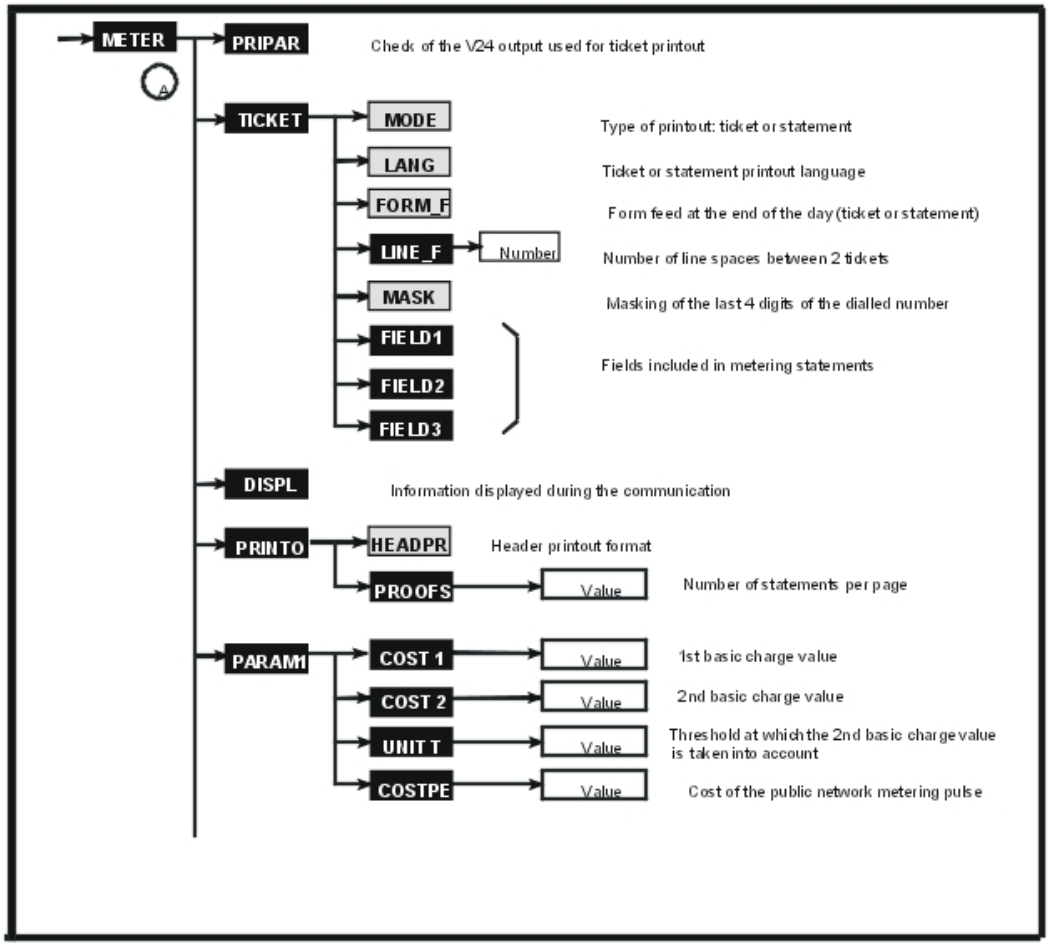
This function makes it possible to de-registre a DECT Reflexes station.

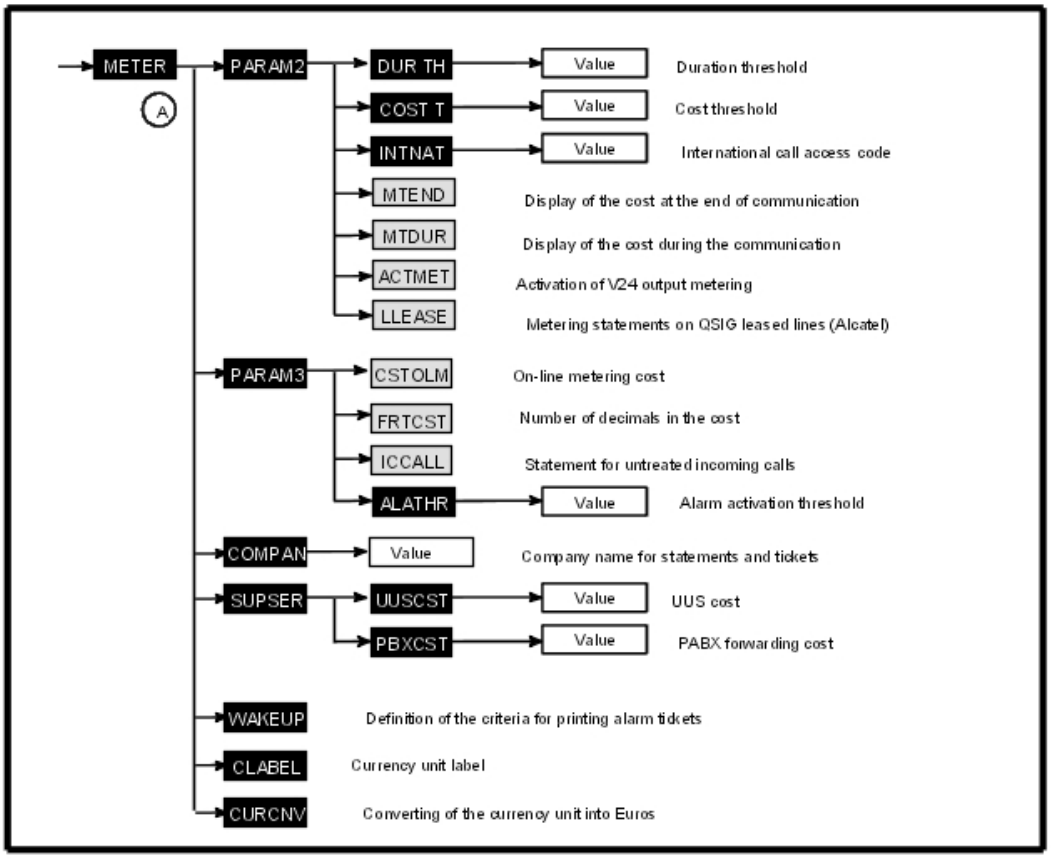
Enter its directory number, erase it and then confirm the de-recording.

11.2.12 Metering Configuration

11.2.12.1 Operation

This feature defines all the parameters related to the signal counting operation.





Press METER.

11.2.12.1.1 CHARACTERISTICS OF THE V24 COUNTING - PRIPAR

PRIPAR (A) makes it possible to check the V24 output used to print metering statements/tickets.

11.2.12.1.2 DEFINITION OF THE PRINTOUT TYPE AND FORMAT - RECORD (TICKET)

Press TICKET (A).

Various parameters - MODE, LANG, FORM_F, LINE_F, MASK

MODE: by successively pressing this key, define the type of printout: RECORD (TICKET), LISTING or NETWORK.

LANG: by successively pressing this key, define the language for the ticket and statement printouts.

FORM_F: by successively pressing this key, define whether a form feed will (YES) or will not (NO) be performed at the end of the day for the printing of statements.

LINE_F: after pressing this key, state the number of lines you wish to have between each metering ticket.

MASK: by successively pressing this key, define whether the last 4 digits of the number dialled are to be masked (YES) or not (NO) in the printouts of statements and tickets.

Fields to be shown on a signal counting statement - FIELD1, FIELD2 and FIELD3

FIELD1, FIELD2 and FIELD3 make it possible to define the fields which are to be shown on the metering statements.

? Field 1: FIELD1

SUB : station number

TYP : call type

TRK : trunk number

DAT : date

TIM : time

DUR : call duration

TAX : number of counting units

SER : remote services

? Field 2: FIELD2

FAC : additional services

DNU : dialled number

DMO : dialling mode

RIN : ringing duration

CST : call cost

ACC : account code

SUN : printout of user name or business code or no printout

? Field 3: FIELD3

IUS : initial user (charged user)

NOD : node number (modifiable only if MODE = NETWORK)

CAR : carrier

SU8 : 8-digit user identification

TR4 : 4-digit trunk identification

The selected field flashes.

FEATUR: by successively pressing this key, you can choose whether the flashing field must be included (label in capitals) or not (label in lower case letters) on the statement.

11.2.12.1.3 INFORMATION DISPLAYED ON A STATION DURING A CALL - DISPL

After pressing DISPL (A), by successively pressing FEATUR, you can choose the type of information to be displayed on the stations during a communication: duration (DISPLAY DURATION), units + duration (DISPLAY UNITS) or cost + duration (DISPLAY COST).

11.2.12.1.4 PRINTOUT FORMATS (HEADER AND NUMBER OF STATEMENTS/PAGE) -

PRINTO (A)

After pressing PRINTO (A), by successively pressing HEADPR, you can choose the type of printout for the header: on each page (EP), on the first page (FP) or no header printout (NO).

PROOFS makes it possible to define the number of statements (0 to 99) per page.

11.2.12.1.5 PARAMETERS CONCERNING THE COST OF A CALL - PARAM1 (A)

Press PARAM1 (A).

COST1: first basic charge value

COST2: second basic charge value

UNIT T: threshold where the second basic charge value is taken into account (number of pulse meters)

COSTPE: cost of the meter pulse sent by the public exchange (this value is used to calculate the number of meter pulses to be displayed during or at the end of a call).

When choosing COST1, COST2, and COSTPE, state the value (value then decimal value).

When choosing UNIT T, state the number of meter pulses after which the second basic charge value is taken into account.

11.2.12.1.6 THRESHOLD VALUES-V24 ON-LINE METERING - PARAM2 (A)

Press PARAM2 (A).

DURTH: state the duration threshold value (in minutes).

COST T: state the threshold value (integer value then decimal value).

INTNAT: state the monitored business code.

MTEND: by successively pressing this key, you can choose whether the total cost is displayed at the end of the call (END) or not (end).

MTDUR: by successively pressing this key, you can choose whether the cost is to be displayed during the communication (DURC) or not (durc).

ACTMET: by successively pressing this key, you can choose whether the V24 metering is activated (TAX) or not (tax).

Note:

When activating the V24 metering, it is recommended you perform a hot reset of the system. (See System Reset section)

LLEASE: by successively pressing this key, you can choose whether the pulse metering statements are to be printed (LEAS) or not (leas) on QSIG leased lines.

11.2.12.1.7 ON-LINE METERING COST-NUMBER OF DECIMALS-ALARM THRESHOLD - PARAM3 (A)

Press PARAM3 (A).

CSTOLM: by successively pressing this key, you can choose the on-line metering cost (0 to 9 pulse meters).

FRTCST: by successively pressing this key, you can choose the number of decimals for the costs (0, to 3).

IAPENT: by successively pressing this key, you can choose whether a statement is printed or not in the case of an untreated incoming call.

ALATHR: to define the percentage of statements stored before an alarm is activated (0 to 100, 0 = no alarm).

11.2.12.1.8 COMPANY NAME - COMPAN (A)

After pressing COMPAN (A), enter the company name (16 alphanumeric characters maximum) shown on the statements and tickets and validate.

11.2.12.1.9 COST OF ADDITIONAL SERVICES - SUPSER

Press SUPSER (A).

UUSCST: cost of the user to user signalling (UUS)

PBXCST: cost of the PBX/PCX forwarding

For these 2 choices, state the value (value then decimal value).

11.2.12.1.10 PRINTOUT OF ALARM TICKETS - WAKEUP (A)

After pressing WAKEUP (A), by successively pressing FEATUR, you can choose whether to validate the various printout criteria or not (a criterion is active when its label is displayed in capital letters on the first line of the display; if not, it is displayed in lower case letters):

ACT : alarm activated

CANC : alarm cancelled

FAIL : alarm aborted

ANSW : alarm answered

11.2.12.1.11 MONEY UNIT- CLABEL (A)

CLABEL (A) makes it possible to define the label for the present money unit used in the country and displays it on the stations.

11.2.12.1.12 CONVERTING THE MONEY UNIT - CURCNV (A)

Press CURCNV (A).

This feature makes it possible to define the application methods for the change over to the Euro.

CLABEL: label displayed (Eur).

DATE: date of change over to Euro.

TIME: time of change over to Euro.

EXRATE: exchange rate of the Euro with the country's own money unit.

PARAM1: cost of basic charge (COST 1 and COST 2); cost of charge sent by the public network (COSTPE); threshold of the basic charge's 2nd value (UNIT T).

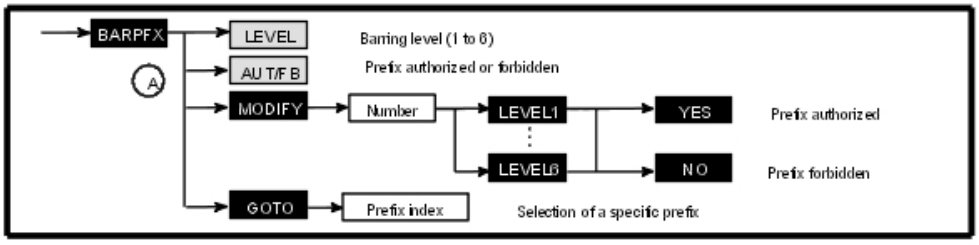
PARAM2: cost of on-line metering and number of decimals.

SUPSER: cost of signalling from user to user and PBX/PCX forwarding.

11.2.13 Barring Prefixes

11.2.13.1 Operation

This function is used for defining a maximum of 100 restriction (barring) prefixes.



Press BARPFX.

LEVEL: by successively pressing this key, you can change the prefix barring level.

AUT/FB: by successively pressing this key, you can change the type: FORBIDDEN or AUTHORIZED prefix.

After pressing MODIFY (A), enter the prefix value (10 digits max.) and validate. The following possibilities are offered:

- Choose the barring level (LEVEL1 to LEVEL6).
- Choose the type of prefix: press YES for an authorized prefix or NO for a forbidden prefix.

GOTO makes it possible to position yourself at any position in the barring prefixes table.

11.2.14 Parameter Duplication

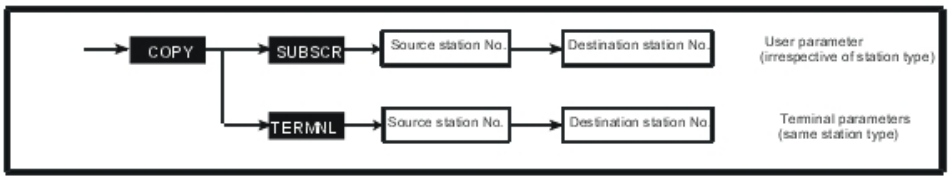
11.2.14.1 Operation

This feature is used for assigning the parameters of a specific station to other stations:

- duplicating user parameters (dynamic forwarding, call detail/metering profile, ...): The source and destination stations can be of different types.
- duplicating terminal parameters (keys): The source and destination stations must be of the same type.

Note:

The personal speed dial numbers, RSL and RSD keys cannot be duplicated from one station to another.



Press COPY.

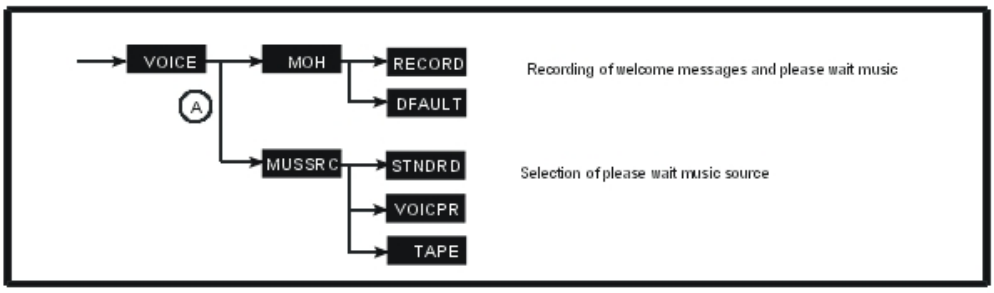
Choose the duplication type (SUBSCR or TERMNL). Enter the source station directory number followed by that of the destination station.

11.2.15 Welcome and Please-Wait Message

11.2.15.1 Operation

The please wait message music is subject to composer's rights. For further information, consult the appropriate body.

This feature makes it possible to record welcome messages and define the source of the music-on-hold.



Press VOICE.

11.2.15.1.1 RECORDING OF WELCOME MESSAGES - MOH (A)

MOH of (A) makes it possible to record 8 welcome messages and one please-wait message.

After selecting the type of message to be recorded, press RECORD.

Record the message using the station handset.

SPLIT makes it possible to stop the recording and then restart it by CONTIN. STOP lets you stop the recording.

DEFAULT lets you return to the default welcome message.

LISTEN lets you listen to the recorded message.

11.2.15.1.2 EMITTING SOURCE OF THE PLEASE-WAIT MESSAGE - MUSSRC (A)

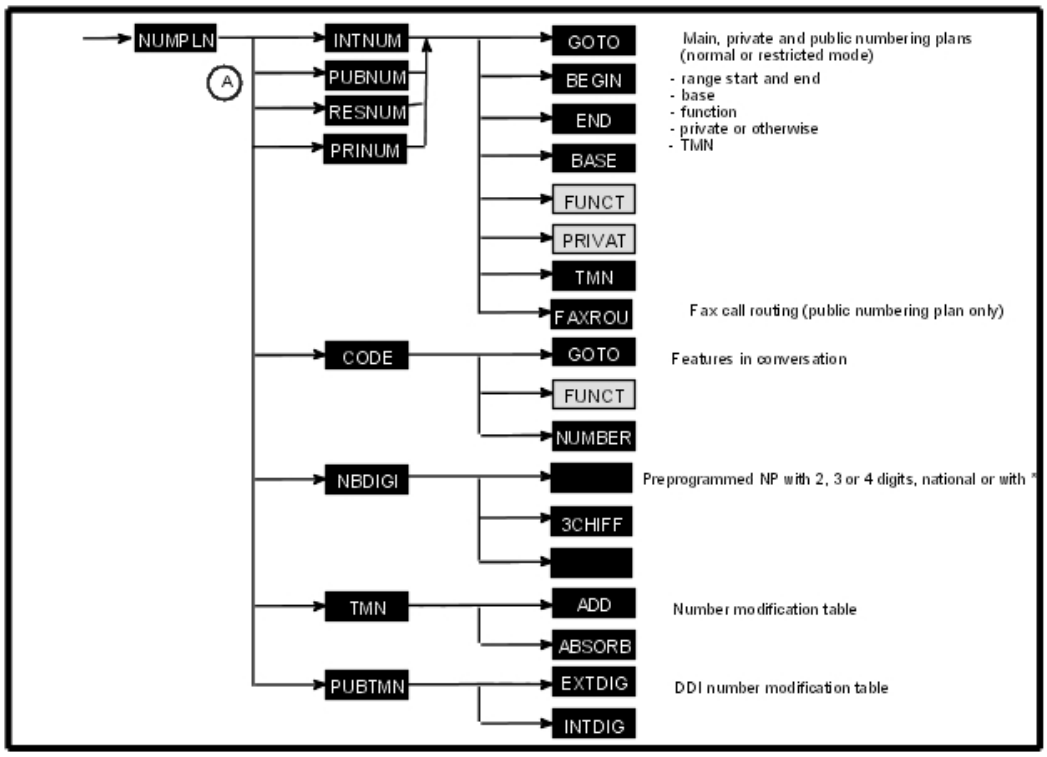
MUSSRC of (A) makes it possible to select the emitting source for the please wait message.

- STNDRD: default please-wait music (DEFAULT displayed on the first line of the display).
- TAPE: external please-wait music (EXTERN displayed on the first line of the display).
- VOICEPR: customized please-wait music (CUSTO displayed on the first line of the display).

11.2.16 Numbering Plans

11.2.16.1 Operation

This feature is used for defining the codes associated with the features of the main dialing (or numbering) plan, the private dialing plan, the public dialing plan and the table of features in conversation.



Press NUMPLN.

11.2.16.1.1 DIALING (NUMBERING) PLANS - INTNUM, PUBNUM, RESNUM AND PRINUM

INTNUM grants access to the selected main numbering plan (99 ranges) for analysis of the dialing made on a terminal.

PUBNUM grants access to the public numbering plan in normal mode (99 ranges), RESNUM grants access to the public numbering plan in restricted mode (99 ranges); these plans are selected for analysis of the dialing received by the system via a T0/T2 access or to carry out call distribution (TL or T0/T2).

PRINUM grants access to the selected private numbering plan (36 ranges) for analysis of the dialing received by the system via a private line.

FUNCT lets you select a function from those offered.

DESIGNATION	Function	USE OF THE BASE	USE OF THE TMN
MTrG	Main trunk group seizure (private or not)	YES	YES (33)
Subsc	Station call (private or not)	YES	
STrG	Secondary trunk group seizure (private or not)	YES	YES (33)
Code	Collective speed dial numbers	YES	
Group	Group call	YES	
Broad	Broadcast group call	YES	
Prog	Switch to programming mode		
Pickp	Call pick-up	YES	
Rdial	Last number redial		
ProCo	Data connection protection against barge-in (intrusion)		
Forwd	Forwardings	YES	
Attd	Attendant call station		
PagS	Paging call answer		
Pagin	Answer to a general paging call		
PagP	Paging by prefix		
CClbk	Automatic callback on busy station cancellation		
Lock	Locking/Unlocking		
Mail	Text mail		
VMU	Voice mail unit LED light		
CVMU	Voice mail unit LED light off		
MTR	Counting (metering) total recall		
Accou	Business account code for new outgoing call		
Disa	DISA Transit		
Appmt	Appointment reminder/Alarm		
CLoop	Loopback of dialing into current dialing plan		YES (1 to 32)
Main	Change of dialing plan (loopback of number in the main dialing plan)		YES (1 to 32)
VisAl	Temporary assignment of a DID number to a room		
VisFr	Cancellation of the assignment of a DID number to a room		

RoomS	Room status		
Replc	Station replacement		
Move	Station movement		
OwnVM	Mailbox call		
Audtx	Audiotex service DID number	YES	

The VisAl, VisFr, Disa and Audtx features are only provided in the public dialing plans (normal and restricted mode).

PRIVAT: by successively pressing this key, state whether the number is private or not; this parameter is only used for the Subsc, Main trunk groups and Secondary trunk groups functions.

TMN makes it possible to enter the index (1 to 32) of the NMT table; enter 33 to retain the initial value (without modifications) for the Main trunk group and Secondary trunk group functions.

BEGIN makes it possible to enter the number which starts the range (0 to DDDD). The characters *, #, A, B, C, D are allowed in the fixed part of the range but not in the variable part (A00 to A99; 100 to 10B: incorrect).

END makes it possible to enter the number which ends the range (0 to DDDD).

BASE: used for working out the directory number. The base is included between 0 and 9999. For the functions which use the base, the calculation is done as follows: Directory number = Dialled number - Begin + Base

FAXROU followed by the destination Fax number: makes it possible to associate the user's DDI number with the Fax number to which incoming Fax calls must be routed. This feature is only provided in the public dialing plan.

11.2.16.1.2 FEATURES IN CONVERSATION - CODE

These codes make it possible to access services during an established call.

Press CODE (A).

GOTO: makes it possible to enter the features in conversation value

FUNCT: makes it possible to select a function from those offered.

DESIGNATION	**Function**
PBX recall	Calibrated loopbreak
Canc enquiry	Consultation (enquiry) call cancellation
Broker	Shuttle call
Callback	Automatic callback
Consult	Waiting call consultation
Conference	Conference
Barge-in	Barge-in (intrusion) on busy
Code paging	Paging
Resend MF	DTMF end-to-end signaling

Parking	Parking
Send MF num	Automatic switch DTMF end-to-end signaling and retransmission of this service access code
Doorphone	Open door
AllotN Cat 1 to 7	Assignment of line with Class of Service Restriction 1 to 7
AllotM Cat 1 to 7	Assignment of line with Class of Service Restriction 1 to 7 + Counting total recall
Mcid	Malicious call identification
DND override	Override Do not disturb
Conv record	Recording of conversations

11.2.16.1.3 PREPROGRAMMED NUMBERING PLANS - NBDIGI

NBDIGI (A) makes it possible to choose one of the preprogrammed numbering plans (2 to 4 digits, national or with *). Validate.

11.2.16.1.4 NUMBER MODIFICATION TABLE - TMN

TMN (A) makes it possible to define the modifications to be made to the incoming dialing. Position yourself at the beginning (index 1 to 32) of the table quoted by the main dialing plan function.

ADD: digits to be added (16 maximum).

ABSORB: number of digits to be deleted (4 maximum).

11.2.16.1.5 DDI NUMBER MODIFICATION TABLE - PUBTMN

PUBTMN (A) makes it possible to define the digits to be substituted before analysis by the DDI numbering plan (this function concerns DDI with more than 4 digits). Position yourself at the beginning (index 1 to 32) of the table quoted by the DID dialing plan.

EXTDIG: digits to be deleted (16 maximum).

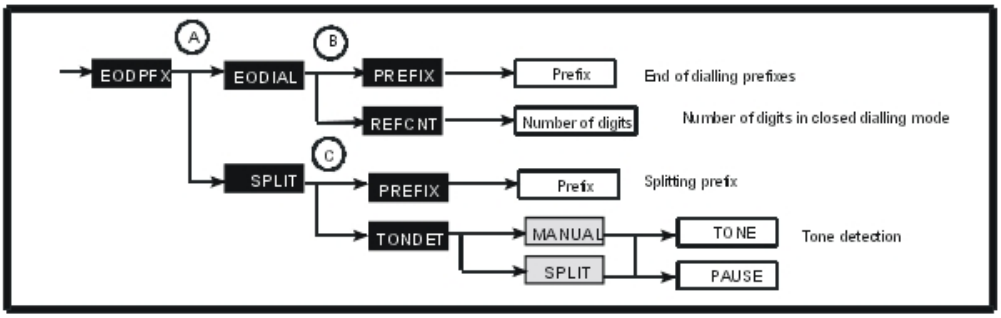
INTDIG: digits to be added (8 maximum).

11.2.17 Splitting and End of Dialling

11.2.17.1 Operation

This feature is used for defining the following elements:

- maximum number of digits in closed dialing mode
- 20 end of dialing prefixes and their associated counters
- 16 splitting prefixes for all lines (PCX or public network)



11.2.17.1.1 END OF DIALING - EODIAL

Press EODPFX then EODIAL (C).

End of dialing prefixes - PREFIX

PREFIX (B) displays the end of dialing prefixes and value of the counters associated with the different prefixes.

After pressing MODIFY, enter the end of dialing prefix (6 digits max) and validate. Then state the value of the counter associated with the prefix and validate.

Reference counter - REFCNT

After pressing REFCNT (B), enter the value of the counter and validate.

11.2.17.1.2 SPLITTING - SPLIT

Press EODPFX then SPLIT (C).

Splitting prefixes - PREFIX

PREFIX of (C) displays the splitting prefixes.

After pressing MODIFY, enter the splitting prefix and validate.

By successively pressing MODIFY, define the type of connection associated with the prefix, PCX, PSTN, ALL or CTRYCD then validate.

Tone detection/pause - TONDET

Press TONDET (C).

TONE or PAUSE are provided by successively pressing MANUAL or SPLIT to define the operation in manual seizure mode (MANUAL key) or during dialing (SPLIT key).

PAUSE: the system must insert a pause.

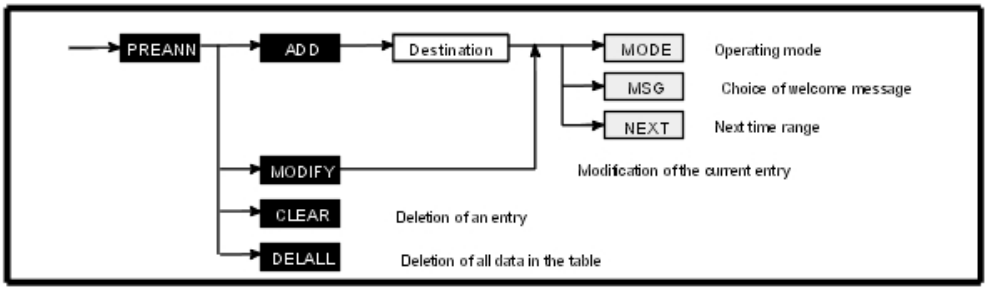
TONE: the system uses the tone detection operation.

11.2.18 Pre-announcement Messages

11.2.18.1 Operation

WARNING: This feature is no longer offered on a R2.0 system's MMC station.

This feature makes it possible to assign up to eight 16-second welcome messages to stations or hunt groups (up to 15 entries with DIDnumbers + 1 entry corresponding to all stations and hunt groups) with validity according to the time ranges.



Press PREANN.

After pressing ADD or MODIFY:

MODE makes it possible to choose the operating mode (OFF, MODE1, MODE2, MODE1 BUSY or MODE2 BUSY).

- MODE 1: the external party hears the message from start to finish then the called station is rung.
- MODE 2: the external party hears the message while the called station is being rung.
- MODE & OCC: message broadcasted in mode 1 only if the station or hunt group is busy.
- MODE 2 OCC: message broadcasted in mode 2 only if the station or hunt group is busy.
- OFF: no access to welcome message

MSG makes it possible to choose the welcome message: Msg 1 to Msg 8.

NEXT makes it possible to choose the time range (the starting time for the range is displayed).

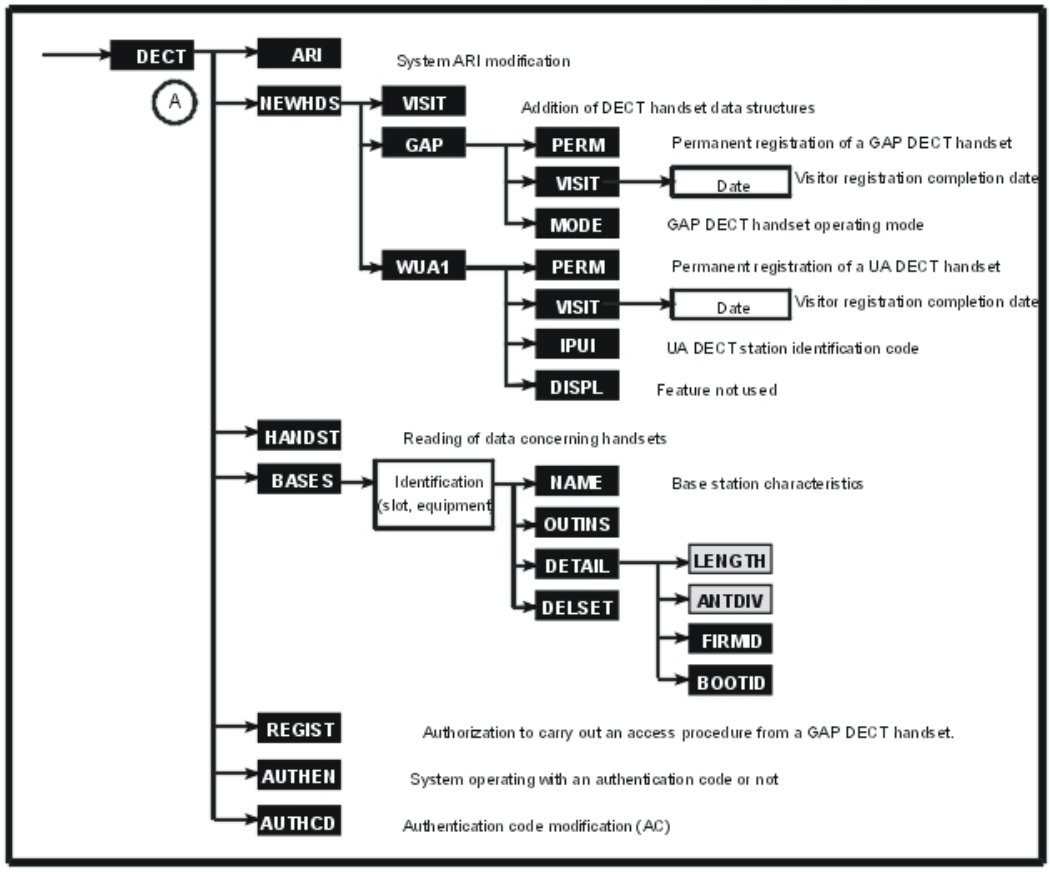
CLEAR makes it possible to delete the data from the selected entry.

DELALL makes it possible to delete all the entries in the table.

11.2.19 DECT

11.2.19.1 Operation

This feature is used to define the parameters for the use of DECT handsets.



Press DECT.

11.2.19.1.1 MODIFICATION OF THE SYSTEM ARI - ARI

When a system is put into service for the first time, its ARI (Access Right Identifier) has the default value. If there are two Alcatel-Lucent DECT systems which belong to two different clients but which have the same radio signalling zones, the default values must be modified and a different ARI value assigned to each one of the systems. After modification of the ARI, the base stations are informed of the new ARI.

After pressing ARI, enter 11 octal digits, the first being non-modifiable (always equal to 1) and the last being equal to 0 or 4.

11.2.19.1.2 ADDITION OF DECT MOBILE DATA - NEWHDS

NEWHDS makes it possible to create new data structures for DECT mobiles.

Data associated with a DECT access - VISIT

VISIT makes it possible to create data associated with a DECT access specified as a visitor. This DECT access is then used to record a DECT station subsequently (UA or GAP).

Data associated with a GAP DECT handset - GAP

This command makes it possible to automatically register a new GAP DECT handset. This

registration is based on the reception of an access right sent by the GAP DECT handset (after a move on the part of the user). Only one GAP DECT handset can be registered at a specific time.

PERM makes it possible to select a permanent association with the system.

VISIT makes it possible to select a temporary association with the system; enter the date on which the mobile is to be automatically disconnected from the system and validate.

MODE makes it possible to define the operating mode for the GAP DECT handset: Bas, Enh or UA (WUA: significant choice for UA + GAP DECT).

Data associated with a UA DECT handset - WUA1

A UA DECT handset is registered manually by entering its IPUI.

PERM makes it possible to select a permanent association with the system.

VISIT makes it possible to select a temporary association with the system; enter the date on which the mobile is to be automatically disconnected from the system and validate.

IPUI makes it possible to modify the DECT handset IPUI value; enter 14 octal digits and validate.

11.2.19.1.3 READING OF THE DATA CONCERNING MOBILES - HANDST

HANDST (A) makes it possible to display the data (directory number, type of association with the system, IPUI) relative to all the DECT mobiles declared in the system.

GOTO makes it possible to display the data of a specific mobile; enter the directory number of the mobile whose data you wish to see.

11.2.19.1.4 BASE STATION FEATURES - BASES

Press BASES (A) and then enter the slot number and the equipment number of the interface to which the base station to be parametered is connected.

NAME makes it possible to modify the name of the base station.

OUTINS makes it possible to display the status of the base station concerned. INSERV and OUTOFS makes it possible to put the base station concerned in or out of service.

DETAIL displays the number of DECT channels (3, when the base station is connected to the system via 1 UA link, or 6 when it is connected via 2 UA links) and gives access to the following sub-features for the 4070 IO base station:

- LENGTH: by successively pressing this key, indicate the connection distance from the base to the system: short line (0-400 m), average line (400-800 m) or long line (800-1200 m). This data is necessary for synchronisation.
- ANTDIV: by successively pressing this key, indicate whether the 2 antennas (Diversity) or only the first (No diversity) are used.
- FIRMID: reading the software version currently on the base station.
  Note: Alcatel-Lucent OmniPCX Office Communication Server R5.1 embeds only 1 software version of the base station. 2 software versions (1G and NG) can be downloaded during the system's start phase. Base stations are plug and play devices.
- BOOTID: reading the software version for initialisation of the base station.

DELSET makes it possible to delete the data relating to the base station concerned.

11.2.19.1.5 ACCESS PROCEDURE FOR A GAP DECT HANDSET - REGIST

REGIST (A) makes it possible for a registered GAP DECT handset to carry out an access procedure. A particular piece of information is sent to the DECT handset enabling it to perform this procedure.

11.2.19.1.6 MANDATORY AUTHENTICATION CODE - AUTHEN

AUTHEN (A) is used to define the system operating mode: recording of stations with or without an authentication code. CHOICE lets you switch from ON to OFF.

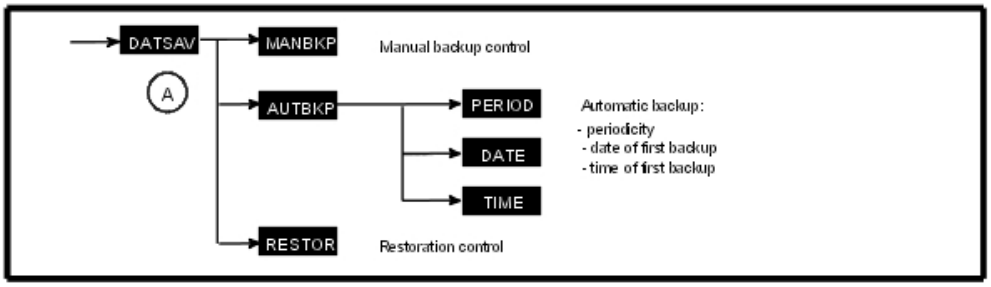
11.2.19.1.7 MODIFYING THE AUTHENTICATION CODE - AUTHCD

AUTHENCD (A) makes it possible to modify the authentication code (up to 8 digit AC code) requested during system access.

11.2.20 Configuration Backup and Restoration

11.2.20.1 Operation

This feature provides manual backup controls and restoration controls and enables the definition of parameters enabling backup and restoration of the configuration.



Press DATSAV.

11.2.20.1.1 MANUAL BACKUP - MANBKP

Press MANBKP (A). Then validate; the backup starts.

11.2.20.1.2 AUTOMATIC BACKUP - AUTBKP

AUTBKP (A) makes it possible to define the date and time of the first automatic backup as well as the periodicity.

PERIOD makes it possible to state the interval (00 to 99 days) separating 2 automatic backups (00 corresponds to an infinite interval: no backup).

DATE makes it possible to state the date (as: Day 01-31/Month: 00-12) of the first backup.

TIME makes it possible to state the time (as: Hour 00-23/Minutes: 00-59) of the first backup.

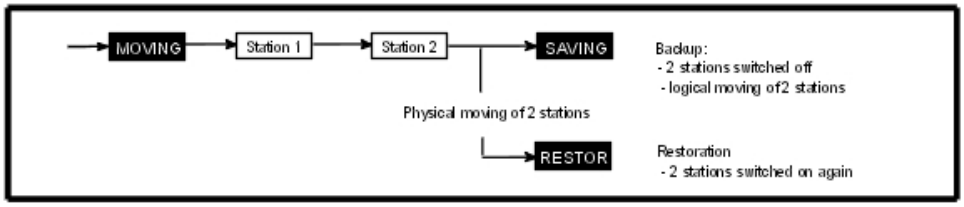
11.2.20.1.3 AUTOMATIC RESTORATION - RESTOR

Press RESTOR (A). Then, validate; the restoration starts.

11.2.21 Moving of 2 Stations

11.2.21.1 Operation

This feature is used to move the physical addresses of 2 stations of the same family.



Press MOVING.

Enter the directory number of station 1 (source station).

Enter the directory number of station 2 (destination station).

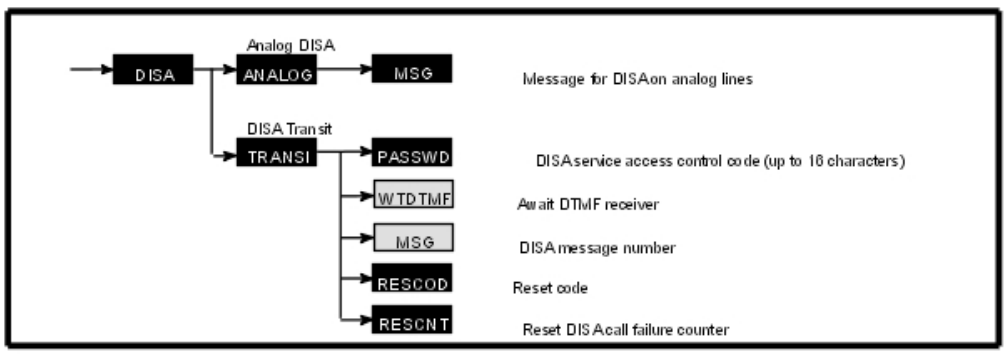
Follow this moving procedure:

- press SAVING: the 2 stations are put out-of-service and logically moved.
- physically move the 2 stations.
- press RESTOR: the 2 stations are put back in service.

11.2.22 DISA

11.2.22.1 Operation

This function is used to define the various parameters necessary for analog DISA and DISA transit services.



Press DISA.

11.2.22.1.1 ANALOG DISA - ANALOG

Press ANALOG.

MSG by successively pressing this key, it is possible to select the message transmitted during a DISA call on an analog line: Msg1 to Msg8.

11.2.22.1.2 DISA TRANSIT - TRANSI

Press TRANSI.

PASSWD makes it possible to modify the personal code for accessing the DISA transit service. Enter the current code then the new code and validate.

WTDTMF by successively pressing this key, it is possible to define the system response in the case of an unavailable MF receiver for a DISA transit call: camp-on authorized or call failure and redistribution.

MSG by successively pressing this key, it is possible to select the message transmitted during a DISA transit call: Msg1 to Msg8.

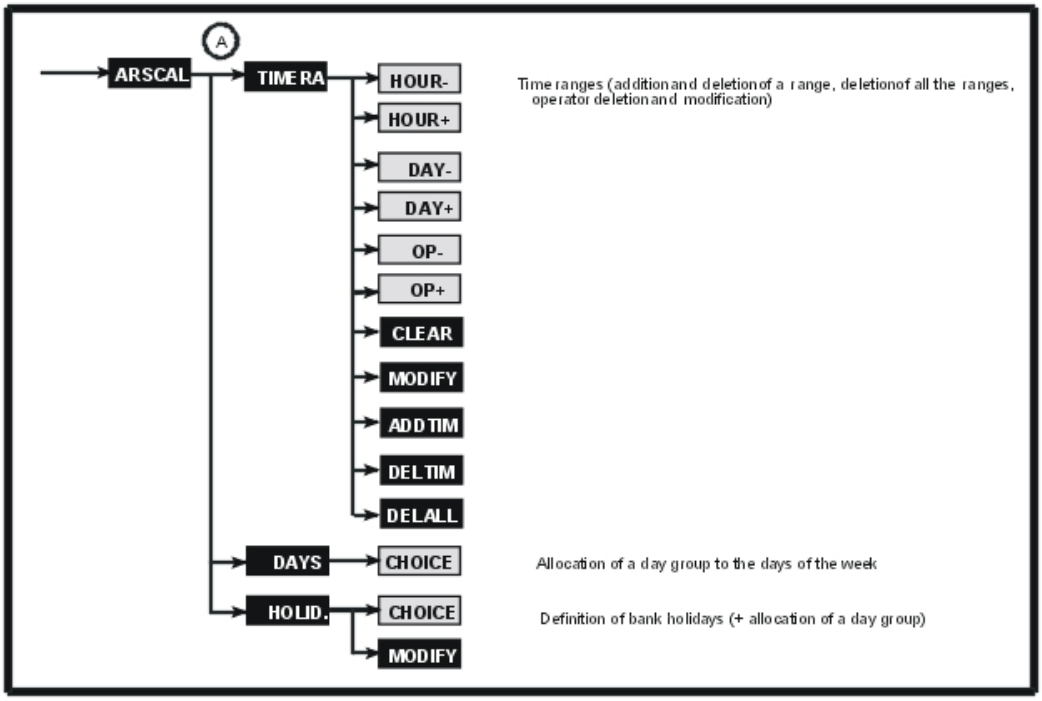
RESCOD makes it possible to reset the DISA service access control code.

RESCNT makes it possible to reset the DISA call failure counter (this counter'S value is not displayed).

11.2.23 ARS Calendar

11.2.23.1 Operation

This feature makes it possible to define the operation parameters by ARS operation time ranges.



Press ARSCAL.

11.2.23.1.1 TIME RANGES - TIMERA

Press TIMERA (A).

By successively pressing HOUR and TIME, it is possible to switch to the previous and next time range.

By successively pressing DAY- and DAY+, it is possible to switch to the group for the previous and next days (Day 1, Day 2, Day 3).

By successively pressing OP- and OP+, it is possible to switch to the group for the previous and next operator (1 to 4) defined for the time range and for the current day's group.

CLEAR makes it possible to delete the name of the operator.

MODIFY makes it possible to modify the name of the operator; press or enter the first letter of the name of the operator using an alphabetic keypad.

ADDTIM makes it possible to add a time range by defining a start time (information in the current visible range is copied into this new time range).

DELTIM makes it possible to delete the current time range (visible range).

DELALL makes it possible to delete all the time ranges and their contents.

Note:

The carriers can only be defined by OMC.

The 7 days of the week can be split up into 3 groups of days (example: Day 1 for Sunday, Day

2 for the 5 working days, Day 3 for Saturday); this makes it easier to assign carriers to the days of the week.

11.2.23.1.2 ASSIGNMENT OF A GROUP FROM DAY TO DAY IN THE WEEK - DAYS

Press DAYS (A).

NEXT makes it possible to switch to the next day of the week.

By successively pressing CHOICE, choose the group of days to be associated with the current day of the week.

11.2.23.1.3 DEFINITION OF BANK HOLIDAYS - HOLID

HOLID (A) makes it possible to enter bank holidays.

NEXT makes it possible to switch to the next bank holiday.

By successively pressing CHOICE, choose the group of days to be associated with the next bank holiday.

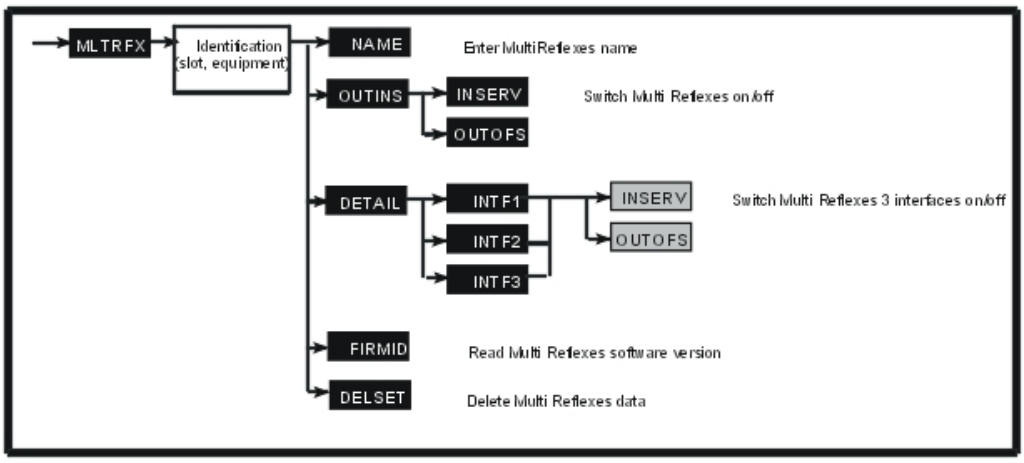
MODIFY makes it possible to modify or create a bank holiday.

- For changeable bank holidays (Easter for example): enter the date as DD/MM/YYYY.
- For set bank holidays (Christmas for example): enter the date as DD/MM (at the next review, the character * is displayed instead of the year).

11.2.24 Multi Reflexes

11.2.24.1 Operation

This feature makes it possible to define the parameters concerning each Multi Reflexes connected to the system; each Multi Reflexes allows 3 Reflexes stations to be connected.



Press MLTRFX and then enter the slot number and equipment number of the interface to which the Multi Reflexes to be parameterized is connected.

11.2.24.1.1 Multi Reflexes NAME - NAME

Press NAME.

Enter the Multi Reflexes name (18 characters):

- either using the alphabetic keypad
- or the station's numeric keypad which automatically switches to "letters" mode

11.2.24.1.2 Multi Reflexes STATUS - OUT INS

OUTINS lets you switch the Multi Reflexes off and then on again. Reminder: a Multi Reflexes is switched on automatically (as in the case of a Reflexes station).

If the secondary UA interfaces (see DETAIL function) are not declared as off, the Multi Reflexes cannot be switched off.

A Reflexes station cannot switch off the Multi Reflexes it is connected to.

The Multi Reflexes can be:

- In Service
- Out-of-Service
- Physical OOS/Logical OOS: Multi Reflexes not operational
- Physical OOS/Logical IS: Multi Reflexes not seen by the system (not declared or disconnected) or switched off by the installer

11.2.24.1.3 STATUS OF SECONDARY UA INTERFACES - DETAIL

DETAIL makes it possible to read the last 3 digits of directory numbers and declare the 3 secondary UA interfaces of the Multi Reflexes as on/off.

INSERV and OUTOFS make it possible to modify the state of each secondary UA interface.

11.2.24.1.4 SOFTWARE VERSION - FIRMID

FIRMID makes it possible to read the software version embedded in the Multi Reflexes.

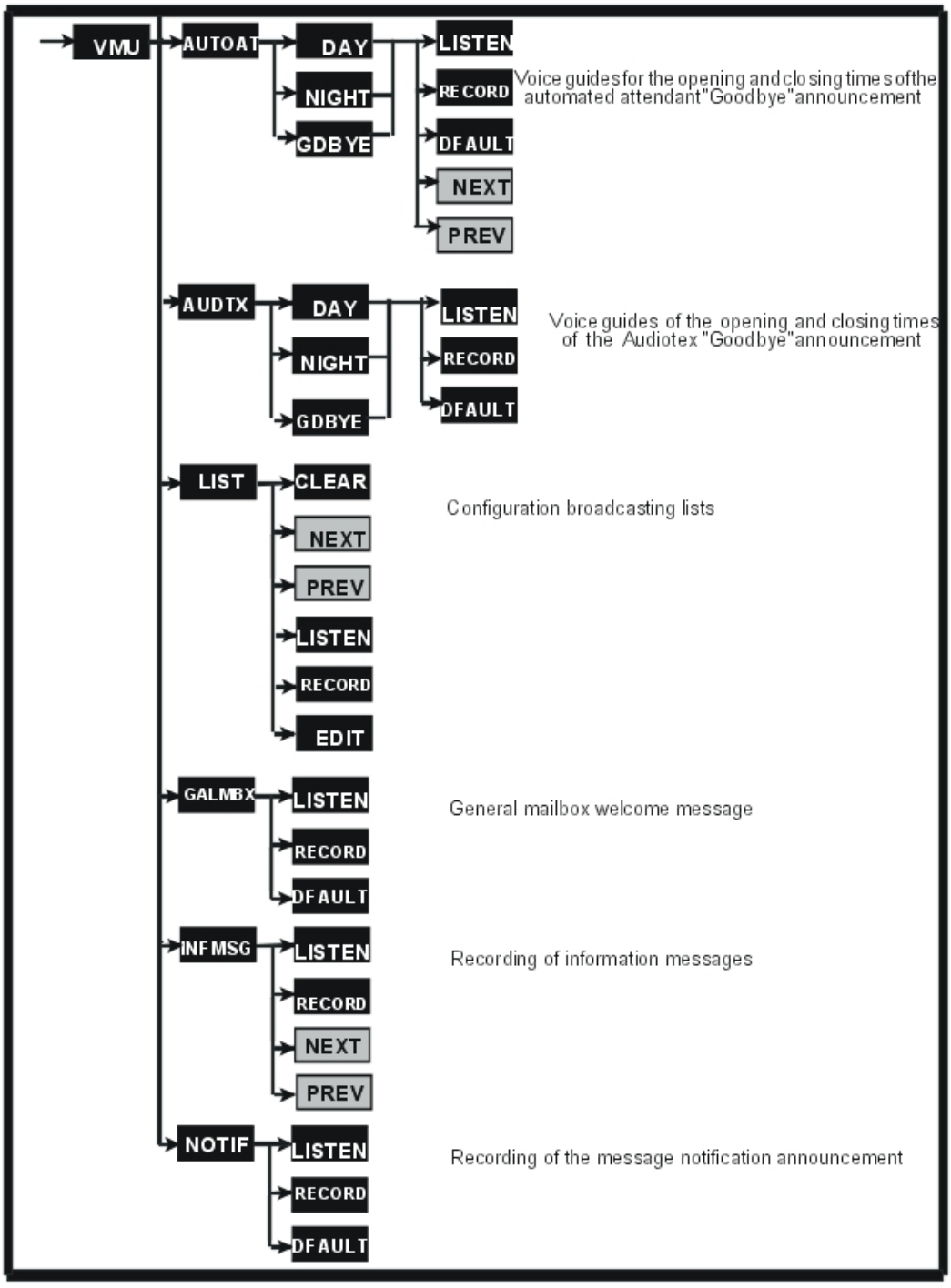
11.2.24.1.5 ERASING OF DATA - DELSET

DELSET makes it possible to delete all Multi Reflexes data (this operation is only possible after the Multi Reflexes is switched off.

11.2.25 Integrated Voice Server

11.2.25.1 Operation

This feature makes it possible to manage voice guides and configure broadcasting lists.



Press VMU.

11.2.25.1.1 AUTOMATED ATTENDANT - AUTOAT

AUTOAT lets you define 3 different types of automated attendants:

- DAY: lets you access voice guides for opening times.
- NIGHT: lets you access voice guides for closing times.
- GDBYE: lets you access voice guides for the “Goodbye” announcement.

For the DAY and NIGHT functions, the following possibilities are provided:

- LISTEN: lets you listen to the recorded or default voice guide.
- PREV: lets you return to the previous voice guide (main menu, sub-menu 0 to 9, welcome message).
- NEXT: lets you go on to the next voice guide (main menu, sub-menu 0 to 9, welcome message).
- RECORD: lets you record a customized voice guide.
- DEFAULT: lets you erase the recorded voice guide and replace it by the default voice guide; this key is only provided if recorded voice guides are available.
  Select YES (return to default voice guide) or NO.

For the GDBYE function (end of "Goodbye" announcement), the following possibilities are provided:

- LISTEN: lets you listen to the recorded or default voice guide.
- RECORD: lets you record a customized voice guide.
- DEFAULT: lets you erase the recorded voice guide and replace it by the default voice guide; this key is only provided if recorded voice guides are available.
  Select YES (return to default voice guide) or NO.

11.2.25.1.2 AUDIOTEX - AUDTX

AUDTX lets you define 3 different Audiotex types.

- DAY: lets you access Audiotex voice guides for opening times.
- NIGHT: lets you access Audio voice guides for closing times.
- GDBYE: lets you access the Audiotex “Goodbye” announcement voice guide.

The following possibilities are offered:

- LISTEN: lets you listen to the Audiotex recorded or default voice guide.
- RECORD: lets you record a customized Audiotex voice guide.
- DEFAULT: lets you erase the recorded voice guide and replace it by the Audiotex default voice guide; this key is only provided if a recorded voice guide is available.
  Select YES (return to default voice guide) or NO.

11.2.25.1.3 BROADCASTING LISTS - LIST

LIST lets you customize broadcasting lists (51 possible lists including a general broadcasting list).

The following possibilities are offered:

- CLEAR: makes it possible to delete all data relative to a broadcasting list.
- EDIT: lets you create/modify the parameters of each broadcasting list.

  - ADD: lets you add a member to a broadcasting list.
  - PREV: lets you return to the previous member.
  - NEXT: lets you go on to the next member.
  - CLEAR: lets you delete a member from the list.
  - NAME: lets you modify the name allocated to the list
- LISTEN: lets you listen to the broadcasting list name.
- RECORD: lets you record the broadcasting list name.

11.2.25.1.4 GENERAL MAILBOX - GALMBX

GALMBX lets you define the general mailbox welcome message:

- LISTEN: lets you listen to the recorded or default welcome message.
- RECORD: lets you record a customized welcome message.
- DEFAULT: lets you erase the recorded welcome message and replace it by the default message; this key is only provided if a recorded message is available.
  Select YES (return to default message) or NO.

11.2.25.1.5 INFORMATION MESSAGES - INFMSG

INFMSG lets you record up to 50 information messages used by the Automated Attendant and the Audiotex service (opening or closing times).

- LISTEN: lets you listen to the recorded information message.
- RECORD: lets you record an information message
- PREV: lets you return to the previous message.
- NEXT: lets you go on to the next message.

Note:

Other parameters (message name, end of message response) have to be configured by OMC.

11.2.25.1.6 MESSAGE NOTIFICATION ANNOUNCEMENT - NOTIF

This feature makes it possible to define the announcement for a remote notification of messages:

- LISTEN: lets you listen to the recorded or default announcement.
- RECORD: lets you record a customized announcement.
- DEFAULT: lets you erase the recorded announcement and replace it by the default announcement; this key is only provided if a recorded announcement is available.
  Select YES (return to default announcement) or NO.

Chapter 12

Maintenance Services

12.1 Problem-Solving Methodology

12.1.1 Maintenance

12.1.1.1 MAINTENANCE

WARNING

A USER IS NOT AUTHORIZED TO WORK ON THE CABINET.
ONLY A REPRESENTATIVE OF THE INSTALLER IS AUTHORIZED TO WORK ON THE CABINET.

This section does not deal with failures caused by configuration errors nor with those caused by errors in the telephone features.

In either of these cases, refer to the sections on MMC-Station and Telephone Features.

In all cases, a thorough knowledge of the system (architecture, distribution of function processing, etc.) and of its telephone features is essential, and in particular the limits of these features.

Errors concerning distribution must be eliminated first.

To avoid taking a wrong track when determining faults, it is vital to define the source of the fault from the outset:

- operating error by the user
- programming error by the user or operator
- programming error in implementation
- genuine system failure

12.1.1.2 TROUBLESHOOTING PROCEDURE

For any system failure, it is essential to make visual checks (LEDs for the various boards, data testing, automatic set testing), to check the power supply voltage (electrical and battery) and to read the system messages.

The procedure is as follows:

- locate the terminal(s) affected by the fault. If several terminals are affected by the same fault, determine the common link which might be the cause (logical numbers of the same board, geographical distribution, same type of programming, etc.)
- determine at what level the error is occurring (internal or external call, etc.).

12.1.1.3 EXTENT OF FAILURE

A failure may be characterized by various aspects:

- Total system failure:
  - In this case, the fault can only be located in the module
  - The failure is most likely to come from the power supply or from the CPU (control unit); the next most likely cause is a set or network interface board interfering with the CPU.
- Total failure of a group of sets:
  - if all the sets are on the same board, then the fault probably lies in the board
  - if all the sets go out on the same cable, then the fault probably lies with the cable.
- Total failure of a single terminal: the fault is probably in the set itself. If not, check the equipment in question.
- Partial failure of a single terminal: the fault is probably due to the configuration or mode of operation.

12.1.1.4 DELIBERATE REPRODUCTION OF DEFAULTS

To make sure that your analysis of the fault is correct, it is essential to try to repeat the failure intentionally, unless it is unequivocal and permanent.

Once the fault is observed or repeated, and depending on the presumed source of the failure, replace the faulty item with a working one and try to repeat the original fault again.

If the fault remains, perform a complete analysis of the failure again.

12.1.1.5 LOCATING ERRORS

Power supply problem

If the electrical and battery operation LEDs are both out, check all the fuses.

If the fuses are OK, this means that the duration of the electrical power outage has been longer than the battery autonomy.

CPU board problem

If the CPU board LEDs are off, or are on steady, the system control unit is not working.

Miscellaneous

For any fault signaled on a terminal (set, add-on module or optional terminal such as a printer, etc), the following operations will be necessary:

- Test of the maintenance terminal in place of the failed terminal
- Test of the terminal at the module level

12.1.1.6 ELEMENT SUBSTITUTION

12.1.1.6.1 RULES TO RESPECT

Any substitution (power supply, CPU/CoCPU/MEX boards) must be performed with the system powered down.

With OMC, you can save and subsequently restore the configuration (see "Data Saving").

If replacing a PRA board, make sure that the configuration of the new board is consistent with the old one.

12.1.1.6.2 Powering up/down the system

- Press the ON/OFF button.
- Wait for the LED to go to steady red (about 30 seconds): system powered down
- Press ON/OFF to power up again after intervening (with the boards plugged back in). Wait 3 to 4 minutes for the system to initialize completely.

12.2 Board Management

12.2.1 Maintenance

12.2.1.1 GENERALITIES

The following conditions require maintenance to handle boards after these are accepted:

- First appearance in the system:
  - System configuration aspect when a new board is detected.
  - Initialisation and start-up of the corresponding hardware.
- Dynamic appearance or disappearance due to physical causes:
  - Warm system reset
  - Board plugged/unplugged while the system is running
  - Problems detected requiring actions on the corresponding board
- Dynamic appearance or disappearance due to logical causes (MMC commands)

The following rules apply:

- Any detected board is considered by the maintenance as PRESENT.
- A PRESENT board can be considered as ACCEPTED or REFUSED depending on the system dimensioning or power budget criteria.
- On cold reset, all the PRESENT boards are acknowledged (accepted or refused).
- Hardware decrease aspects are only applied at cold reset. A board seen as PRESENT on cold reset might not be detected on warm reset (board detection failure or board unplugged). In such a situation, such a board is considered by maintenance as ABSENT (the board configuration data is still available) after warm reset.

12.2.1.2 SYSTEM WITH A SOFTWARE VERSION OLDER THAN R2.0

The system should always be powered down before plugging/unplugging a board.

12.2.1.2.1 Plugging a board

When a board is plugged, the system assigns numbers to the board equipment (user directory numbers or line numbers); these numbers are assigned in ascending order of free system numbers. The board equipment is initialised with the corresponding default configuration.

When a board is plugged into a slot previously taken up by another board, this board is managed in the following way:

- if the new board is of the same type (same scan point) as the board previously plugged, the new board is assigned the same data (numbers and configuration) as the previous one.
- if the new board is different from the previous one, the system deletes the previous board

and associated data (the numbers assigned are now available and the default configuration is cancelled). The new board is then recognized as if it was plugged into a free slot (the equipment numbers are assigned in ascending order and the board initialised with the default configuration corresponding to the new board type).

12.2.1.2.2 Unplugging a board

In general, unplugging a board from the module does not trigger an update of the data assigned to the board (directory numbers, key programming, line parameters, etc.) ; the unplugged board is considered as "absent and accepted" (it is taken included when the system checks the equipment limits) as long as no other board is plugged into this slot or a cold reset performed on the system.

12.2.1.3 SYSTEM WITH A SOFTWARE VERSION FROM R2.0

Except for power and CPU/CoCPU/MEX, any board can be plugged/unplugged when the system is powered up.

Before unplugging or plugging a CoCPU-1/CoCPU-2 board, it MUST be switched off using the On/Off button on this board.

Interface boards can be replaced on a powered-up system if their OBC's version allows it (version legible by OMC -> Hardware and Limits).

- **from the 2.006 version for old boards.**
- **from the 3.003 version for the APA, LANX-1, UAI16-1, SLI-1 boards.**

12.2.1.3.1 Plugging a board

- **Plugging a board in an unused environment:**The board is considered as "present, accepted or refused"; it depends on the various configuration settings: authorised or unauthorised slot, equipment limits, software keys, etc. A "present and accepted" board is taken into account by the system.
- **Plugging a board into a slot which was previously used by a similar board with the same number of interfaces or accesses:** The data related to the old board are not deleted; the new board is considered as "present, accepted or refused" with the same number of accesses or interfaces as the previous board.
- **Plugging a board into a slot which was previously used by a different board or by a similar board with a different number of interfaces or accesses:** All the data related to the old board are deleted; the new board is then considered as if it had been plugged in a new slot.

12.2.1.3.2 Unplugging a board

If the board is unplugged when it is in "present and accepted" status, it is deactivated and declared "absent"; the other data related to the board configuration remain unchanged. The processing is the same for a board in a "present but refused" state, but that board will not be deactivated.

Note:

In case of a "gentle" plugging-in, it is possible that the plugged board may not be detected by the CPU board or detected with the wrong slot number.

In online Mode, if OMC does not automatically detect a plugged/unplugged board on a powered-up system, the session should be closed, then restarted for the board to be included.

12.2.1.4 ASSIGNING DIRECTORY NUMBERS

At start up, a default telephone number is associated to each internal and virtual extension, according to the default numbering plan and following the order of appearance of the interfaces and their extensions:

The interfaces appear in the same order as the boards, so the order in which the system gives a number to each interface is the following:

- The master cabinet extension board interfaces.
- The first satellite cabinet extension board interfaces if present.
- The second satellite cabinet extension board interfaces if present.
- The Mini-MIX daughter board interfaces if present.
- The virtual board interfaces (XRA, DECT, badge, IVPS, IP).

At the end of the start up, the next numbers are assigned to the sub-device extensions according to their order of appearance.

The order of appearance is the same for every sub-device and the device to which it is attached.

Example:

We have a system with 2 cabinets:

- a master cabinet with a 16UA extension board.
  The UA set connected to the first interface has a V24 sub-device.
  The UA set connected to the last interface also has a V24 sub-device.
  2 IVPS ports.
- a satellite cabinet with a 16UA extension board.
  The UA set connected to the first interface has a V24 sub-device.

After the system is started, 10 DECT handsets are added using MMC.

In the above configuration, and with a 3-digit numbering plan, the phone numbers are assigned as follows:

- From 101 to 116 to the UA interfaces on the master cabinet.
- From 117 to 132 to the UA interfaces on the satellite cabinet.
- Numbers 133 and 134 to the IVPS ports.
- Numbers 135 and 136 to the V24 sub-devices on the master cabinet.
- Number 137 to the V24 sub-devices on the satellite cabinet.
- From 138 to 147 to the DECT handsets.

Example:

We have an XS-N with an AMIX board, a main CPU-3m with a Mini-MIX daughter board.

For sets, the numbering order is:

- UA of AMIX.
- Z of AMIX.
- Z of Mini-MIX.

- VMU ports, RA.

For trunks, the numbering order is:

- Trunks of AMIX.
- T0 of Mini-MIX.

Advantages

- This numbering order associates the phones numbers with the devices following their physical positions in the 3 cabinets.
- No undetected interface (because of an underequipped board) gets a telephone number. Therefore, no telephone number is wasted.
- DECT handsets can be created through MMC, after the system is started. The corresponding phone numbers follow the number given to the sub-device last detected.
- In case of a Mini-MIX, the Z interfaces are not always in the operator group.

Drawback

An interface connected to no device is given a number.

12.2.1.4.1 Configuration checks

If there are hardware or configuration changes, the following limits are checked (for detailed quantifications, please see "Capacities and limits" in the "Product Presentation" section):

- **Maximum number of corded interfaces:** Any additional interface will be refused.
- **Maximum number of directory numbers:** Any attempt to add another number will be rejected. The directory numbers assigned to the auxiliaries (VMU, XRA, etc) are not covered by these checks, and are always accepted.
- **Maximum number of D-channels (T0/T1/T2/DASS2 interfaces):** Any additional interface (T0) or board (PRA) will be refused.
- **Maximum number of B-channels (TLs, ISDN access, VoIP access):** any attempt to add another interface will be rejected (and the interface containing the B-channel in question declared out of service).

12.2.1.5 INITIALISING SETS

On powering up, dedicated sets execute a self-test:

- display test
- test of the LEDs or icons of the set and add-on module, if any
- audio test

12.3 Replacing/Relocating Sets

12.3.1 Maintenance

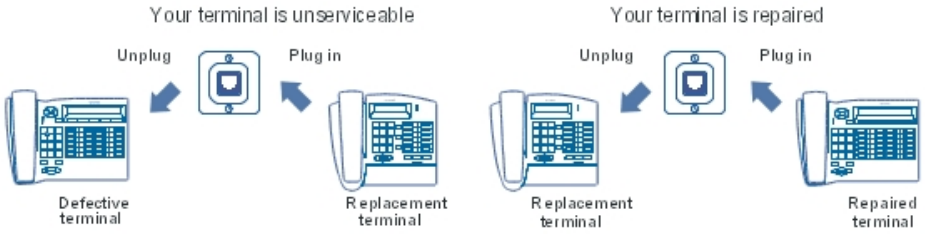
12.3.1.1 REPLACING A SET

You can replace your digital set by connecting a set of the same family, but of a different type, into your phone socket. This substitution can be temporary or permanent.

Replacing an analog set by another analog set, or replacing a digital set by a set of the same type, requires no special procedure (simple hardware exchange).

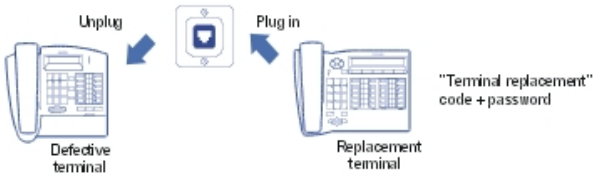
12.3.1.1.1 Temporary substitution

The replacement set keeps its own default functions (customized settings are not transferred). The data not transferred are stored in the Alcatel-Lucent OmniPCX Office Communication Server system until a set of the same type as the initial one is connected.



12.3.1.1.2 Permanent replacement

The maximum quantity of data from the initial set is transferred to the replacement. Data not transferred are deleted.



12.3.1.1.3 Characteristics preserved during temporary or permanent set substitution

- Rights (restricted features)
- Barring level
- Metering profile
- Messages and last caller repertories
- Destination set for metering reminder, forwarding and/or monitoring
- Set belonging to a hunting group and/or a Manager-Secretary relation
- Appointment reminder
- Locked or unlocked set
- Callbacks
- Active forwarding

- Last number redial

12.3.1.1.4 Data preserved during permanent set replacement

Replacement of digital sets

Regardless of the type of the initial digital set and that of the replacement, the function and resource keys are not preserved. The directory numbers are preserved in accordance with the size of the directories of the stations concerned (for example, when replacing a Advanced Reflexes set with a Premium Reflexes set, only the first 10 numbers are preserved).

Note 1:

The add-on modules are always transferred provided the substitution set supports these modules.

Note 2:

It is possible to replace a Reflexes set with an Alcatel-Lucent 9 series set. It is not possible to replace an Alcatel-Lucent 9 series set with a Reflexes set.

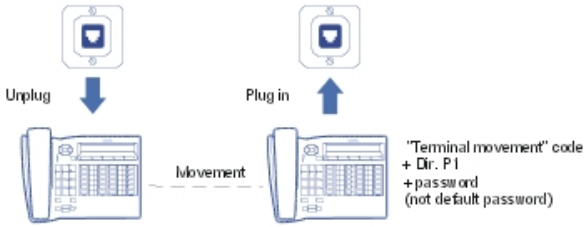
12.3.1.2 RELOCATING A SET

If you move office, you can move your set from one socket to another and still preserve all or part of its settings.

Before relocating the set:

- You need to change the personal code, which must be different from the default code.
- It is advisable to lock the set.

12.3.1.2.1 Relocating a set to an unused socket



12.3.1.3 ADDING SETS

When adding sets, attention must be paid to the limits on the number of sets and the features offered by the system software key.

The set is recognized as soon as it has been plugged into the socket.

12.4 Data Saving

12.4.1 Maintenance

12.4.1.1 OVERVIEW

Configuration backup

The backup operation concerns all the parameters not reinitialised during a warm reset:

- global data (software version, backup time and date, etc.)
- configuration data (types of boards and terminals, characteristics of terminals and groups, keys and directory settings, numbering plans, directory, Class of Service restrictions tables)
- data recorded by users (mail, appointment reminders, forwarding)
- call details counters

The configuration data backup can be activated in either of the following 2 ways:

- manually by the installer (OMC or MMC-Station backup command)
- automatically and periodically, at a time programmed by the installer, using OMC or MMC-Station

The backup session is exclusive of any OMC or MMC-Station operation or customization session; any modification is ignored during backup; avoid any activation or inhibition of services (appointment reminders are not protected, forwarding and filtering are refused) which would modify the settings.

Any system data modification and any hardware modification by OMC or MMC-Station must be followed by a backup.

Duration of a backup session: more than a minute for a multi-module installation or an installation with Internet services.

At the end of the session, a message appears in the hardware message table (to signal failure) or in the system history table (to signal success).

Configuration restore

The restore session is activated manually by the installer (OMC or MMC-Station restore command). All the saved data are restored.

Duration of a backup session: more than a minute for a multi-module installation or an installation with Internet services.

At the end of the session, a message appears in the hardware message table (failure indication) or in the system history table (success indication).

12.4.1.2 CONFIGURATION

- **Manual backup:**

- by OMC (Expert View): **Data Saving & Swapping -> Commands** -> check Backup
- by MMC-Station: **DatSav** -> **ManBkp**

- **Automatic backup:**

- by OMC (Expert View): **Data Saving & Swapping -> Data Saving** -> Enter date, time and periodicity
- by MMC-Station: **DatSav** -> **AutBkp** -> Enter date, time and periodicity

- **Restore:**

- by OMC (Expert View): **Data Saving & Swapping -> Commands** -> check Immediate Restore
- by MMC-Station: **DatSav** -> **Restor**

12.5 System Messages

12.5.1 Maintenance

The system messages are divided into 2 tables:

- the hardware message table
- the history message table

12.5.1.1 INTERFACE MARKERS

XX # 1 for the first half-board of slot XX, XX # 2 for the second half-board, XX - YY for the YY access of slot XX, ***** concerning the system messages.

A board can be cut into 2 half boards, this means that the same board uses 2 LCP codes (one per half-board). The 2 half boards may or may not be identical.

12.5.1.2 FORMAT OF SYSTEM MESSAGES ON Advanced Reflexes SETS

To see the messages, go into an Installer session and choose the GLOBAL feature out of the available features. Choose the MAINTE sub-feature, then RDHIST to read the history messages, RDANOM to read the hardware messages, or RRANOM to empty the hardware messages table.

30-12 15 : 30 106 ** 01030000 001/005**

- 30-12 : date
- 15 : 30 : time
- 106 : type of message
- **** : location (XX - YYY: access YYY of slot XX, *****: system)
- 01030000 : INFO 0 to INFO 3 hexadecimal (INFO 0 = 01; INFO 1 = 03; INFO 2 and 3 = 00)
- 001 / 005 : message index in relation to the total number of saved messages

12.5.1.3 HARDWARE MESSAGES

All of the hardware faults detected locally by a board or by the CPU board are listed in this table.

When the table is full, a new fault is stored in place of the most recent message (the table may be emptied by an OMC command or by cold starting the system).

Type	Message	Location	Additional Information	Action
5	CONFIGURATION BACKUP FAILURE			Check the configuration
9	CONFIGURATION RESTORATION FAILURE			Check the configuration
33	KEY REDUCED The features normally associated with the active key have been reduced due to a hardware problem (CPU type, insufficient memory, etc).	CPU board (80)	INFO 0 = reduced feature set index - 01 : VMU storage capacity diminished - 02 : number of VMU and Automated Attendant ports diminished - 03 : Automated Attendant unavailable - 04 : Audiotex unavailable - 05 : welcome messages unavailable - 06 : distribution list names unavailable - 07 : recording of conversations unavailable - 08 : duration of please-wait message diminished - 10 : number of NMC metering statements diminished - 12 : number of languages diminished	
50	ISDN ACCESS REBOOT PROBLEM	Board location. Interface marker	INFO 0 = D-channel	
51	CLOCK PROBLEM Clock synchronisation problem detected on an add-on module interface	Board location. Access marker	INFO 0 = type of interface: T0, T2, DASS2, etc.	Check there is no synchronising access in the add-on modules
52	SPECIFIC ACCESS PROBLEM DETECTED BY AN ISDN BOARD LEVEL 2	Board location. Access marker	INFO 0 =1: FCS (Frame Check Sequence) 2: CRC (Cyclic Redundancy Check)	If the fault recurs frequently, check the connection to the public network.

Type	Message	Location	Additional Information	Action
53	ALARM DETECTED ON A PRIMARY ACCESS	Board location. Access marker	INFO 0 = XX : type of alarm - 00 : Level 1 synchronised; all systems go. - 01 : Synchronisation loss in "multiple frame" mode (synchronisation in "double-frame" mode is correct). - 02 : No multiple frames; T2 automatically starts "double-frame" mode. - 03 : RDS (...) - 04 : Remote Frame Alarm. - 05 : Synchronisation loss in "double-frame" mode. - 06 : Alarm Indication Signal; sequence of "1's received, interface not synchronised. - 07 : Loss of Frame Alignment (occurs when the cable is disconnected). - 08 : Temporary clock lag; synchronisation established. - 09 : Error rate; number of error frames > 5 in 1 second. - 10 : Erroneous frames received in the checksum (CRC). - 11 : The network emits this alarm when the FALC sends erroneous frames in the CRC.	Ensure that the alarm disappears. If the fault recurs frequently, check the connection to the public network.
54	EXTERNAL FAULT ON S0 External problem detected on an S0 access following release message giving cause as "deactivation of level 1"	Board location. Access marker		
55	INTERNAL FAULT ON S0 Internal problem detected on an S0 access following release message giving cause as "deactivation of level 1"	Board location. Access marker		If the fault keeps recurring, check the bus wiring.
58	ISDN BOARD FAULT A level 1 error was detected by the board's OBC	Board location. Access marker	INFO 0 = type of error (not significant)	If the fault keeps recurring, check the bus wiring.

Type	Message	Location	Additional Information	Action
72	UNSUCCESSFUL ATTEMPT TO PRINT Message sent by the output device (printer) after every 5 failed print attempts.			Check the printer and its connection cable.
103	OBC FAULT	Board location.	INFO 0 and 1 = type of fault	
200	4070 IO/EO BASE: SLAVE LINK CONNECTED TO INVALID INTERFACE	Board location. Interface marker	INFO 0 = interface number invalid INFO 1 = base station operating status	Check the cables on the 2nd link in the base station
201	4070 IO/EO BASE: FREQUENCY REJECTION Discrepancy between the number of frequencies configured by the installer and the number of DECT frequencies processed	Board location. Interface marker	INFO 0 to 3 = bitmap of frequencies authorised and in use For more information, refer to the "Installing 4070 IO/EO base stations", file in the "Mobility" section.	
202	4070 IO/EO BASE: LOSS OF SYNCHRONISATION ON UA LINK 0	Board location. Interface marker	INFO 0 = link status (0 = link KO; 1 = link OK)	Check cabling Replace the 4070 base station
203	4070 IO/EO BASE: LOSS OF SYNCHRONISATION ON UA LINK 1	Board location. Interface marker	INFO 0 = link status (0 = link KO; 1 = link OK)	Check cabling Replace the 4070 base station
204	4070 IO/EO BASE: NO REPLY ON DSP PRESENT (RESET)	Board location. Interface marker		
205	4070 IO/EO BASE: TRANSMISSION ERRORS DETECTED ON SERIAL LINK TO DSP (RESET)	Board location. Interface marker		
206	4070 IO/EO BASE: ERRORS DETECTED DURING INITIALISATION PHASE OF BOOT PROGRAM (RESET)	Board location. Interface marker		
207	4070 IO/EO BASE: ERRORS DETECTED DURING SOFTWARE DOWNLOAD PHASE	Board location. Interface marker		
208	4070 IO/EO BASE: TRANSMISSION BUFFER FULL	Board location. Interface marker		
209	4070 IO/EO BASE: TRANSMISSION BUFFER FULL	Board location. Interface marker		

Type	Message	Location	Additional Information	Action
210	4070 IO/EO BASE: A MESSAGE IS SENT TO THE BASE WITH A FALSE LINK IDENTITY	Board location. Interface marker		
212	4070 IO/EO BASE: WRONG LINE LENGTH	Board location. Interface marker		
213	4070 IO/EO: RECEPTION OF AN ERRONEOUS MESSAGE	Interface marker		
214	4070 IO/EO: RECEPTION OF AN ERRONEOUS FREQUENCY PLAN	Board location. Interface marker		
215	4070 IO/EO BASE: WRONG LINE LENGTH	Board location. Interface marker		
216	4070 IO/EO BASE: RECEPTION OF AN ERRONEOUS MESSAGE	Board location. Interface marker		
217	4070 IO/EO BASE: RECEPTION OF AN ERRONEOUS FREQUENCY PLAN	Board location. Interface marker		
220	DSP OUT OF SERVICE ON ONE OF THE BOARDS	Board location.	INFO 0 = DSP number INFO 1 = cause (resource problem, DSP overload, etc)	
239	STORAGE MEMORY CHANGED OR LOST	CPU (80)	INFO 0 = type of error - 0 : medium KO - 1 : medium full - 2 : checksum error - 3 : system file control error INFO 1 = type of medium - 0 : NAND FLASH CPU - 1 : NAND FLASH XMEM - 2 : HARD DISK INFO 2 = type of initial medium INFO 3 = assigned memory area (metering, alarms, voice prompts, etc)	
242	ERROR ON OPENING VOICE PROMPT FILE	CPU (80)	INFO 0 to 3 = type and value of voice prompt	
243	ERROR ON CLOSING VOICE PROMPT FILE	CPU (80)	INFO 0 to 3 = type and value of voice prompt	
244	ERROR ON READING VOICE PROMPT FILE	CPU (80)	INFO 0 to 3 = type and value of voice prompt	
245	ERROR ON WRITING VOICE PROMPT FILE	CPU (80)	INFO 0 to 3 = type and value of voice prompt	

Type	Message	Location	Additional Information	Action
246	ERROR ON OPENING VOICE PROMPT FILE	CPU (80)	INFO 0 to 3 = type and value of voice prompt	
247	ERROR ON OPENING VOICE PROMPT FILE	CPU (80)	INFO 0 to 3 = type and value of voice prompt	
248	DISCHARGED BATTERY OR BATTERY REPLACEMENT This results in an incorrect date/time	CPU (80)		
249	THE CPUe-1/CPUe-2 BOARD DOES NOT BOOT UP WITH THE HARD DRIVE. The system runs on Flash with reduced services.	CPU (80)		

12.5.1.4 HISTORY MESSAGES

The events identified by the codes in the system history messages table concern modifications to the system hardware configuration (appearance/disappearance of boards or terminals, refusal of a board on exceeding equipment limits) or other events (reset execution, buffer fill rate attained, etc).

When the table is full, a new event is stored in place of the oldest message.

This table is only emptied in the event of a cold system reset.

Type	Message	Location	Additional Information	Action
0	SYSTEM RESTART		INFO 0 = reason to restart 1 : MMC reset command 2 : reset due to hardware fault 3 to 5: reset following software problem 7 : reset following software licence problem (the values of the default key are used) 11 : reset following software swap or after restoration after swap 12 : too many one-way communications 13 : automatic restart programmed by MMC 14 : timeout expiration 55 : normal reset	

Type	Message	Location	Additional Information	Action
1	DOWNLOAD INFORMATION	CPU (80)	INFO 0 = information 1 : download started 2 : download finished 3 : download failure INFO 1 = cause of failure 0 : download complete 9 : invalid date 11 : file transfer error 14 : download incomplete	
2	SWAP INFORMATION Program change-over	CPU (80)	INFO 0 =1: swap complete; 2: data saving error; 3: fault during swap INFO 1 = type of swap: 0 : normal with data saving; 1: normal without data saving; 2: forced with data saving INFO 2 = acknowledgement: 0 : no problem; 1: save KO; 2: restore KO; 3: save/restore KO	
3	LAUNCH OF DATA SAVING Data Saving	CPU (80)		
4	DATA SAVING BACKUP OK	CPU (80)		
6	AUTOMATIC DATA SAVING BACKUP REFUSED MMC session was active	CPU (80)		End the MMC session. Save manually or wait for the next automatic save.
7	LAUNCH OF DATA RESTORE Data Saving	CPU (80)		
8	DATA RESTORE OK	CPU (80)		Check if the hardware configuration has been changed since the last backup
9	DATA RESTORE FAILED	CPU (80)		Check if the hardware configuration has been changed since the last backup
10	DATA SAVING REFUSED No data saving option	CPU (80)		
11	END OF START-UP The system is operational			

Type	Message	Location	Additional Information	Action
20	NOT ENOUGH MEMORY Available space < 15 %	CPU (80)		
21	FULL BUFFER MESSAGE	CPU (80)	INFO 0 = type of pool	
22	FLOW CONTROL ON MEMORY POOLS Alert level size of memory allocated to flow control on a memory reached	Board location	INFO 0 = type of pool INFO 1 = level (95 = exceeded 95 % threshold; 75 = gone under 75 % threshold)	
30	DBMS CRASH	CPU (80)	INFO 0 to 3 = causes of crash	
31	CURRENCY CONVERSION	CPU (80)	INFO 0 =1: conversion OK	
32	PRIORITY CALL	CPU (80)	INFO 0 = Directory Number High Byte , INFO 1 =Directory Number Low Byte	
34	SOFTWARE KEY CHANGE	CPU board (80)	INFO 0 = type of key (0= main key; 1 = CTI key) INFO 1 = type of event (see Information Displayed / Software key states) INFO 2 and 3 = Bytes corresponding to the acknowledgement code (respectively High and Low)	
35	PS-BOOST BOARD FAULT A PS-BOOST board problem has been detected	CPU board (80)	INFO 0 = type of error (1 = more than one boost present or boost in a small rack; 2 = no boost nor external feeding; 3 = external power loss; 4 = external power recovery)	
56	ISDN BOARD ACCESS The ISDN protocol management module detected a layer 1 problem on a T0 or T2 access	Board location. Access marker	INFO 0 = access status (0 = access KO, 1 = access OK) INFO 1 = type of access (03 = T0, 23 = DLT0)	
57	TEI DELETION	CPU (80)	INFO 0 = D-channel INFO 1 = TEI	Analyse the reason why the TEI was modified by the network carrier.

Type	Message	Location	Additional Information	Action
59	R_ANO_VOWLAN_ACCESS. Voice over WLAN access problems.		INFO 0 = Code of error: 1 = Rate of calls cut/total calls on system reached 5% 2 = Saturation time on one AP reached 1 minute 3 = Saturation number on one AP reached 3 times 4 = Rate of refused calls/total calls on system reached 5% 5 = Rate of calls cut/total calls on one handset reached 5% 6 = Rate of refused calls cut/total calls on one handset reached 5%	
70	PRINTER THRESHOLD K.O. Message emitted by the spooler when the array where the tickets are stored is 70% full			Check the printer and its cable connection
71	PRINTER THRESHOLD O.K. Message emitted by the spooler when the array where the tickets are stored is less than 70% full again			
90	ENTERING AN MMC SESSION	CPU (80)	INFO 0 =1: ADMINISTRATOR password; 2: INSTALLER password; 3: OPERATOR password; 5: GUARDED password	
91	END OF MMC SESSION	CPU (80)		
100	BOARD BACK IN SERVICE (Following a system stoppage or after being unplugged)	Board location	INFO 0 = type of board	
101	BOARD UNPLUGGED	Board location	INFO 0 = type of board (if known) INFO 1 = cause of rejection	
104	TEMPORARY BOARD RESET	Board location	INFO 0 =1: hardware fault; 2: no response from board; 3: fan fault; 4: running on battery; 5: licence problem; 6: maintenance problem; 7: reason unknown INFO 1 = cause of reset	
105	PERMANENT BOARD RESET	Board location.	INFO 0 =1: hardware fault; 2: no response from board; 3: fan failure; 4: running on battery; 5: licence problem; 6: maintenance problem; 7: reason unknown; 8: power supply problem INFO 1 = cause of reset	Disconnect and reconnect the board. If the fault persists, replace the board

Type	Message	Location	Additional Information	Action
106	BOARD REFUSED The board has been refused and, in the case of an intelligent board, a permanent reset is performed on it	Board location	INFO 0 = type of board INFO 1 = cause of refusal (See Information Displayed / Reasons for board refusal)	Check the hardware configuration (the system limits may have been exceeded).
107	MMC BOARD RESET The reset of an interface board processor has been requested by MMC	Board location		
108	POWER OFF: LAUNCH OF BACKUP PROCEDURE FOR A BOARD	Board location		
109	BOARD INFO CLEARED BY OMC	Board location		
110	APPEARANCE OF A TERMINAL A terminal has been recognised by the system. This terminal is now operational NB: this message will only be sent if the NMC is present and active	Board location. Interface marker	INFO 0 = type of terminal INFO 1 = reason for restarting	
111	DEVICE REFUSED Configuration limit attained	Board location. Interface marker	INFO 0 = type of device INFO 1 = cause of refusal INFO 2 = 1 (software licence problem; in this case, INFO 1 = 255 (terminal not totally refused, because recognised by MMC)	Check the hardware configuration (the system limits may have been exceeded).
112	FAULT ON A DEVICE	Board location. Interface marker	INFO 0 = type of device INFO 1 = type of error	If the fault recurs frequently, check the terminal and its connections.
113	INTERFACE REFUSED An interface was refused because the system limits were exceeded	Board location. Interface marker	INFO 0 =type of interface INFO 1 = cause of refusal	Check the hardware configuration (the system limits may have been exceeded).

Type	Message	Location	Additional Information	Action
120	CABINET OPERATIONAL	Controller board (81 or 82)	INFO 0 = type of backpanel board (3 = wall mounted; 4 = RACK1U; 5 = RACK2U; 6 = RACK 3U; 7 = RACK 1U G2; 8 = RACK 2U G2; 9 = RACK 3U G2; 10 = RACK XS; 11 = RACK XS-N INFO 1 = module operating mode (0 = restricted mode, running on battery; 1 = normal mode, running on the electrical power supply)	
121	CABINET REFUSED	Controller board (81 or 82)	INFO 0 = reason for rejection	
122	CABINET UNPLUGGED	Controller board (81 or 82)		
123	MAIN FAILURE	CPU (80)	INFO 0 = Main power supply state (0 = Electrical power supply KO - battery activated; 1 = Electrical power supply OK; 2 = System on battery, only with 2G power supply)	
124	FAN STATUS	CPU (80) or Controller Board (81) or (82)	INFO 0 = fan identity (0 = fan 1; 1 = fan 2) INFO 1 = fan status (True = OK; False = KO)	
125	POWER SAVING System in power-saving mode; only the 2 first Reflexes telephones as well as all T0 accesses will be taken into account		INFO 0 = module (0 = basic module; 1 = extension 1; 2 = extension 2) INFO 1 = reason (0 = Fan problem)	Check rotation of the module fans.
126	DSP RESOURCE KO Message not processed by the DSP of one of the controller boards	Controller board (81 or 82)	INFO 0 = DSP type 0 or 1 (DSP0 or DSP1)	
127	DSP RESULT CODES These codes are used in confirmation messages and by the reception buffer	Controller board (81 or 82)	INFO 0 = DSP type 0 or 1 (DSP0 or DSP1) INFO 1 = Result code INFO 2 = Result sub-code INFO 3 = Type of resource	
128	DSP KO The DSP of one of the controller boards is out of service.	CPU (80) or controller board (81 or 82)	INFO 0 = 0 or 1 (DSP0 or DSP1)	

Type	Message	Location	Additional Information	Action
129	CPU KO CPU board not detected by the backpanel board 10 minutes after initialisation		INFO 0 = type of CPU (0 = Internet access; 1 = VoIP) INFO 1 = number of CPU resets during the-10 minute period INFO 2 = CPU state INFO 3 = last byte of MAC (Ethernet) Internet address of CPU	
140	UN-REGISTRATION SIP un-registration	CPU (80)	INFO 0 = byte 1 of the IP address of the remote registry INFO 1 = byte 2 of the IP address of the remote registry INFO 2 = byte 3 of the IP address of the remote registry INFO 3 = byte 4 of the IP address of the remote registry	
141	REGISTER OK SIP registration success	CPU (80)	INFO 0 = byte 1 of the IP address of the remote registry INFO 1 = byte 2 of the IP address of the remote registry INFO 2 = byte 3 of the IP address of the remote registry INFO 3 = byte 4 of the IP address of the remote registry	
142	REGISTER 500 SIP registration failure (500: Server error)	CPU (80)	INFO 0 = byte 1 of the IP address of the remote registry INFO 1 = byte 2 of the IP address of the remote registry INFO 2 = byte 3 of the IP address of the remote registry INFO 3 = byte 4 of the IP address of the remote registry	
143	REGISTER 423 SIP registration failure (423: Interval too brief)	CPU (80)	INFO 0 = byte 1 of the IP address of the remote registry INFO 1 = byte 2 of the IP address of the remote registry INFO 2 = byte 3 of the IP address of the remote registry INFO 3 = byte 4 of the IP address of the remote registry	
144	REGISTER 400 SIP registration failure (400: Invalid request)	CPU (80)	INFO 0 = byte 1 of the IP address of the remote registry INFO 1 = byte 2 of the IP address of the remote registry INFO 2 = byte 3 of the IP address of the remote registry INFO 3 = byte 4 of the IP address of the remote registry	

Type	Message	Location	Additional Information	Action
145	REGISTER 403 SIP registration failure (403: Forbidden)	CPU (80)	INFO 0 = byte 1 of the IP address of the remote registry INFO 1 = byte 2 of the IP address of the remote registry INFO 2 = byte 3 of the IP address of the remote registry INFO 3 = byte 4 of the IP address of the remote registry	
146	REGISTER 404 SIP registration failure (404: Not found)	CPU (80)	INFO 0 = byte 1 of the IP address of the remote registry INFO 1 = byte 2 of the IP address of the remote registry INFO 2 = byte 3 of the IP address of the remote registry INFO 3 = byte 4 of the IP address of the remote registry	
147	REGISTER TIMEOUT SIP registration failure (Timeout)	CPU (80)	INFO 0 = byte 1 of the IP address of the remote registry INFO 1 = byte 2 of the IP address of the remote registry INFO 2 = byte 3 of the IP address of the remote registry INFO 3 = byte 4 of the IP address of the remote registry	
148	REGISTER FAILED SIP registration failure	CPU (80)	INFO 0 = byte 1 of the IP address of the remote registry INFO 1 = byte 2 of the IP address of the remote registry INFO 2 = byte 3 of the IP address of the remote registry INFO 3 = byte 4 of the IP address of the remote registry	
160	THRESHOLD HARDWARE TABLE The critical threshold (80 % by default) of the hardware fault table has been reached	CPU (80)		
161	THRESHOLD HISTORY TABLE The critical threshold (80 % by default) of the history fault table has been reached	CPU (80)		
162	THRESHOLD METERING TABLE The critical threshold (80 % by default) of the data metering buffer has been reached	CPU (80)		

Type	Message	Location	Additional Information	Action
163	THRESHOLD URGENT TABLE The critical threshold (80 % by default) of the urgent alarms table has been reached	CPU (80)		
164	HARDWARE TABLE FULL The hardware anomaly table is full	CPU (80)		
165	HISTORY TABLE FULL The history event table is full	CPU (80)		
166	METERING TABLE FULL The metering table is full	CPU (80)	INFO 0 = Origin (1 byte); 0 = Account ticket table; 1 = VoIP RTP ticket table	
167	URGENT TABLE FULL The urgent alarms table is full	CPU (80)		
168	NMC CONNECTION START The NMC application has established a connection with the PCX	CPU (80)		
169	NMC CONNECTION END The NMC application has ended the connection with the PCX	CPU (80)		
170	NMC NOT ALLOWED CALL NMC call by analog XRA (not allowed)	CPU (80)		
171	NMC ERRONEOUS CALL The PCX tried to establish a call to an NMC but it was erroneous	CPU (80)		
172	NMC NON ANSWERED CALL The PCX tried to establish a call to an NMC, but the call was not answered	CPU (80)		
173	NMC INFO TIMEOUT The PCX connected to an NMC and sent an INFO message saying that an urgent alarm should be read. The PCX did not respond to this message.	CPU (80)		
174	NMC PUT DATA TIMEOUT The PCX received no acknowledgement for the data sent in the message. The communication failed.	CPU (80)		
175	NMC WAIT ACK TIMEOUT The PCX received no acknowledgement for the establishment request sent to the NMC	CPU (80)		

Type	Message	Location	Additional Information	Action
176	NMC PHONE NB MISSING The PCX attempted to call the NMC to send urgent alarms, but the NMC number was not specified	CPU (80)		
177	ADDRESS NOT REGISTERED The PCX attempted to call the NMC, but the NMC refused the call because it didn't recognise the PCX	CPU (80)		
178	UNEXPECTED ALARM Unsuccessful anomaly translation for the NMC	CPU (80)		
190	UNKNOWN IPUI A GAP handset tried to access the PBK without being registered	CPU (80)	INFO 0, INFO 1, INFO 2, INFO 3 = corresponding byte of port identifier	
221	ETHERNET DOWN Ethernet interface of the IP-LAN board is down.	Board location. Ethernet interface marker.		Check the LAN connection and, if necessary, the LAN elements (hub, switch).
222	ETHERNET UP Ethernet interface of the IP-LAN board is working.	Board location. Ethernet interface marker.		
223	REMOTE GATEWAY DOWN Remote gateway is out of service.		INFO 0 to INFO 3: bytes corresponding to the IP address Network format	Check the IP connectivity to the remote gateway (LAN, intermediate IP router) and the remote gateway status.
224	REMOTE GATEWAY UP Remote gateway is working		INFO 0 to INFO 3: bytes corresponding to the IP address Network format	

Type	Message	Location	Additional Information	Action
225	GATEWAY TRAFFIC Too much traffic to the remote gateway xxxxx	CPU (80)	INFO 0 to INFO 3: bytes corresponding to the IP address Network format	If this alarm keeps recurring, increase the bandwidth associated with the gateway in the ARS table, and the number of DSPs assigned to VoIP access.
226	EXTERNAL GATEKEEPER INACCESSIBLE			Check the IP connectivity to the remote gatekeeper (LAN, intermediate IP router) and check that the remote gatekeeper is online.
227	NOT ENOUGH IP TRUNK VoIP call refused: no DSP channel available	CPU (80)		If this alarm keeps recurring, increase the number of DSPs assigned to VoIP access, or increase the bandwidth in the ARS, or add a CoCPU@ + VoIP board.

Type	Message	Location	Additional Information	Action
228	NOT ENOUGH DSP VoIP telephony failure: no DSP channel available.	CPU (80)		If this alarm keeps recurring, increase the number of DSPs assigned to the IP user pool (decrease the number of VoIP-access DSPs or add a CoCPU@ + VoIP board).
229	NO MORE TSC IP DYN ADDRESS TSC/IP phone cannot be initialised due to a DHCP problem			Increase the number of IP addresses in the DHCP server range (this address range must be greater than or equal to the number of IP Enablers to be installed).
230	EXTERNAL GATEKEEPER REJECTED			
231	IA EMAIL Anomaly sent if the call handling receives a log from IA concerning e-mail features.	CPU (80)	INFO 0 = Type of alert. INFO 1 = Log unique identifier High Byte INFO 2 = Log unique identifier Low Byte	
232	IA SECURITY Anomaly sent if the call handling receives a log from IA concerning security features.	CPU (80)	INFO 0 = Type of alert. INFO 1 = Log unique identifier High Byte INFO 2 = Log unique identifier Low Byte	
233	IA NETWORK Anomaly sent if the call handling receives a log from IA concerning network features.	CPU (80)	INFO 0 = Type of alert. INFO 1 = Log unique identifier High Byte INFO 2 = Log unique identifier Low Byte	

Type	Message	Location	Additional Information	Action
234	IA ACCESS Anomaly sent if the call handling receives a log from IA concerning access features.	CPU (80)	INFO 0 = Type of alert. INFO 1 = Log unique identifier High Byte INFO 2 = Log unique identifier Low Byte	
235	IA REMOTE ACCESS Anomaly sent if the call handling receives a log from IA concerning remote access features.	CPU (80)	INFO 0 = Type of alert. INFO 1 = Log unique identifier High Byte INFO 2 = Log unique identifier Low Byte	
236	IA DATA CONFIGURATION Anomaly sent if the call handling receives a log from IA concerning configuration data features.	CPU (80)	INFO 0 = Type of alert. INFO 1 = Log unique identifier High Byte INFO 2 = Log unique identifier Low Byte	
240	NO VOICE MESSAGE AVAILABLE Anomaly sent at the init if the BIOS does not detect the whole RAM.	CPU (80)	INFO 0 = number of megabytes of DRAM detected by the BIOS.	
241	VMU MEMORY THRESHOLD The voice message recording memory area is nearly full.	CPU (80)	INFO 0 = 1 (ON) if there are just a few minutes of recording time left; 0 (OFF) end of the anomaly.	
250	START-UP SCRIPT Anomaly sent when an error in the Linux start-up script occurs.	CPU (80)	INFO 0 = Error line / 256 INFO 1 = Error line mod. 256 INFO 2 = Critical error INFO 3 = Status	
251	R_NOE_DLD_SUCCESS Alcatel-Lucent 9 series downloading successful.	CPU (80)	INFO 0 = Device type INFO 1 = Files downloaded: one bit for each kind of file.	
252	R_ANO_NOE_DLD_FAIL Alcatel-Lucent 9 series downloading unsuccessful.	Board location. Interface marker	INFO 0 = Device type INFO 1 = Phase of failure INFO 2 = Reason of failure INFO 3 = Files downloaded failure	
255	R_OVERLOADED_TRUNK_ OUTCALL_FAILED An outgoing call could not be set up because the trunk group was overloaded.		INFO 0 to INFO 3: displays the trunk group information. Exception: comp info: FF FF FF FF No trunk group no. is available (Error in configuration).	

12.5.1.5 INFORMATION DISPLAYED

The information given below concerns the hardware messages as well as those contained in the system history.

12.5.1.5.1 TYPES OF BOARD (INFO 0 of messages 100, 101, and 244)

- Boards R1.0 and R1.1
  82H : integrated voice server

9EH : SLI board
A0H : UAI board
A1H : PRA board = E1
A2H : PRA board = DLE1
A3H : PRA board = T1
A4H : PRA board = DASS2
A7H : virtual XRA board
B0h : main or applications CPU board
B1H : MIX board
B2H : BRA board
B3H : LanX board
96h : ATA board (Analog lines)

- Additional boards R2.0
  B4h : APA board (Analog lines)
  B5h : T1 CAS board
  B6h : LanX-1 board
  B7h : UAI-1 board
  B9h : DDI board
- Additional boards R2.1
  A5h : PRA board = PCM
  B9h : SLI-1 board (legerity)
  BAh : SLI-1 board (ST)
- Additional boards R3.0
  BBh : Media virtual board
  BCh : LANX-2 board
  BDh : MIX-1 board (Legerity)
  BEh : MIX-1 board (St)
- Additional boards R3,1
  BFh : AMIX-1 board (Legerity)
  C0h : AMIX-1 board (St)

12.5.1.5.2 TYPES OF TERMINAL (INFO 0 of messages 111 and 112)

Types of terminal	Value of INFO 0 in message 111 and 112

	Before R3.1	R3.1	R4,0/R4,1	R5.0	R5.1
4034 1G set	00h	00h	00h	00h	00h
4023 1G set	02h	02h	02h	02h	02h
4034 2G set	06h	06h	06h	06h	06h
5028 set	07h	07h	07h	07h	07h
4023 2G set	08h	08h	08h	08h	08h
4012 set	0Ah	0Ah	0Ah	0Ah	0Ah
5022 set	0Bh	0Bh	0Bh	0Bh	0Bh
4011 set	0Ch	0Ch	0Ch	0Ch	0Ch
4001 set	0Eh	0Eh	0Eh	0Eh	0Eh
5010 set	0Fh	0Fh	0Fh	0Fh	0Fh

5018 set	12h	12h	12h	12h	12h
5015 set	14h	14h	14h	14h	14h
4003 set	15h	15h	15h	15h	15h
4088 adapter	16h	16h	16h	16h	16h
First set	17h	17h	17h	17h	17h
Easy set	19h	19h	19h	19h	19h
Premium set	1Bh	1Bh	1Bh	1Bh	1Bh
Advanced set	1Dh	1Dh	1Dh	1Dh	1Dh
4070 IO base station	1Fh	1Fh	1Fh	1Fh	1Fh
4099 Multi Reflexes	20h	20h	20h	20h	20h
4070 PWT base station	22h	22h	22h	22h	22h
Alcatel-Lucent 4019 Digital Phone set	n/a	n/a	23h	23h	23h
Alcatel-Lucent IP Touch 4018 Phone set	n/a	24h	24h	24h	24h
Alcatel-Lucent 4029 Digital Phone set	n/a	n/a	25h	25h	25h
Alcatel-Lucent IP Touch 4028 Phone set	n/a	25h	25h	25h	25h
Alcatel-Lucent 4039 Digital Phone set	n/a	n/a	26h	26h	26h
Alcatel-Lucent IP Touch 4038 Phone set	n/a	26h	26h	26h	26h
Alcatel-Lucent IP Touch 4068 Phone set	n/a	27h	27h	27h	27h
Alcatel-Lucent Mobile IP Touch 300/600	n/a	n/a	n/a	28h	28h
Alcatel-Lucent IP Touch 4008 Phone set	n/a	n/a	n/a	n/a	29h
4081/4090 L 40-key add-on module	23h	28h	28h	29h	2Ah
4081/4090 M 20-key add-on module	24h	2Ah	2Ah	2Bh	2Ch

10-key add-on module for Alcatel-Lucent 8 series/Alcatel-Lucent 9 series sets	n/a	2Ch	2Ch	2Dh	2Eh
40-key add-on module for Alcatel-Lucent 8 series/Alcatel-Lucent 9 series sets	n/a	2Dh	2Dh	2Eh	2Fh
4091 MAC/PC option (Reflexes 2G set)	25h	2Eh	2Eh	2Fh	30h
External alphanumeric keyboard for Reflexes set	26h	2Fh	2Fh	30h	31h
4093 V24 option (Reflexes 3G set)	27h	30h	30h	31h	33h
4095 Z option (Reflexes 3G set)	29h	32h	32h	33h	34h
DECT option (Reflexes 3G set)	2Ah	33h	33h	34h	35h
4094 S0 option (Reflexes 3G set)	2Bh	34h	34h	35h	36h
Z standard 2-wire set	2Ch	35h	35h	36h	37h
Z class standard 2-wire set	2Dh	36h	36h	37h	38h
Alcatel-Lucent GAP DECT handset without display	2Eh	37h	37h	38h	39h
Alcatel-Lucent GAP DECT handset with 16 character-display	2Fh	38h	38h	39h	3Ah
Third-party DECT GAP handset without display	30h	39h	39h	3Ah	3Bh
Third-party DECT GAP handset with 16 character-display	31h	3Ah	3Ah	3Bh	3Ch
Reflexes set + 4097 CBL adapter	32h	3Bh	3Bh	3Ch	3Dh
4073 set	33h	3Ch	3Ch	3Dh	3Eh
Mobile Reflexes 100/200 set	34h	3Dh	3Dh	3Eh	3Fh
4073 PWT set	35h	3Eh	3Eh	3Fh	40h

Mobile Reflexes MR300 set	n/a	n/a	n/a	n/a	41h
Mobile Reflexes MR400 set	n/a	n/a	n/a	n/a	42h
CSTA virtual set	37h	40h	40h	41h	44h

12.5.1.5.3 REASONS FOR BOARD REFUSAL (INFO 1 of message 106)

01H : consumption limits exceeded

04H : unknown board type

05H : board refused

06H : no primary access in basic module

07H : feature denied (rights linked to licence)

08H : max. number of applications CPUs attained

09h : board cannot be initialised

0Dh : max number of CoCPU RA exceeded

0Fh : max number of trunks on mixed boards exceeded

12.5.1.5.4 REASONS FOR TERMINAL REFUSAL (INFO 1 of message 111)

04H : exceeding the max number of corded interfaces in the system

05h : exceeding the use of terminals

06H : UA devices exceeded (2 add-on modules per set and 4 options)

07H : total number of terminals exceeded

08H : number of users exceeded

09H : max. number of B-channels exceeded

0AH : max. number of T0 accesses exceeded

0BH : max. number of primary accesses exceeded

0CH : max. number of multi UA reached

0DH : incompatible terminal

0EH : number of programmable keys exceeded

0FH : memory capacity exceeded

10H : number of S0 accesses exceeded

11H : unauthorized terminal

12h : number of DLT0 accesses exceeded

13H : number of DLT2 accesses exceeded

19H : max. number of DECT base stations exceeded

21h : B channel init failed

22h : max. number of analog trunks reached for a cabinet

23h : max. number of analog trunks reached for the system

24h : maximum of resources reached

1CH : exceeded equipment level in module in terms of available energy

1DH : exceeded max. number of HSL resources in a module

1EH : exceeded max. number of HDLC resources for the overall system

1FH : exceeding max number of analog lines in a module (RackX)

20H : exceeding the max number of analog lines in the system

12.5.1.5.5 Additional information contained in message 112 (INFO 1: type of error)

This message only concerns the Reflexes stations.

60h : unequipped station

61h : transmission of erroneous message

62h : bad checksum message

63h : occupation of UA link

64h : receipt of a reset

65h : out of order option dedicated handset

66h : unplugging of the handset

67h : maintenance seized handset

12.5.1.5.6 TYPES OF INTERFACE (INFO 0 of message 113)

01H : analog set interface

03H : T0 access interface

04H : T2 access interface

05h : S0 set interface

14H : Reflexes set interface

20H : master DECT base interface

21H : slave DECT base interface

22H : DECT Reflexes interface

25H : Multi Reflexes interface

26H : IP interface

27h : IP network interface

28h : TSC IP set

29h : IA access on IA board

2Ah : PCM digital network interface

2Bh : PCM analog network interface

2CH : RAS access on RAS board

2Dh : T1-CAS digital network interface

2Eh : T1-CAS analog network interface

2Fh, 30h, 31h, 32h : MSG1 to MSG4 interfaces

34h : Audio In interface

35h : Audio Out interface

36h : General bell interface

3Eh : integrated analog modem interface

3Fh : integrated ECMA modem interface

40h : integrated IA access

41h : integrated RAS access

1Dh : "integrated voice mail" interface

12.5.1.5.7 Software key states (Info 1 of message 34)

01 : system boot; the current key does not correspond to the system (wrong serial number): the services are open for a limited time.

02 : system booted with a valid key.

03 : system booted with a key problem. The services are closed.

04 : system boot; the current key version does not correspond to the system software version: the services are open for a limited time.

05 : system boot; the current key version does not correspond to the system software version; the end of the limited period causes the services to close.

06 : system boot; the current key is too old; the services are open for a limited time.

07 : system boot; the current key is too old; the end of limited time causes the services to close.

12 : valid key entered.

13 : the current key does not correspond to the system (invalid serial number); end of limited time causes the services to close.

14 : serial number problem with the system key; a new key with a valid serial number but with a version which does not correspond to system software version has been entered: the services are open for a limited time.

16 : serial number problem with the system key; a new key with a correct serial number but too old has been entered: the services are open for a limited time.

21 : the key entered does not correspond to the system: the services are open for a limited time.

24 : the software key entered does not correspond to system software version (invalid serial number): the services are open for a limited time.

26 : a software key with too old an edition has been entered: the services are open for a limited time.

32 : the services were closed; entering a valid key causes the services to open.

35 : the services were closed; the new key entered has a valid serial number but a version which does not correspond to the system: the services remain closed.

37 : the services were closed; the new key entered has a valid serial number but too old: the services remain closed.

41 : the key version does not correspond to the system; the new key entered does not correspond to the system (invalid serial number): the services are open for a limited time.

42 : the key version does not correspond to the system; a valid key was entered: the services are open.

45 : the key version does not correspond to the system; the end of the limited time causes the services to close.

46 : the key version does not correspond to the system; a new key with a valid serial number but too old an edition has been entered: the services are open for a limited time.

52 : the services were closed; a valid key was entered: the services are open.

53 : the services were closed; the key entered does not correspond to the system: the services remain closed.

57 : the services were closed; the key entered has a valid version but does not correspond to the system (invalid serial number): the services remain closed.

61 : the system's edition is too old; the new key entered does not correspond to the system: the services are open for a limited time.

62 : the system's edition is too old; a valid key was entered: the services are open.

64 : the edition of the system's key is too old; a new key with a valid edition, but an old version, was entered: the services are open for a limited time.

67 : the system’s key is too old; the end of limited time causes the services to close.

72 : the system’s key is too old; the services were closed; the new key entered is valid: the services are open.

73 : the system's edition is too old; the services were closed; the new key entered has a problem with the serial number: the services remain closed.

75 : the system's key is too old; the services were closed; the new key entered has a valid serial number, but a version which does not correspond to the system: the services remain closed.

12.5.1.6 MANAGEMENT OF TWO-COLOUR LED ON ATTENDANT STATION

The two-colour LED on the attendant station flashes quickly (orange) in the following cases:

- either of the 2 following T2 alarms(message 53):
  - MS: Missing Signal
  - RFA: Remote Frame Alarm
- the call detail record storage buffer is 70% full (default value) (message 70)
- counting printer fault (message 72); this alarm is only transmitted if the "PrintFault" flag is other than 0
- problem regaining ISDN access (message 50)
- electrical power supply fault (message 123)
- the hardware message table is 80% full (message 160); this alarm is only transmitted if the "OperAlarm" flag is other than 0
- erroneous NMC call (message 171)

- unanswered NMC call (message 172)
- NMC communication failure (messages 173, 174 or 175)
- NMC: alarm report failure (message 176)
- NMC: PCX not registered (message 177)
- NAND Flash memory (CPU or XMEM) or hard disk not detected (message 239)

12.5.1.7 URGENT ALARMS

Alcatel-Lucent OmniPCX Office Communication Server will generate a call to the network management centre (NMC) if any of the following alarms is detected:

- the system reboots (message 0)
- the system is operational after start-up (message 11)
- either of the 2 following T2 alarms (message 53):
  - MS: Missing Signal
  - RFA: Remote Frame Alarm
- the ISDN protocol management module detected a level 1-fault on an ISDN access (message 56)
- the call detail record storage buffer is 70% full (default value) (message 70)
- counting printer fault (message 72); this alarm is only transmitted if the "PrintFault" flag is other than 0
- the board is back in service after a system stoppage or after being unplugged (message 100)
- the board is disconnected (message 101)
- the board is permanently reset (message 105)
- the board is refused (message 106)
- the board info has been erased by MMC (message 109)
- the module is back in service (message 120)
- the module is disconnected (message 122)
- there is a power supply problem (message 123)
- there is a problem with the fan (message 124)
- the hardware message table is 80% full (message 160); this alarm is only transmitted if the "OperAlarm" flag is other than 0
- NMC: history event table 80% full (message 161)
- NMC: call detail record table 80% full (message 162)
- NMC: call detail record table full (message 166)
- IBS synchronization lost on UA link 0 (message 202)
- IBS synchronization lost on UA link 1 (message 203)
- the Ethernet interface of the IP-LAN board xxxx is out of service (message 221)
- the Ethernet interface of the IP-LAN board xxxx is in service (message 222)

- the duration of the VMU messages is reaching maximal duration (message 241)
- an error occurred at the opening of the voice prompt file (message 242)
- an error occurred at the reading of the voice prompt file (message 244)
- an error occurred at the writing of the voice prompt file (message 245)
- the downloading of an Alcatel-Lucent 9 series terminal has failed (message 252)

12.6 Data Restorations

12.6.1 Maintenance

In maintaining and exchanging a CPU board (main CPU and/or CoCPU@), the data stored on the daughter board XMEM128 and/or on the Hard Disk will or will not be restored depending on the conditions described that follow.

12.6.1.1 PROCEDURE TO EXCHANGE A MAIN CPU BOARD

12.6.1.1.1 CPU-4 with XMEM128 (no Hard Disk)

The XMEM128 is not faulty and does not have to be exchanged

- Install the old XMEM128 on the new main CPU board.
- All data stored on the XMEM128 board will normally still be available after the CPU exchange. However, data saved on the XMEM128 board (messages, conversations, call detail records) will not be restored if for some reason it is not stored (see Note). After which it will be required to make a cold reset of the system, launch the "Data saving" process via OMC to restore the data configuration information (see paragraph A).

Note:
It is possible to find a new/replacement CPU delivered from the factory which will not always restore the data from the XMEM. However it would only occur if the exchange CPU is not charged with a software version.

Paragraph A: The XMEM128 is faulty and has to be exchanged

When the new XMEM128 board is installed, launch the "Data restore" process via OMC to restore the data configuration information.

Select **Comm ->Write to PBX**, select the box **Voice Prompts** (screen **"Write to PBX"**).

The data restored are:

- names and announcements of the voice mail unit.
- auto attendant announcements, greetings.

Voice mail messages, NMC call detail records and recorded conversations cannot be restored.

12.6.1.1.2 CPU-4 without XMEM128

Launch the "Data restore" process via OMC to restore configuration information. The voice files will be available based on the conditions of paragraph A (except for customizable voice announcements used from the Hard Disk or XMEM128).

12.6.1.1.3 CPU-4 with Hard Disk

The Hard Disk is not faulty and does not have to be exchanged

- Install the old Hard Disk on the new main CPU board.
- After a cold reset of the system, launch the "Data restore" process via OMC (see paragraph A). All information saved on the Hard Disk is normally available (including voice messages and recorded conversations).
- The Internet Access configuration (FAI, users, proxy, security, etc.) can be restored. Select the box "Internet Access Data" during the database restoration (screen **Write to PBX**).

The Hard Disk is faulty and has to be changed

- All messages, recorded conversations and NMC call detail records are lost.
- The cache memory is also lost.
- Voice files (voice prompts) are available if the condition explained in paragraph A is followed.

12.7 Start and Stop of a System

12.7.1 Maintenance

12.7.1.1 START MONITORING

It is possible to follow the progress of the start in 2 ways:

- On the display of the dedicated stations
- Using the Web browser
- On station

12.7.1.1.1 On station

The display on the dedicated set indicates the different steps for starting the system with the following elements: Start x.y (x is the step and y the sequence)

Detail:

- Start 2-6: detection of the cards of the main cabinet
- Start 2-5: search of extension 2 and loading of the DSP if the extension exists
- Start 2-4: detection of the expansion card 2 (optional)
- Start 2-3: search of extension 2 and loading of the DSP if the extension exists
- Start 2-2: detection of the expansion card 2 (optional)
- Start 2-1: end of detection of telephony (appearance of virtual cards XRA IVPS)
- UNBLOCKING of the telephony (stations are operational)
- Start 1-0: starting of the CoCPU
- Normal display

12.7.1.1.2 Web navigator (browser)

1. Disable the proxy used by your browser (navigator):
   - on Netscape: Edit/ Preferences/ Advanced/ Proxy
   - on Internet Explorer: Tools/ Internet options/ Connections/ LAN settings
2. In the address file enter: http://192.168.92.246 :81/ or http:// IP address of the CPU followed by " :81/ "
3. In the login window, enter:
   - user name: operator
   - password: help1954
4. Click Main monitoring on the left of the screen. On your right, you will have the sequence to start the CPU.

This operation is available as soon as the system is in phase 1-6 (as per the station display) and is stored for later access.

12.7.1.1.3 Web-Based Tool

Web-Based Tool is a monitoring tool that offers a means to observe the OmniPCX Office through Internet.

Web-Based Tool is located within OmniPCX Office and can be reached by simple remote Web browsers.

It does not require any installation or specific program on the Client side and is available on any OmniPCX Office model.

You can access Web-Based Tool at the following URLs: **https://IP_address/services/webapp/** or **https://host_name/services/webapp/** with the following Web browsers: Internet Explorer, Mozilla and Mozilla Firefox.

2 classes of clients may be connected to OmniPCX Office.

These clients get different services according to their roles.

- Users (login name: operator, password: help1954)
- Managers (login name: installer, password: pbxk1064)

SERVICES PROVIDED

Service	Details	Operator	Installer
MOH upload	Load audio files for the Music On Hold feature	X	
System Start	Display System Start log file		X
Data Saving	Display Data Saving log file		X
Swap Serial	Select application connected to CPU config socket		X
General Information	Show CPU hardware equipment and state, memory use and software version		X
Cabinet Topology	Show hardware equipment of cabinets		X

Service	Details	Operator	Installer
Boot Information	Show the order in which boot devices are tried		X
Disk Smart Fs&disks	Display hard disk smart information Display mount table and partition table		X
System files	Give read access to log files in /current /boot and /current /debug directories, to current and alternate configrc files. Give read access to all file system including /proc		X
Net Configuration	Display net devices, routing table and cached routing table		X
Dump System	Display in a typewriter format a summary of system state Download debug and log files Display proc file system in a typewriter format		X
Memory Info	Display the contents of /proc/meminfo		X
Traces&Debug	Give read access to WLAN and NMC log files, allow trace activation and collection on T1		X

ARCHITECTURE

Type of configuration

Web-Based Tool is a client-server architecture that uses the HTTPS communication protocol. The client is a browser and the server is embedded in OmniPCX Office.

There are 3 types of configuration according to the access path:

- LAN
- Remote Access Server (management)
- WAN

LAN access

The computer running the client browser is connected to the same LAN as OmniPCX Office.

Remote Access Server access (management)

The remote user is connected to the OmniPCX Office Remote Access Server (RAS) board through ISDN.

The RAS board routes the packets to WBT through the LAN.

WAN access

The remote user connects to the Internet and reaches OmniPCX Office on its WAN access (through VPN or not).

The HTTPS port must be open on the WAN. This is possible through the Internet Access Web-Based Management feature of OmniPCX Office.

DESCRIPTION

Function specifications

Web-Based Tool is only available in English.

Operator session

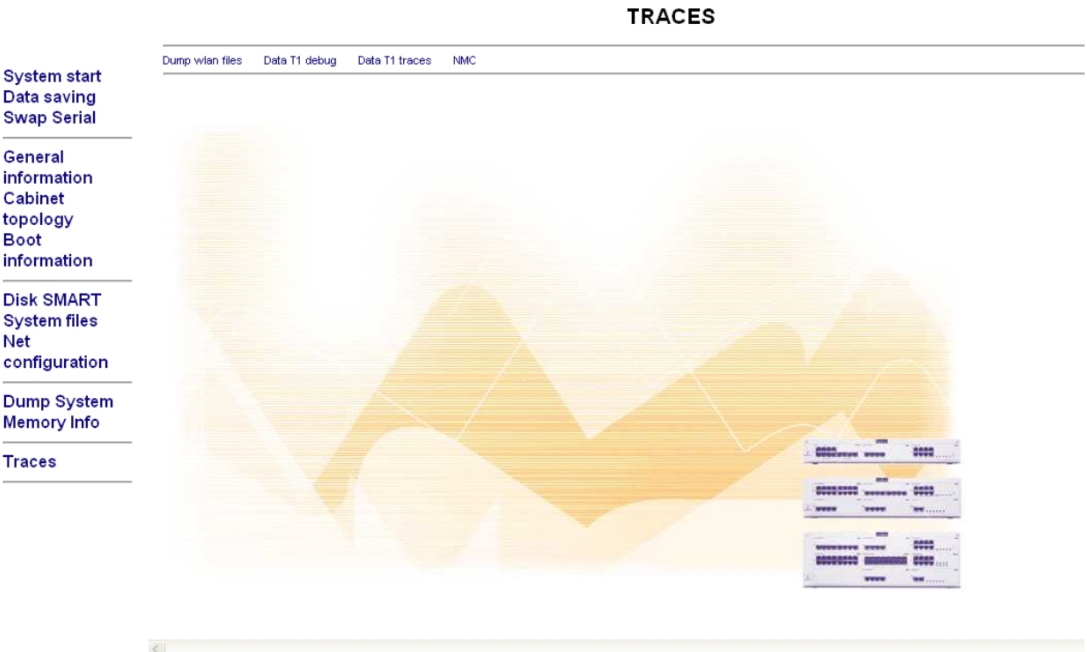
- Enter the audio file name in the **File** box or browse your system to find it.
- Click the **Submit** button.

Installer session

Click any of the items in the menu on the left to access the corresponding pages.

The pages that show up are self-explanatory.

Traces



The **Traces** page opens a submenu with the following items:

- **Dump wlan files**: To display the WLAN log files that store up to 4500 events that occurred on the Mobile IP Touch and WLAN access points.
- **Data T1 debug**
- **Data T1 traces**
- **NMC**: is the Alcatel-Lucent Network Management Centre which enables a telephone network manager to manage, administer and optimize one or several Alcatel-Lucent 4200 communication system from a remote site.
  The NMC submenu offers a means to activate/deactivate the monitoring of the OmniPCX Office embedded NMC server and to display the corresponding traces.

INTERACTIONS

Web-Based Tool is accessed through the Secure Application Server (SAS). SAS provides HTTPS access and centralized authentication.

MAINTENANCE PROCEDURES

Incident

The server may send error messages in HTTP packets; the Web browser displays these messages.

12.7.1.1.4 Console port

To follow progress of start-up on the console port, use the following characteristics:

- Login: swap_serial
- Password : alcatel

12.7.1.2 TIME EXAMPLES

Configuration	CPU	CoCPU	Application	Start	Stop
Rack 2	CPU-3	No	Telephony	5 min. 03 sec.	30 sec.
Rack 2	CPU-3 + HardDisk	2 x VOIP	Telephony + VoIP + Automatic Call Distribution	10 min. 15 sec.	38 sec.
Rack 2	CPUe-1 + HardDisk	2 x VOIP	Telephony + VoIP + Automatic Call Distribution + Internet Access	5 min. 41 sec.	44 sec.

Note:

The given times are equivalent to hot or cold reset.

For the swap/restore procedure, count 2(start+stoptime).*

The times given are only approximate times, without CoCPU BIOS upgrade.

12.7.1.3 EXAMPLE OF START MONITORED BY NAVIGATOR (BROWSER)

```
The main system is starting up. Please wait ...
----------------------------
--- CPU TYPE: MAIN ---
----------------------------
--- Start of BIOS ---
Succeeded
--- Start of Linux kernel ---
Operating system: Linux 2.2.13-RTL2.0
Succeeded
--- Ramdisk initialisation ---
Succeeded
--- Hardware detected ---
CPU: AuthenticAMD 486 DX/4-WB
CPU speed: 133 MHz
RAM size: 64 MB
Flash size: 30075kb
Xmem flash: present
Xmem flash size: 60879kb
Hard disk: present
Hard disk size: 5729 Mo
Hard disk manufacturer: FUJITSU MHK2060AT
--- Start of the software ---
++++++++++++++++++++++++
++ 8 ++ Start of Init of telephony ++ 8 ++
++++++++++++++++++++++++
Type of reset : WARM
Cti licence Status : open
++++++++++++++++++++++
++ 7 ++ Init controller Master ++ 7 ++
++++++++++++++++++++++
Dld DSP 0 : OK
Type of Backpanel : RACK 3
Dld DSP 1 : KO
Power supply Status : MAIN
++++++++++++++++++++++++++++++++
++ 6 ++ Detection of boards on controller Master ++ 6 ++
```

```
++++++++++++++++++++++++++++++++
Slot : 2 - Board : EBUA - hb in slot : 1
status : accepted
Slot : 3 - Board : EBZ_LH - hb in slot : 1
status : accepted
Slot : 7 - Board : BRA - hb in slot : 1
status : accepted
FAN1 Status : OK
FAN2 Status : OK
++++++++++++++++++++++
++ 5 ++ Init controller Sat 1 ++ 5 ++
++++++++++++++++++++++
++++++++++++++++++++++
++ 3 ++ Init controller Sat 2 ++ 3 ++
++++++++++++++++++++++
+++++++++++++++++++++++++
++ 1 ++ End of Init of telephony ++ 1 ++
+++++++++++++++++++++++++
- > Creation of virtual boards :
Slot : 91 - Board : XRA - hb in slot : 1
status : accepted
Slot : 92 - Board : IVPS - hb in slot : 1
status : accepted
Comment: no restore, call handling is available
++++++++++++++++++++++++
++ 0 ++ telephony is running ++ 0 +++
++++++++++++++++++++++++
Comment: no restore, call handling is available
Comment: no restore, call handling is available
Comment: no restore, call handling is available
Slot : 6 - Board : CPU - hb in slot : 1
status : accepted
Slot : 9 - Board : CPU - hb in slot : 1
status : accepted
Comment: no restore, call handling is available
+ SLOT: 1 - CPU TYPE : MAIN
```

ANV number : 3EH73026ACAA 04
db1 : absent
db2 : xmem
db3 : absent
db4 : absent
CPU speed: 133 MHz
RAM size: 64 MB
Flash size: 32 kB
Hard disk: present
Hard disk size: 5729 MB
Hard disk manufacturer: FUJITSU MHK2060AT a_
+ SLOT: 5 - CPU TYPE : VOIP
ANV number : 3EH73026ACAA 04
db1 : absent
db2 : absent
db3 : absent
db4 : absent
CPU speed: 133 MHz
RAM size: 64 MB
Flash size: 32 kB
Hard disk: absent

Detected sets :
=========
UA: 5
MUA: 0
IBS: 0
Analog (Z): 8
mobile set: 0
Password: 0
TA: 0
S0: 0
AOM: 0

12.8 Minimum Service after a Hard Disk Crash

12.8.1 Maintenance

e-Business solutions require a CPUe-1/CPUe-2 board equipped with a hard disk. In case of hard disk crash, the system works with reduced services, using NAND Flash memory.

In case of hard disk crash, the system works with the following characteristics:

- all telephone services are available.
- configuration data are saved by the NAND Flash.
- system configuration by OMC is possible.
- VoIP services are available.
- Internet Access services are not available.
- NMC tickets are not saved, but new tickets can be generated; only 1,000 taxation tickets can be stored.
- only the system's first language is available (for voice prompts and station displays).
- recordings of conversations, welcome messages and names are not kept.
- configuration data modified in the last 24 hours (maximum) are lost.
- only one software version is stored in NAND Flash; it is not possible to download a new version using OMC.
- OmniTouch Call Center Office services are not available.

When the system switches to minimum service, a hardware message (message 239) is emitted, indicating a hard disk problem.

Chapter 13 System Services

13.1 Glossary

13.1.1 Glossary

13.1.1.1 A

Automatic Call Distribution
A computerised phone system that responds to the caller with a voice menu and connects the call to the required agent. It can also control call flows by automatically routing calls in the order of arrival.

ACSE
Association Control Service Element. OSI convention used for establishing, maintaining and releasing connections between two applications.

ADN
Additional Designation Number.

AFU
Auxiliary Function Unit. Daughter board of the CPU/CPUe/CPU-1/CPU-2/CPUe-1/CPUe-2/CPU–3 board supporting ancillary functions such as general bell, doorphone, audio in, audio out, etc.

AMIX-1
Mixed analog equipment board: analog accesses with CLIP functionalities, analog and digital terminal connection interfaces.

AP
Access Point. A device that acts as a switch between the wireless LAN (802.11a, b, or g) and the wired LAN (802.3). There are two types of APs: Thin and Fat. The newer Thin technology AP consists of a thin AP and an access controller (also known as a wireless controller). Only the time-critical functions are managed by the thin AP. The other features are managed by the access controller.

APA
Analog Public Access. Board allowing the connection of analog network lines (switched network) with CLIP functionality. That board, equipped with GSCLI boards (Ground Start), is compatible with the American public network.

API
Application Programming Interface

ARI
Access Right Identifier. System identification number (DECT feature).

ARS
Automatic Route Selection. A logic direction is a set of trunks used for a call with the following facilities: seeking out the optimal path for a call, using the least-cost operator or network; overflow management: enables a PCX to find a new route to make an outgoing call when there are no resources available in the initial trunk.

ASN-1
Abstract Syntax Notation 1. OSI language for describing data types independently of processor structures and technical representations.

ATA
Analog Trunk Access. Board for connecting analog network lines (switched network).

13.1.1.2 B

BACKGROUND MUSIC
External device (e.g. radio tuner) that can broadcast music over the loudspeakers of idle terminals; broadcasting is stopped automatically if there is an incoming call to the terminal or if the user makes a call.

BACP
Bandwidth Allocation Control Protocol. Control protocol associated with BAP.
BAP
Bandwidth Allocation Protocol. PPP protocol that manages bandwidth by allocating it dynamically between two ports, i.e. between the two extremities of a point-to-point link.
BOD
Bandwidth On Demand. Service that allocates bandwidth automatically in response to traffic volume.
BRA
Basic Rate Access. Board for connecting T0 or DLT0 digital basic accesses; each access supports a data rate of 144 kbps, structured as 2 B-channels at 64 kbps for voice and data transmission, and 1 D-channel at 16 kbps for signalling.

13.1.1.3 C

CCP
Compression Control Protocol
CHAP
Challenge-Handshake Authentication Protocol. Security function supported on connections that use PPP encapsulation: prevents unauthorised access.
CIFS
Common Internet File System. This protocol is an extension to the SMB file sharing system. Its main benefit is to provide compatibility with locking operations and multiple SMB read/write operations.
CLIP
Calling Line Identification Presentation. Complementary service for digital protocols that allows the caller number to be presented to the called party.
CLIR/COLR
Calling/COnnected Line Identification Restriction. Service that inhibits CLIP or COLP.
CNIP
Calling Name Identification Presentation. Complementary service for private digital protocols (ISVPN or ABC-F) that allows the caller's name to be presented to the called party.
COLP
COnnected Line identification Presentation. Complementary service for digital protocols that allows the number of the connected user (the one who answers the call) to be presented to the caller.
CONP
COnnected Name identification Presentation. Complementary service for private digital protocols (ISVPN or ABC-F) that allows the name of the connected user (the one who answers the call) to be presented to the caller.
CPU
Central Processing Unit. Term designating the processor or microprocessor. The central processing unit executes computer program instructions.
CSTA
Computer Supported Telephony Application. ECMA standard that defines command exchanges between a PCX and a server.
CTI
Computer-Telephone Integration. Interaction mechanism between 2 sections, namely a data processing section (computer) and a telecommunications section (PCX), independently of the physical layout of the 2 sections.

13.1.1.4 D

DASS2
Digital Access Signalling Specification number 2
DDI
Direct Dialling In. Direct external call number for the system terminals (depending on the configuration with

the public network operator).

DECT
Digital Enhanced Cordless Telecommunication. European cordless telephony standard. DECT terminal: cordless terminal that complies with this standard.

DHCP
Dynamic Host Configuration Protocol. Protocol that manages IP address allocation dynamically so that addresses can be reassigned when no longer being used by LAN hosts.

Direct RTP
A feature which optimizes the RTP flow of VoIP in SIP, thus optimizing the number of VoIP CODEC resources.

DISA
Direct Inward Station Access. Services (Analog DISA and Transit DISA) enabling outside callers to dial a specific number giving direct access to the system.

DLL
Dynamic Link Library. Windows library linked dynamically to an application.

DLT0
Digital Line T0. Basic access configured with the QSIG protocol (= digital LIA).

DLT2
Digital Line T2. Private 2 MHz link in PRA mode (= digital ATL).

DNS
Domain Name Server. System used on the Internet for converting domain names or machine names into IP addresses. A domain name, unlike an IP address, is an easily memorized Internet address.

13.1.1.5 E

ECMA
European Computer Manufacturers Association

ETHERNET
Local network (LAN) operating at 10 or 100 Mbps (10 base T or 100 base T) over a coaxial cable. Ethernet is similar to the IEEE 802.3-series standards.

13.1.1.6 F

FoIP
Fax over IP. Refers to the message and data transmission from a G3 Fax using the Internet protocol (usually T38).

FTP
File Transfer Protocol. Standard protocol for exchanging files between remote computers over the Internet.

FTP/STP/UTP
Foiled Twisted Pairs/Shielded Twisted Pairs/Unshielded Twisted Pairs. Types of connection cables to be used between an Alcatel-Lucent OmniPCX Office Communication Server and an external distribution panel.

13.1.1.7 G

GATEKEEPER
Secure directory server

GATEWAY
Device connecting different networks

GENERAL BELL
If the operator is absent, internal and external calls to the operator are directed to an external signalling device that lets any authorized terminal take these calls.

13.1.1.8 H

H.323
ITU standard for multimedia communication (voice, video, data).

H.450
Additional services associated with H.323 version 2.
HSL
High Speed Link. Link between the basic module and an add-on module; requires an HSL daughter board to be fitted on the CPU and MEX boards.
HTTP
HyperText Transfer Protocol. Standard application protocol for exchanging files (text, images, audio, video, etc.) over the Internet.
HTTPS
Secure HyperText Transfer Protocol. Secure version of HTTP: encrypts and decrypts pages containing user requests as well as pages retrieved from a web server.

13.1.1.9 I

IAP
Internet Access Provider. See ISP.
IBS
Intelligent Base Station. There are 2 kinds of IBSs: one that can be installed indoors, one outdoors.
ICMP
Internet Control Message Protocol. Network protocol that provides error reports and information on the processing of IP packets.
IMAP4
Internet Message Access Protocol. A protocol of the same type as POP3, the difference being that the messages always stay on the ISP server, even after consultation. IMAP requires continuous access to the server while the messaging service is in use.
IN
Installation Number
IP
Internet Protocol. The main protocol supporting the Internet. IP governs the forwarding and transmission of data packets over supporting multivendor packet-switched networks.
IPSec
Internet Protocol Security. Standard taking network security into account. Protocol used in the implementation of VPNs, and for remote access by connection to a VPN.
ISDN
Integrated Services Digital Network. Standard for the transmission of digital data over telephone cables or other communication vectors.
ISDN-EFM
Integrated Services Digital Network- Emergency Forwarding Module. T0/S0 Forwarding Module.
ISP
Internet Service Provider. Internet Access Provider. A company that provides Internet access for individuals and companies, along with other services, such as web site construction and hosting.
ISVPN
Integrated Services Virtual Private Network. Protocol used in a private virtual digital network; it offers functions such as transfer optimization and the transmission of information such as the name, busy status or diversions.
ISVPN+
Includes metering information in addition to the usual ISVPN services.
ITU
International Telecommunications Union : global coordination body.

13.1.1.10 K

INTERCOM (mode)
Dedicated terminal operating mode in which the terminal features as many resource keys (RSP) as there

are network lines in the system.

13.1.1.11 L

LAN
Local Area Network. Network of interconnected switches, routers, and servers that share the resources of a processor or server in a relatively restricted geographical area, usually the premises of a company. In the context of the OmniPCX Office, the LAN includes an IP network and provides services to the wired client and to the WLAN client: file server, proxy, main server.

LOUDSPEAKER
External loudspeaker used for broadcasting messages.

13.1.1.12 M

MANAGER/SECRETARY
Set of specific services (profile, filtering, diversion) between a manager terminal and a secretary terminal.

MEX
Add-on module. Controller board for extension or "add-on" module.

MIPT
Mobile IP Touch. A wireless terminal that is connected to the system through a wired Access Point (AP). The radio connection between the wireless terminal and the AP is specified by the 802.11 family of specifications.

MIX
Mixed equipment board: T0 accesses, analog and digital terminal connection interfaces.

MLAA
Multiple Automated Attendant: Software component used for automatic incoming calls routing via voice guides.

MMC
Man Machine Configuration. Command lines that a user types to the interface of an application to change the parameters of system elements. It can also be in the form of graphic images that the user can select to make changes.

MPPP
Multi-link PPP. A protocol that aggregates bandwidth from a number of links to obtain faster communication speeds.

MULTILINE TERMINAL
Terminal that has several lines for managing several calls at the same time.

13.1.1.13 N

NAT
Network Address Translation. A service that converts the IP address used on one network into another IP address recognisable by another network. Address translation allows companies to keep their own private IP addresses for internal purposes, while using just one IP address for external communication.

NMC
Network Management Centre. Workstation allowing a communication server administrator to remotely manage, administer (storage of call metering tickets for example) and optimize one or more Alcatel-Lucent OmniPCX Office Communication Server systems.

NMT
Numbering Modification Table

NNTP
Network News Transfer Protocol. Protocol used by computers to handle messages created in Usenet forums.

13.1.1.14 O

ODC

On Demand Communication - Commercial name of On Demand mode.

On Demand mode

This mode introduces a “user” definition and the validity of the licence in OPEN state is limited and checked daily by the system.

PO

Operator Station. Dedicated terminal for answering incoming calls from the public network.

OMC

OmniPCX Office Management Console (formerly PM5). A PC-based management and configuration tool.

13.1.1.15 P

PAP

Password Authentication Procedure. Procedure used by PPP servers to validate connection requests.

PASSWORD

Code acting as a password, controlling access to the voice mail unit and the terminal locking function.

PAT

Port Address Translation

PATA

Parallel Advanced Technology Attachment - Hard disk interface bus.

PCBT

PC Based Telephony

PCX (mode)

Mode of operation ofdedicated terminals; in this mode, all the network lines are materialized by general-purpose resource keys (RSB).

PE

Public Exchange. Public central terminal (switch).

PLEASE WAIT MESSAGE

An audio component of the system (or an external device, such as a cassette player) which plays a message or piece of music while keeping an external correspondent on hold.

POP3

Post Office Protocol. Standard Internet protocol for receiving electronic messages. POP3 is a client/server protocol in which the messages are received and hosted by the ISP. When a message is read, it is transferred to the client terminal and is no longer hosted by the ISP.

PPP

Point-to-Point Protocol. Protocol used in communication between two computers using a serial interface (typically a PC connected to a server via a telephone line).

PRA

Primary Rate Access. Board for connecting a T2 digital primary access; the access supports 48 kbps structured as 30 B-channels at 64 kbps for voice and data transmission, and 1 D-channel at 64 kbps for signalling.

PROXY

A proxy server is used as an interface between a user and the external Internet network.

PSTN

Public Switched Telephone Network.

PTN(X)

Private Telecommunications Network (eXchange). A private network consisting of switches and terminals connected together by telephone links.

PWT

Personal Wireless Telecommunications. Corresponds to the DECT standard for the North American countries (especially the US).

13.1.1.16 Q

QOS

Quality Of Service. Network characteristics (transmission speed, etc.) can be measured, improved and, to some extent, guaranteed in advance.

QSIG

Q Signalling Protocol. Set of standard signalling protocols between the private PBXs of a telephone network (Q reference point) interconnected by digital ATLs.

13.1.1.17 R

RADIUS

Remote Authentication Dial-In User Service. A client/server protocol that enables remote access servers to communicate with a central server in order to authenticate remote users before allowing them access to the systems or services they have requested.

RAS

Remote Access Server. Remote access server to the system LAN.

RGO, RGI, RGM

General resource keys supporting local and/or external calls, whether outgoing (RGO), incoming (RGI), or mixed (RGM).

RNIS

"Réseau Numérique à Intégration de Services". French equivalent of ISDN.

ROSE

Remote Operations Service Element

RSB

Resource key dedicated to a trunk group (bundle); used for making external outgoing calls on a particular trunk group and receiving all network calls.

RSD

Resource key for a particular destination; supports local calls for this number if assigned to a speed dial number, incoming calls for the number if assigned to a DDI number, or outgoing calls on a trunk group if assigned to a trunk group.

RSL

Resource key dedicated to a set; supports calls to and from a particular set.

13.1.1.18 S

SATA

Serial Advanced Technology Attachment - Hard disk interface bus.

S0 BUS

Type of connection for S0 digital terminals (passive short bus, long/short point-to-point bus, extended bus); S0 buses and terminals are connected up via an S0 option embedded in an Alcatel Reflexes terminal.

SELV

Safety Extra Low Voltage. Classification of interfaces in accordance with standards EN60950 and IEC 950.

SIP

Session Initiation Protocol. A signalling protocol for Internet conferencing, telephony, events notification, and instant messaging. SIP initiates for example, call setup, routing and authentication within an IP domain.

SLAN

LAN Switch. Daughter board for mounting on a CoCPU/CoCPU-1/CoCPU-2 board to enable it to communicate with the CPU/CPUe/CPUe-1/CPUe-2.

SLI

Single Line Interface. Board allowing the connection of analog terminals (also known as Z terminals).

SMB

Server Message Block. File sharing protocol which enables a terminal to localize one or more files across the network, and then to open/read/edit/delete them.

SMTP

Simple Mail Transfer Protocol. Standard protocol used for sending and receiving mails.

SPI

Service Provider Interface

SSH

Secure Shell. A UNIX interface protocol for obtaining secure access to remote computers.

SSID

Service Set Identifier. In Wi-Fi wireless LAN computer networking, an SSID is a code attached to all packets on a wireless network to identify each packet as part of that network. The code consists of a maximum of 32 alphanumeric characters. All wireless devices attempting to communicate with each other must share the same SSID. Apart from identifying each packet, the SSID also serves to uniquely identify a group of wireless network devices used in a given "Service Set".

SSL

Secure Socket Layer. Encryption and authentication layer which ensures the authentication, integrity and privacy of the documents distributed by the World Wide Web.

13.1.1.19 T

TAPI

Telephony IP. Standard defined by Microsoft.

TCP/IP

Transmission Control Protocol/Internet Protocol. Standard protocol used on the Internet. TCP corresponds to the Transport layer (layer 4) of the OSI model. IP corresponds to the Network layer (layer 3) of the OSI model.

TERMINAL GROUP

Series of terminals grouped under the same directory number. Any call to that number is routed to a free terminal line.

TFTP

Trivial File Transfer Protocol. The simplest network application for transferring files.

TL

(Analog) Trunk Line connecting the system to the public switched network.

TSAPI

Telephony Services API. Standard defined by Novell, based on ECMA's CSTA standard.

13.1.1.20 U

UAI

Universal Alcatel Interface. Board used for connecting up digital terminals or DECT 4070 IO/EO base stations.

UPS

Uninterruptible Power Supply. Device increasing the system's back-up time.

URL

Uniform Resource Locator. Address of a resource (file, program, image, etc.) accessible on the Internet.

UUS

User to User Signalling. Information carried clear end-to-end by ISDN to enable exchanges between network subscribers; the ISVPN protocol is contained within this information.

13.1.1.21 V

VMU

Voice Mail Unit. The integrated voice server provides a voice mailbox for each user, as well as a general voice mailbox and features such as Personal Assistant, Automatic Attendant and Audiotex.

VoIP

Voice over IP. Term designating voice transmission over a data network using the Internet protocol.

VoWLAN

Voice over WLAN. Term designating voice transmission over a data network using the WLAN.

VPN

Virtual Private Network. Private data network that uses the public telecommunications infrastructure (e.g.

the Internet) while maintaining confidentiality by means of tunnelling protocols and security procedures.

13.1.1.22 W

WAN
Wide Area Network. A geographically dispersed telecommunications network. The term WAN is used in contrast to LAN.

WBM
Web-Based Management. Management tools for the system's Internet features.

WINS
Windows Internet Naming Service. In Windows environment, the service that manages the correspondence between client station names and LAN locations relative to their IP addresses.

WLAN
Wireless Local Area Network. A LAN that provides networking using radio frequencies rather than wires for communication.

WLAN association
An association refers to the connection between the WLAN client and the AP. There are two types of associations: passive scanning and active scanning. In passive scanning, APs send out information such as SSIDs and supported rates, while the client passively scans the radio channels for beacons and probe responses. The client then selects an AP. The client keeps scanning even after the association is made (to support roaming). In active scanning, clients send out probe requests. If the probe request contains an SSID, only the APs with the correct SSID will respond. If the probe request contains a broadcast, all the APs will respond.

WLAN client
Any PC, PDA, or phone set that supports the 802.11a and 802.11b/g protocols can be a WLAN client.

13.1.1.23 X

XMEM
eXpansion Memory. Daughter board of the CPU board that extends the memory capacity and allows a hard disk to be connected.

13.2 Software Keys

13.2.1 Services provided

13.2.1.1 DESCRIPTION

In the Alcatel-Lucent OmniPCX Office Communication Server system, a software key is represented by an alphanumeric string of characters, which opens functions. Two types of software keys correspond to each Alcatel-Lucent OmniPCX Office Communication Server system:

- the **MAIN software key** for the system functions (voice, Internet, etc.)
- the **CTI Software key** for the CTI functions
- the **Try and Buy keys** for the CTI functions

The software key corresponds to a text file where the name is the CPU hardware number with the **.MSL** (MAIN key) or **.CSL** (CTI key) extension.

Example: file 000068DA.msl and 000068DA.csl for main CPU no. 000068DA.

Each system needs the Main and CTI Software keys even if no CTI application is used on the system.

The systems can be delivered with a key that is already personalized for the client. The Distributor needs to load, if necessary, the personalised key on the non-factory-configured systems.

Service limits in the software key are subject to the hardware limitations of the client's configuration.

Try and Buy only apply to the CTI aspects.When first initialised, ,the PIMphony Pro and PIMphony Team applications are available to every user.

The integrated TAPI 2.0 is also available.

As soon as one Try and Buy licence is used, the countdown starts. The licence will last 60 days.

After the 60 days, only the services defined in the CTI Software key are available.

13.2.1.2 CONFIGURATION

Keys must be downloaded in the event of CPU replacement or modifications to improve the system features.

However, the installation can be adapted to meet new needs when the system is in place by entering a new software key:

- by OMC (Expert View): **Modification Typical -> System -> Software key**
- by MMC-Station: **Global -> SwKeys** -> **Main/CTI**

Note 1:

When using MMC-Station with Alcatel-Lucent 8 series terminals, licences can only be displayed, not up-dated.

Two software keys must be entered: one for the system functionality (Main key, 42 to 138 characters), the other for CTI functionality (CTI key, 17 to 161 characters).

Keys consist of:

- all upper-case letters except I and O
- all digits except 1 and 0
- the special characters #, $, /, %, &, *, +, @,(and)

Note 2:

The software key must not contain a carriage return or space bar at the end of the key.

In some cases it is necessary to do a warm reset to activate the new key. A message is displayed for doing this reset.

Note 3:

In OMC, the values contained in the key are displayed in the first column "Authorised by software key" and the functions that are really open are displayed in the second column "Really activated". Since the equipment has no influence on the CTI functions, a single display column is available.

Remark:

In the event of a software key change or a reduction in the number of Web Communication Assistant users, it is recommended to withdraw Web Communication Assistant rights from the relevant users before loading the new software key. Otherwise the system randomly selects users and withdraws their rights. For a more detailed description of the allocation and withdrawal of Web Communication Assistant

rights via the WBM, refer to "Users and user groups" in the Internet Applications section.

13.2.1.3 SOFTWARE KEY CONTROL ON THE SYSTEM

On starting up the system, different cases are possible:

- **The services needed by the customer are open and work properly:** the software key present on the system is correct.
- **The services needed are not open**
- **The key is valid but some services are not open** (verify using OMC).
  - Verify that the order meets the client's needs. If not, contact the "orders" department. A new software key needs to be created including the new features.
  - When loading the key via OMC a warning message is displayed. In this case the services may be limited due to insufficient memory (Hard disk or XMEM) or CPU power.
- **The software key present on the system is not correct:**
  - The software key syntax is correct but it does not match the CPU's serial number. The system functions correctly with all its services for 30 days. A message "Software Key problem" is displayed on the Attendant station. Press the Alarm key to show the expiry date. When loading a correct key (valid CPU serial number) during this period, the system state is normal. If no correct key is loaded after 30 days, the system will restart in limited state with only sets belonging to the Operator group working, all other sets being out of service; the "Software Key problem" is displayed on the operator station.
  - The software key syntax is incorrect. The system starts in limited mode. When loading the correct Software key (with the correct serial number), the system restarts with all services working.
  - **New control starting with R2.0:**
    - The software key syntax is correct, but the software key does not match the system's software release. The system functions correctly with all its services for 30 days.
    - The software key syntax is correct, the software release is correct but a more recent key has already been entered on this system and it is not possible to revert to a previous key. The system functions correctly with all its services for 30 days.

Remark:

For a system in limited mode, when a valid software key is loaded, the system restarts with all its services.

13.2.1.4 CONTROL OF THE SOFTWARE VERSION

Starting with version R2.0, each key works with a specific system software version.

This mechanism concerns only the "major" versions: R2, R3, R4, R5, etc.

If the key version does not correspond to the system software version, the system starts with the requested functions but for a limited period (30 days). At the end of this period, it reinitialises in limited mode.

When entering a key by OMC, if the software version is not correct, OMC signals it and requests confirmation.

13.2.1.5 EDITION NUMBER AND ACKNOWLEDGEMENT CODE

The edition number is incremented with each implementation of a new key on a specific installation.

The acknowledgement code is indicated in message 34 (bytes 2 and 3) of the history messages table.

When a key is provided by Alcatel-Lucent and is implemented in the system, this procedure is irreversible.

It is possible to reload a previous key but the system will only open the requested functions for a limited period (30 days). At the end of this period, the system reinitialises in limited mode.

13.2.1.6 PROCEDURE IN CASE OF PROBLEM

To obtain a key corresponding to the main CPU, you must contact Alcatel-Lucent. Specify if the system was delivered with a software key corresponding to the CPU but does not work. If the client's main CPU has been changed, indicate the old and new CPU numbers.

13.2.2 Detailed description

13.2.2.1 Services Controlled by Main Software Key

The following table lists the services controlled by the Main software key of Alcatel-Lucent OmniPCX Office Communication Server. If a software key is not present in the system, or is incorrect, the system starts in a limited state. The table also gives the limited state service levels, the granularity of upgrades, the maximum service level for each service, and if a hardware extension exists.

Services	Valid for Software Version	Service level in limited state	Upgrade Granularity	Max Service Level	Hardware extension
STANDARD TELEPHONY					
Number of digital sets	All	According to selected model	+1	236	No
Number of analog sets	All		+1	236	No
MOBILITY					
Number of DECT sets	All	0	+1	200	No
Number Mobile IP sets	From R5	0	+1	120	No
CALL MANAGEMENT					
ARS	All	R1: open Since R2: closed	open		No
DISA/Transit DISA	All		open		No
ISVPN on ISDN (ARS required)	All	closed	open		No
QSIG + (ARS required)	All	closed	open		No
Number of Meet Me Conferences	From R5.1	0	+1	1	
NETWORKS					
Number of B-channels	All	0	+1	120	No
Number of B-channels on MIX boards	From R4	0	+2	120	No

Services	Valid for Software Version	Service level in limited state	Upgrade Granularity	Max Service Level	Hardware extension
INTERNET ACCESS					
Internet and Intranet Access	All	closed	open		No
Proxy: Web caching and Access control (Internet Services required)	All	closed	open		No
E-mail server (Internet Services required)	All	closed	open		No
Internet VPN	All	closed	open		No
DSL	From R1	closed	open		No
LAN to LAN	From R1	closed	open		No
Save/Restore	From R2	closed	open		No
Downloading URL filters	From R2	closed	open		No
Uploading statistical data	From R2	closed	open		No
Files and Web server (Intranet)	From R2	closed	open		No
WEB APPLICATION					
Web Communication Assistant (WCA) number of users	From R2	0	+1	25	No
RAS					
Number of accesses (B-channels)	From R2	0	+2	16	Yes if greater than 2
LAN TELEPHONY					
Number of IP Phones (IP Touch)	All	0	+1	200	No
Number of PIMphony IP	All	0	+1	200	No
VoIP GATEWAY					
Number of VoIP channels	All	0	+1	96	Yes
Number of B channels with VoIP on main CPU	All	0	+1	88	Yes
VoIP on CoCPU	All				Yes
VOICE MAIL UNIT AND AUTOMATED ATTENDANT					
Number of VMU ports	All	0	+1	8	No
Storage capacity (minutes)	All	20 From R5: 60	+10	200 hours	Yes
Automated Attendant	All	closed	open		No
Audiotext	All	closed	open		No
Fax switching	All	closed	open		No
Mailbox welcome messages	All	closed	open		Yes
Name in mailing lists	All	closed	open		Yes
Recording of conversations	All	closed	open		Yes
Remote customizing	From R2	closed	open		No

Services	Valid for Software Version	Service level in limited state	Upgrade Granularity	Max Service Level	Hardware extension
GREETING					
Number of messages (of length 16 seconds)	All	4	+4	8	Yes
MUSIC-ON-HOLD					
Duration of Music on Hold (minutes)	All	2	+2	10	Yes
METERING					
Number of NMC tickets	All	0	+1000	30000	Yes
Metering over IP	From R5	closed	open		No
MULTIPLE AUTOMATED ATTENDANT					
Number of tree structures	From R6		+1	5	
LANGUAGES					
Number of languages	All	2	+1	4	Yes
On Demand Licence					
On Demand	From R6	R6 : Indication that On Demand option is active.			
Licence validity date	From R6	This date is only used when On Demand mode is activated. It controls the validity of the licence.			
Number of users	from R6	> R6 : Not controlled by the system : Only used for information in OMC.			
SWL RELEASE (for e-licensing purchasing process)					
Required system version	From R2	R1: 0	+1	R2: 1 R3: 2 R4: 3 R5: 4 R6: 5	Yes
ACKNOWLEDGEMENT CODE (for e-licensing purchasing process)					
Random code provided by ecom.	From R2	1		FFFF	No
EDITION (for e-licensing purchasing process)					
Edition number of licence	From R2	0	+1	FFFF	No
Automatic Call Distribution					
Number of Automatic Call Distribution groups	From R3	8	0	8	Yes
Number of active Automatic Call Distribution agents	From R3	5, 10, 20, or 32 depending on licence		32	
Automatic Call Distribution Statistics Manager	From R3	closed	open		
Number of Agent Assistants	From R3	0,10,20,32		32	Yes

Services	Valid for Software Version	Service level in limited state	Upgrade Granularity	Max Service Level	Hardware extension
Number of Supervisor Consoles	From R3	0	+1	4	

13.2.2.2 Services Controlled by the CTI Software Key

The following table lists the functions controlled by the "CTI" software key.

Controlled services	Valid for Software Version	Service level in limited state	Upgrade Granularity	Max Service Level (ASPEN/PIII)
APPLICATION				
PIMphony Pro	All	0	+1	250
PIMphony Team	All	0	+1	250
Nomadic mode	From R3	0	+1	25 50 (R5)
PIMphony release 5.0 and 6.0	From R4	0	+1	50 (R4) 60 (R5)
PIMphony Attendant	From R5	0	+1	250
INTEGRATED TAPI 2.0 [6]				
Number of sessions	All	25 (R1) 0 (from R2)	+1	75/200 *
Number of monitors	All	250 (R1) 0 (from R2)	+1	250/500 **
Features	All	None		All
Alcatel-Lucent OmniPCX Office Communication Server CALL CENTER				
Number of sessions	All	0	+1	28/200 *
Number of monitors	All	0	+1	250/500 **
Features	All	None		All
CSTA DESKTOP CLIENT				
Number of sessions	All	0	+1	28/200 *
Number of monitors	All	0	+1	250/500 **
Features	All	None		All
CENTRAL SERVICES				
Number of sessions	All	0	+1	28/200 *
Number of monitors	All	0	+1	250/500 **
Features	All	None		All
CSTA (ALL FEATURES)				
Number of sessions	All	0	+1	28/200 *
Number of monitors	All	0	+1	250/500 **

Features	All	None		All
TAPI 2.1 SERVER				
Number of sessions	All	0	+1	28/200 *
Number of monitors	All	0	+1	250/500 **
Features	All	None		All
BUSY LAMP FIELD				
Number of sessions	All	0	+1	28/200 *
Number of monitors	All	0	+1	250/500 **
Features	All	None		All
XML SERVER				
Number of sessions	All	0	+1	1 *
Number of monitors	All	0	+1	250/500 **
Features	All	None		All
PIMphony **UNIFIED**				
Number of sessions	From R3,1	0	+1	1 *
Number of monitors	From R3,1	5	+10	75 **
Features	From R3,1	None		All
SOFTWARE LICENCE VERSION (for e-licensing purchasing process)				
Required system version	From R2	0 (R1/R1.1)	+1	1 (R2) 2 (R3) 3 (R4) 4 (R5)
ACKNOWLEDGE CODE (for e-licensing purchasing process)				
Random code given by ecom.	From R2	0		FFFF (Hex)
EDITION (for e-licensing purchasing process)				
Edition of licence	From R2	0	1	FFFF (Hex)

* The maximum number of simultaneous sessions is 80 on ASPEN and 200 on PIII.

** The maximum number of simultaneous monitors is 250 on ASPEN and 500 on PIII.

[6] In R1.x, this service is always present in the CTI key. Per session, only two monitors are allowed.