



Alcatel-Lucent OXO Connect

Expert Documentation: Mobility
Release 3.0 - July 2018

8AL91204USAF Ed. 01

Legal notice

The Alcatel-Lucent name and logo are trademarks of Nokia used under license by ALE. To view other trademarks used by affiliated companies of ALE Holding, visit: www.al-enterprise.com/en/legal/trademarks-copyright. All other trademarks are the property of their respective owners.

The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein.

© 2018 ALE International. All rights reserved. <http://www.al-enterprise.com>

Disclaimer

While efforts were made to verify the completeness and accuracy of the information contained in this documentation, this document is provided "as is". To get more accurate content concerning Cross Compatibilities, Product Limits, Software Policy and Feature Lists, please refer to the accurate documents published on the Business Partner Web Site.

In the interest of continued product development, ALE International reserves the right to make improvements to this documentation and the products it describes at any time, without notice or obligation.

The CE mark indicates that this product conforms to the following Council Directives:

- 2014/53/EU for radio equipment
- 2014/35/EU and 2014/30/EU for non radio equipment (including wired Telecom Terminal Equipment)
- 2014/34/EU for ATEX equipment
- 2011/65/EU (RoHS)



Chapter 1

Expert Documentation structure

Chapter 2

IBS DECT

2.1	DECT overview.....	15
2.2	DECT components.....	16
2.2.1	IBS base stations.....	16
2.2.2	DECT GAP handsets.....	16
2.3	DECT features.....	17
2.3.1	Mobility management	17
2.3.2	System access and dynamic channel selection	17
2.3.3	Inter- and intra-cell handover procedures.....	17
2.4	List of countries by region for DECT	17
2.5	DECT engineering rules.....	23
2.6	IBS base station deployment.....	23
2.6.1	Base station deployment procedure.....	24
2.6.2	Installation.....	24
2.6.3	Connection.....	29
2.6.4	Configuration.....	30
2.7	DECT configuration.....	32
2.7.1	Configuring the ARI number.....	32
2.7.2	Configuring GAP authentication	32
2.7.3	Registering a GAP handset.....	33
2.8	DECT traffic counters.....	33

3.1	Detailed description.....	35
3.1.1	Overview.....	35
3.1.2	Description.....	35
3.1.3	Quality of Service (QoS).....	38
3.1.4	Using VLAN Ids and Priority (IEEE 802.1q and IEEE 802.1p).....	38
3.1.5	Handset management.....	38
3.1.6	Dial by name.....	38
3.1.7	Emergency calls.....	39
3.1.8	Security.....	39
3.1.9	Limits and restrictions.....	39
3.2	Topologies.....	40
3.2.1	IP network deployment rules.....	40
3.2.2	DAPs synchronization, roaming and handover.....	40
3.2.3	IP-DECT only topology.....	43
3.2.4	Dual DECT topology.....	48
3.3	Configuration procedure.....	52
3.3.1	Overview.....	52
3.3.2	Deploying the IP-DECT solution.....	52
3.3.3	Managing IP-DECT handsets.....	54
3.3.4	Managing DAPs.....	56
3.4	Maintenance.....	57
3.4.1	Cold reset.....	57
3.4.2	Save/restore.....	57
3.4.3	Software upgrade.....	58
3.4.4	Incidents.....	58

4.1	xBS overview	59
4.2	xBS components	59
4.3	xBS synchronization and mobility	60
4.3.1	Site	60
4.3.2	Sync Cluster	61
4.3.3	Data synchronization	61
4.3.4	Clock synchronization	61
4.3.5	xBS mobility	64
4.4	xBS signaling and voice flows	65
4.5	xBS and IBS DECT	68
4.6	xBS topologies	69
4.6.1	xBS topology with one site and one Sync Cluster	69
4.6.2	xBS topology with one site and multiple Sync Clusters	70
4.6.3	xBS topology with multiple sites	71
4.7	List of countries by region for DECT	71
4.8	DECT traffic counters	77
4.9	DECT engineering rules	78
4.10	xBS solution deployment	78
4.10.1	Installing the xBS hardware	78
4.10.2	Configuring the xBS solution	86
4.10.3	Deploying xBS	87
4.10.4	Configuring Sync Clusters and clock synchronization in a site	90
4.10.5	Deploying DECT handsets	91
4.10.6	xBS initialization with LED states	91

Chapter 5

8212/8232/8242/8262 DECT Handset Registration

5.1	Registering the Handset.....	93
5.1.1	Prerequisite.....	93
5.1.2	Service Level offered on IBS and IP-DECT systems.....	93
5.1.3	Registering Procedure.....	94
5.1.4	Declaring the Handset on the OXO Connect.....	94
5.1.5	Registering the handset.....	94
5.1.6	Internal/external ringing tune.....	95
5.2	FAQ and troubleshooting tips.....	95
5.2.1	Can I use the 50 mW low power mode: probably NOT.....	95
5.2.2	Economy mode versus 50 mW low power mode.....	96

Chapter 6

Geolocation and Notification Management on DECT

6.1	Overview.....	98
6.2	Architecture.....	98
6.2.1	Alarm server architecture.....	98
6.2.2	Message Mode Supported.....	99
6.2.3	Supported Trunks.....	99
6.3	OXO Connect Configuration.....	99
6.3.1	Configuring the T2 Trunk.....	99
6.3.2	Configuring the SIP Trunk.....	102
6.3.3	Configuring Handsets.....	105
6.4	Other Configuration Documents.....	106

Chapter 7 Advanced Cellular Extension

7.1	Overview.....	107
7.1.1	Overview.....	107
7.1.2	Implementation.....	107
7.2	Configuration procedure.....	108
7.2.1	Configuration Example Values.....	108
7.2.2	Pre-Requisites.....	108
7.2.3	PCX Configuration.....	109
7.2.4	Client Installation and Configuration.....	111
7.2.5	Nomadic Activation.....	111

Chapter 8 Alcatel-Lucent Enterprise OpenTouch Conversation for iPhone

8.1	Introduction.....	112
8.1.1	Apple hardware.....	112
8.2	Architecture.....	112
8.2.1	Overview.....	112
8.2.2	Access Provided from the WAN/Internet.....	113
8.2.3	SIP Mode.....	114
8.3	Detailed description.....	116
8.3.1	Features Provided.....	116
8.3.2	Business Communications.....	117
8.3.3	Call Routing Profiles.....	118
8.3.4	Directory Services.....	119
8.3.5	Business Call Logs.....	120
8.3.6	Business Voice Mail.....	120
8.3.7	Collaboration Services.....	121
8.3.8	Ring tones.....	121

8.4	Configuration procedure.....	121
8.4.1	Checking the license.....	121
8.4.2	Checking the VoIP protocol.....	121
8.4.3	Declaring the OTCV iPhone.....	121
8.4.4	Configuring the dual-mode (Wi-Fi/Cellular).....	122
8.4.5	Associating a desk phone to the OTCV iPhone.....	123
8.4.6	Microphone access.....	123
8.5	Operation.....	123
8.5.1	Loading the Application from the iPhone AppStore.....	123
8.5.2	Configuring Server Settings to Access the OXO Connect.....	124
8.5.3	Configuration File Deployment.....	124
8.5.4	Initialization Process.....	124

Chapter 9

OpenTouch Conversation for Android

9.1	Overview.....	125
9.1.1	Introduction.....	125
9.2	Architecture.....	125
9.2.1	Overview.....	125
9.2.2	Access Provided from the WAN/Internet.....	126
9.2.3	SIP Mode.....	127
9.3	Detailed description.....	129
9.3.1	Main Features.....	129
9.3.2	Business Communications.....	130
9.3.3	Dual mode Wi-Fi/cellular.....	130
9.3.4	Call routing Profiles.....	131
9.3.5	Directory Services.....	133
9.3.6	Business Call Logs.....	134
9.3.7	Business Voice Mail.....	134
9.3.8	Collaboration Services.....	134
9.3.9	Limitations.....	135
9.4	Configuration procedure.....	135

9.4.1	Checking the license.....	135
9.4.2	Checking the VoIP protocol.....	135
9.4.3	Declaring the OTCV Android.....	136
9.4.4	Configuring the dual-mode (Wi-Fi/Cellular).....	136
9.4.5	Associating a desk phone to the OTCV Android.....	137
9.4.6	Installation.....	137
9.4.7	Application installation in the mobile device.....	137
9.5	Operation.....	139
9.5.1	WiFi or 3G/3G+ coverage.....	139
9.5.2	EDGE or GPRS coverage.....	140

Chapter 10

OpenTouch Conversation for Windows Phone

10.1	Overview.....	141
10.2	Architecture.....	141
10.2.1	Overview.....	141
10.2.2	Access Provided from the WAN/Internet.....	142
10.2.3	Public and Private Domains.....	143
10.2.4	Engineering rules.....	143
10.3	Detailed description.....	144
10.3.1	Main Features.....	144
10.3.2	Business Communications.....	145
10.3.3	Call routing Profiles.....	145
10.3.4	Directory Services.....	146
10.3.5	Business Call Logs.....	146
10.3.6	Business Voice Mail.....	147
10.4	Configuration procedure.....	147
10.4.1	Checking the license.....	147
10.4.2	Checking the VoIP protocol.....	147
10.4.3	Declaring the OTCV Windows.....	148
10.4.4	Associating a desk phone to the OTCV Windows.....	148
10.5	Operation.....	148

10.5.1	Overview.....	148
10.5.2	Prerequisites.....	148
10.5.3	Installing directly the application from the mobile device.....	149
10.5.4	Launching the OTCV Windows.....	149
10.5.5	Modifying the connection parameters to the OXO Connect.....	149
10.5.6	Accessing logs.....	150

Chapter 11

WLAN Infrastructure for OpenTouch Conversation applications

11.1	Introduction.....	151
11.2	Network architectures.....	151
11.2.1	Standalone Access Point.....	151
11.2.2	OAW controller based architecture.....	154
11.2.3	VPN topologies.....	155
11.3	VoWLAN design recommendations.....	157
11.3.1	MAC layer retransmissions.....	157
11.3.2	Coverage and capacity tradeoff.....	158
11.3.3	Roaming.....	158
11.3.4	QoS.....	159
11.3.5	VoIP VLAN.....	161
11.4	General recommendations.....	162
11.4.1	Network engineering.....	162
11.4.2	VoWLAN engineering.....	163
11.5	Troubleshooting tools.....	163
11.5.1	OpenTouch Conversation® for iPhone syslog client.....	164
11.5.2	OpenTouch Conversation RTP statistics pushed on OXO Connect.....	164
11.5.3	OXO Connect WebDiag VoIP channels statistics.....	165
11.5.4	OpenTouch Conversation QoS tickets.....	165
11.5.5	OXO Connect webdiag's tcpdump.....	166
11.5.6	WLAN analysis tools.....	166
11.5.7	OXO Connect historic event.....	167
11.5.8	Logs on OpenTouch Conversation.....	167

Chapter 12 Mobility Deployment

12.1	Presentation.....	168
12.2	Available configurations.....	168
12.2.1	Single set configuration.....	168
12.2.2	Multi-set configuration.....	170

The OXO Connect Expert Documentation is split into fifteen separated documents. Each document only describes the features supported by OXO Connect RC2.0* or higher (for example: MMC station is not described since it is not supported). Please refer to the OXO Connect Documentation Note, for historical information. In addition, the Cross Compatibility document is the reference for detailed status about supported and unsupported devices and applications.

* RCz.n, with z greater than or equal to 2, stands for any release starting from 2016 introducing Connect capabilities.

It appears on:

- Product stickers with release format: RC0zn/xx.yy
- In any documentation (including this one) as: Rz.n

These documents are:

table 1.1: Expert Documentation structure

	Documentation title	Part number
[1]	OXO Connect Expert Documentation: General Presentation Summary: this document contains general information on OXO Connect, such as a brief description of services provided, platform hardware, handsets and user applications available, limits, compatibility with standards, environmental constraints.	8AL91200xxxx
[2]	OXO Connect Expert Documentation: Hardware: Platform, interfaces and devices Summary: this document covers all hardware aspects related to OXO Connect: this includes description of platforms (racks), boards, sets and complementary equipment such as additional modules or interface modules. This document also contains commissioning procedures for sets.	8AL91201xxxx
[3]	OXO Connect Expert Documentation: User services Summary: this document gives the presentation and configuration procedure of features available for end-users. The final chapter of the document synthesizes features availability according to the type of device or application.	8AL91202xxxx
[4]	OXO Connect Expert Documentation: Voice mail Summary: this document details the integrated voice mail system and automated attendant (general description, management, services available for end-users), as well as the configuration procedure to connect an external voice mail unit.	8AL91203xxxx

	Documentation title	Part number
[5]	OXO Connect Expert Documentation: Mobility Summary: this document contains a detailed description of mobility services available on OXO Connect. This includes useful information to deploy an IBS DECT, PWT, IP-DECT or xBS infrastructure, the description of associated base stations and handsets, and necessary information to implement OpenTouch Conversation clients. <i>Note:</i> <i>This document does not cover VoWLAN.</i>	8AL91204xxxx
[6]	OXO Connect Expert Documentation: VoIP services Summary: this document describes VoIP protocols supported by OXO Connect (such as SIP), configuration procedure of private or public access through IP links, as well as dimensioning and maintenance basic information.	8AL91205xxxx
[7]	OXO Connect Expert Documentation: Private networks Summary: this documentation gives a description of architectures and protocols (such as SVPN, QSIG) supported for a private network, a description of ARS, metering, clock synchronization, and the configuration procedure of accesses.	8AL91206xxxx
[8]	OXO Connect Expert Documentation: General applications This document gives a description of various applications available on OXO Connect, such as Hotel, Call metering, CTI, doorphones, Network management center, point-to-point/point to multipoint T0, permanent logical link, multiple automated attendant, multiple entities, My IC Plugin for Outlook®, My IC Web, PIMphony Touch.	8AL91207xxxx
[9]	OXO Connect Expert Documentation: Web-based tool Summary: this document describes the web-based tool, which is the integrated monitoring tool of OXO Connect.	8AL91208xxxx
[10]	OXO Connect Expert Documentation: OmniTouch Call Center Office Summary: this document provides the description and installation procedure of OmniTouch Call Center Office. The document also includes presentation and operation of Announcement, Traceability, and a short description of Agent, Statistics and Supervisor applications.	8AL91209xxxx
[11]	OXO Connect Expert Documentation: Management tools Summary: this document describes the management tool available for OXO Connect(OMC). The document describes the OMC installation procedure, the different types of access between OMC and OXO Connect (local, remote, with or without proxy), the software installation procedure of OXO Connect via OMC and the list of services that can be managed by OMC.	8AL91210xxxx

	Documentation title	Part number
[12]	OXO Connect Expert Documentation: Maintenance services Summary: this document contains basic information concerning the maintenance of your OXO Connect. This includes a diagnosis methodology in case of system of terminal(s) failure, the list of system messages, procedure to save/restore data, procedure to stop/restart your system, to replace CPU, boards and sets.	8AL91211xxxx
[13]	OXO Connect Expert Documentation: Security Summary: this document gives essential information to secure your OXO Connect. This includes deployment guide for certificate, management of passwords, management of accesses to services from LAN/WAN and network configuration for remote accesses.	8AL91212xxxx
[14]	OXO Connect Expert Documentation: System services Summary: this document gives information about software keys, including their complete list. The document also describes operation of OXO Connect with NTP (as client or server) and the configuration of the embedded DHCP server.	8AL91213xxxx
[15]	OXO Connect Glossary Summary: this document contains a glossary of general telecommunications terms as well as specific terms related to OXO Connect.	8AL91214xxxx

In the present document, cross-references are identified by the number in the first column of the above table.

Part numbers are given in the last column, where xx corresponds to the language code of the document.

Outlook is either a registered trademark, or a trademark of Microsoft Corporation in the United States and/or other countries.

2.1 DECT overview

The OXO Connect offers a wireless telephone service based on the DECT (Digital Enhanced Cordless Telecommunications) protocol.

On the OXO Connect, the DECT service is based on use of the following components:

- IBS base stations connected to the PBX via one or two UA links. The two UA links allow six simultaneous communications.

IBS base stations are available in several versions such as IBS NG and 8379 DECT IBS (see: [IBS base stations](#) on page 16)

- DECT handsets connected to the IBS base stations via radio links complying with the DECT protocol.

The DECT service supports DECT handsets running in GAP and A-GAP modes (see: [DECT GAP handsets](#) on page 16)

Several IBS base stations can be connected to the same PBX. Each IBS base station covers a geographical area referred to as a **cell**, and the entire group of cells is referred to as the **DECT coverage area**. OXO Connect only handles one DECT coverage area.

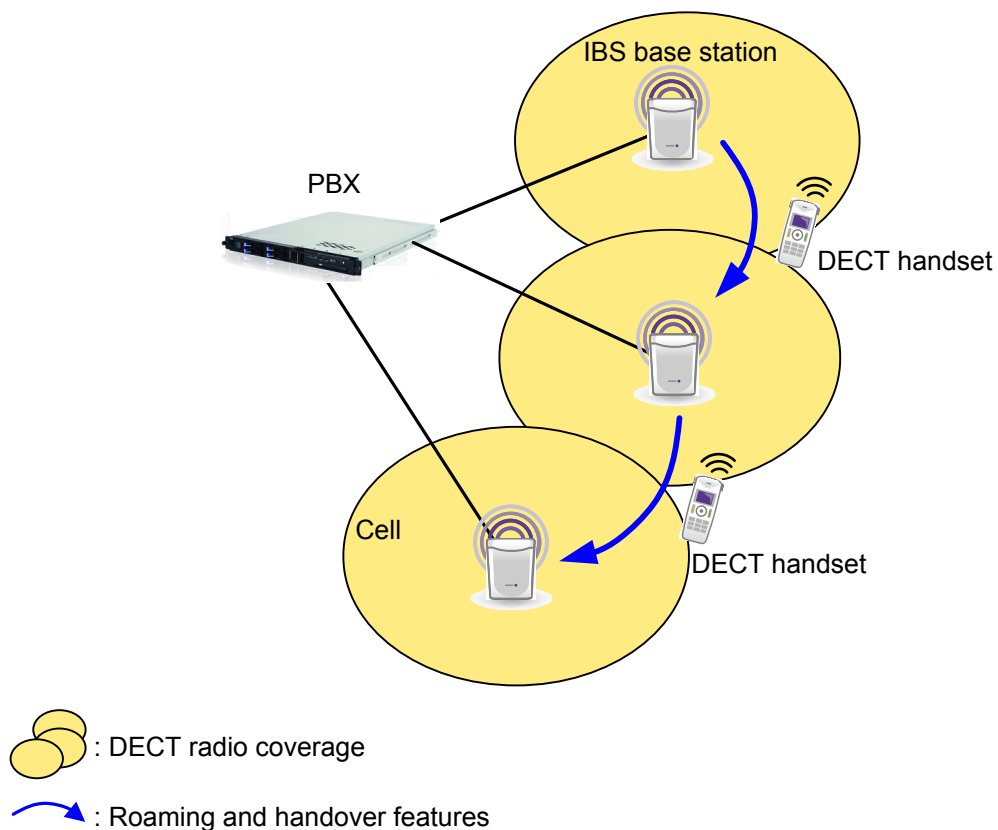


Figure 2.1: DECT service view example

IBS base stations handle mobility features (roaming and handover) and communications to/from DECT handsets (see: [DECT features](#) on page 17). The roaming feature allows DECT handset users to make

or receive calls from any location in the DECT coverage area. The handover feature allows DECT handset users to move from one IBS base station to another one during a call. Transfer to the other IBS base station does not affect users (seamless handover): there is no interruption of the call.

2.2 DECT components

2.2.1 IBS base stations

The IBS base stations are available in several versions:

- IBS NG (4070 DECT IBS)
- 8379 DECT IBS (available as of OXO Connect R3.0)

All IBS base stations include a radio frequency module able to handle any of the DECT frequency ranges addressed by the PBX:

- DECT Europe (frequency range between 1881.792 and 1898.206 MHz)
- DECT LATAM (frequency range between 1912.896 and 1929.312 MHz)
- DECT Asia/Thailand (frequency range between 1902.598 and 1918.944 MHz)
- DECT US (frequency range between 1916.060 and 1934.496 MHz)

IBS base stations operate in the DECT frequency range configured on PBX (see: [Configuring the DECT frequency range used by IBS base stations](#) on page 30), and sent to the station at initialization. IBS NG and 8379 DECT IBS are detected by the PBX during their initialization. The base stations reboot and run with the frequency range defined in PBX configuration.

As of release 3.0, 8379 DECT IBS and IBS NG share the same software binary stored on the PBX (8379 DECT IBS software binary). This 8379 DECT IBS software binary also addresses IBS NG base stations. In a release prior to 3.0 (without any available 8379 DECT IBS software binary), 8379 DECT IBS downloads the software binary available on the PBX, but does not install it. 8379 DECT IBS runs with its current software version.

8379 DECT IBS is fully compatible with IBS NG. 8379 DECT IBS can be added to an existing installation including IBS NG.

All IBS base stations can be deployed in indoor or outdoor environment.

2.2.2 DECT GAP handsets

By default, Alcatel-Lucent DECT GAP handsets operate in proprietary mode (i.e. like 8232 DECT sets); third party DECT GAP handsets usually operate in basic mode (though some may operate in advanced mode):

- Proprietary mode: This mode is based on a proprietary protocol over GAP between the DECT handset and PBX, offering a rich level of service
- 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.

2.3 DECT features

2.3.1 Mobility management

- roaming
- intracell handover (on the same base station)
- intercell handover (between base stations).

2.3.2 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 synchronize 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 recognize 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 synchronized with the system, the handset decides on the most appropriate channel for a call. It chooses the least disrupted of the free channels.

2.3.3 Inter- and intra-cell handover procedures

The radio coverage of a base station forms a "cell".

Intercell handovers 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 handover is performed on the same base station towards a higher quality channel.

2.4 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.

ALE International 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 catalog and approval zone.

table 2.1: DECT list of countries and regions

Country or zone of registration	Corresponding region denomination	ALE International DECT availability	
		Approval	Catalog
All CE countries	1	Eur	Eur
US+Canada	2	US	US
APAC/ ASIA			
Australia	1	Eur	Eur
Bangladesh (2T)	1	Eur	Eur
Bhutan (2T)			
Cambodia	1	Eur	Closed
China	4	Asia	Asia
Hong Kong	1	Eur	Eur
India	1	Eur	Eur
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

Country or zone of registration	Corresponding region denomination	ALE International DECT availability	
		Approval	Catalog
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
Peru	3	Latam	Closed

Country or zone of registration	Corresponding region denomination	ALE International DECT availability	
		Approval	Catalog
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

Country or zone of registration	Corresponding region denomination	ALE International DECT availability	
		Approval	Catalog
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
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

Country or zone of registration	Corresponding region denomination	ALE International DECT availability	
		Approval	Catalog
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
Belorussia (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
Hungary	1	Eur	Eur

Country or zone of registration	Corresponding region denomination	ALE International DECT availability	
		Approval	Catalog
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

2.5 DECT engineering rules

The DECT engineering rules are described in the document: **DECT and IP-DECT Engineering Rules and Site Survey Kit Manual** (reference: 8AL90874).

2.6 IBS base station deployment

This section describes the deployment of indoor and outdoor IBS base stations.

2.6.1 Base station deployment procedure

To deploy the IBS 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).

2.6.2 Installation

2.6.2.1 Attaching an indoor base station

The indoor base station is supplied with an attachment kit comprising:

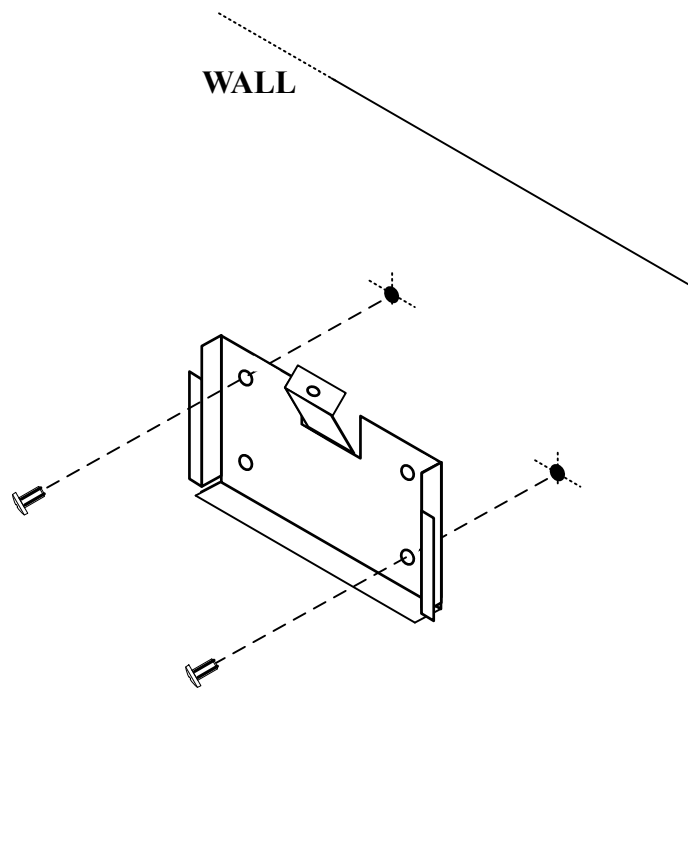
- a metal attachment bracket,
- 2 screws (Ø3.5 x 25 mm) and 2 dowels (Ø6 x 30 mm).

There are two methods of fixing the base station to a wall (in the vertical position):

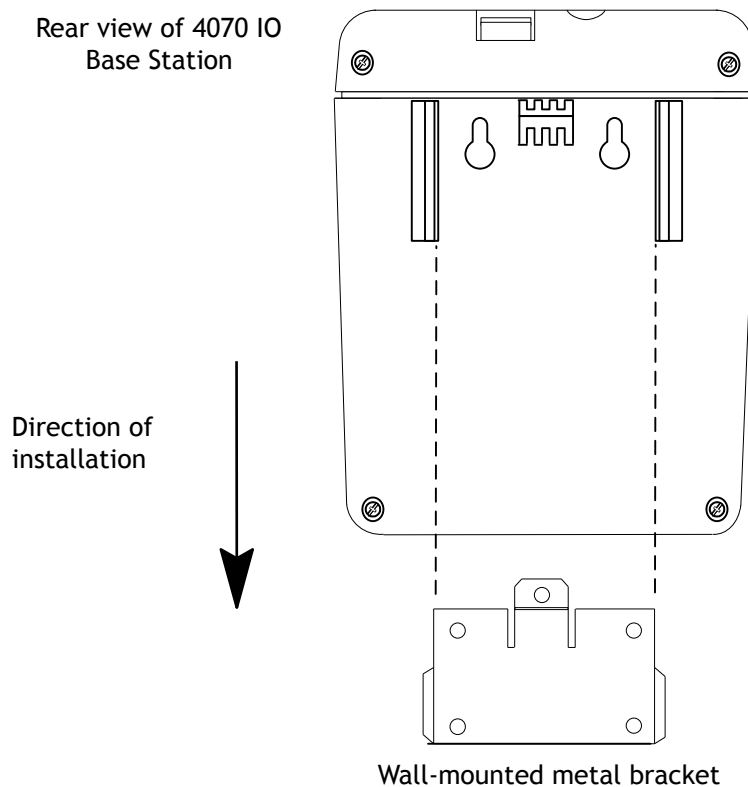
1. by mounting the base station on a metal bracket,
2. directly on the wall, by means of the two slots provided in the base station.

2.6.2.1.1 Mounting an indoor 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 indoor base station into the slots provided on the bracket as shown below:

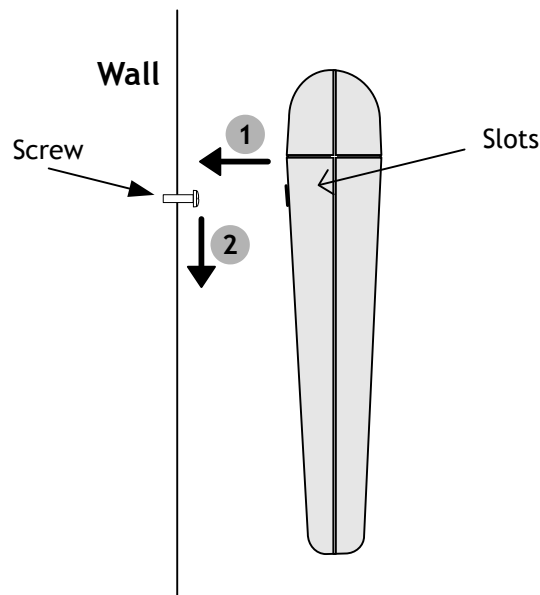


Remark:

The base station must be installed with the LED at the top.

2.6.2.1.2 Attaching an indoor 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.



2.6.2.2 Attaching an outdoor base station

2.6.2.2.1 Wall and mast mounting kit

2.6.2.2.1.1 Wall attachment

The outdoor base station can be mounted on a wall:

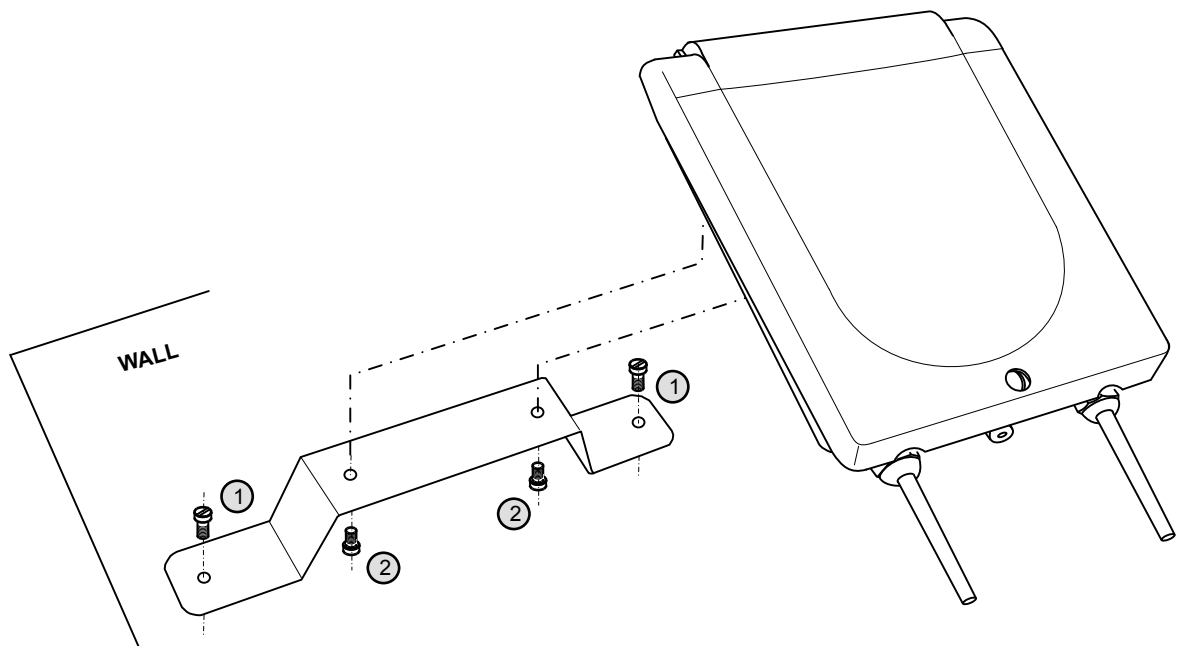


Figure 2.2: Wall attachment for an outdoor base station

1. Attach the wall support to the wall with two screws (not provided)
2. Attach the outdoor base station to the support with the two screws provided

2.6.2.2.1.2 Mast attachment

The outdoor base station can be mounted on a mast:

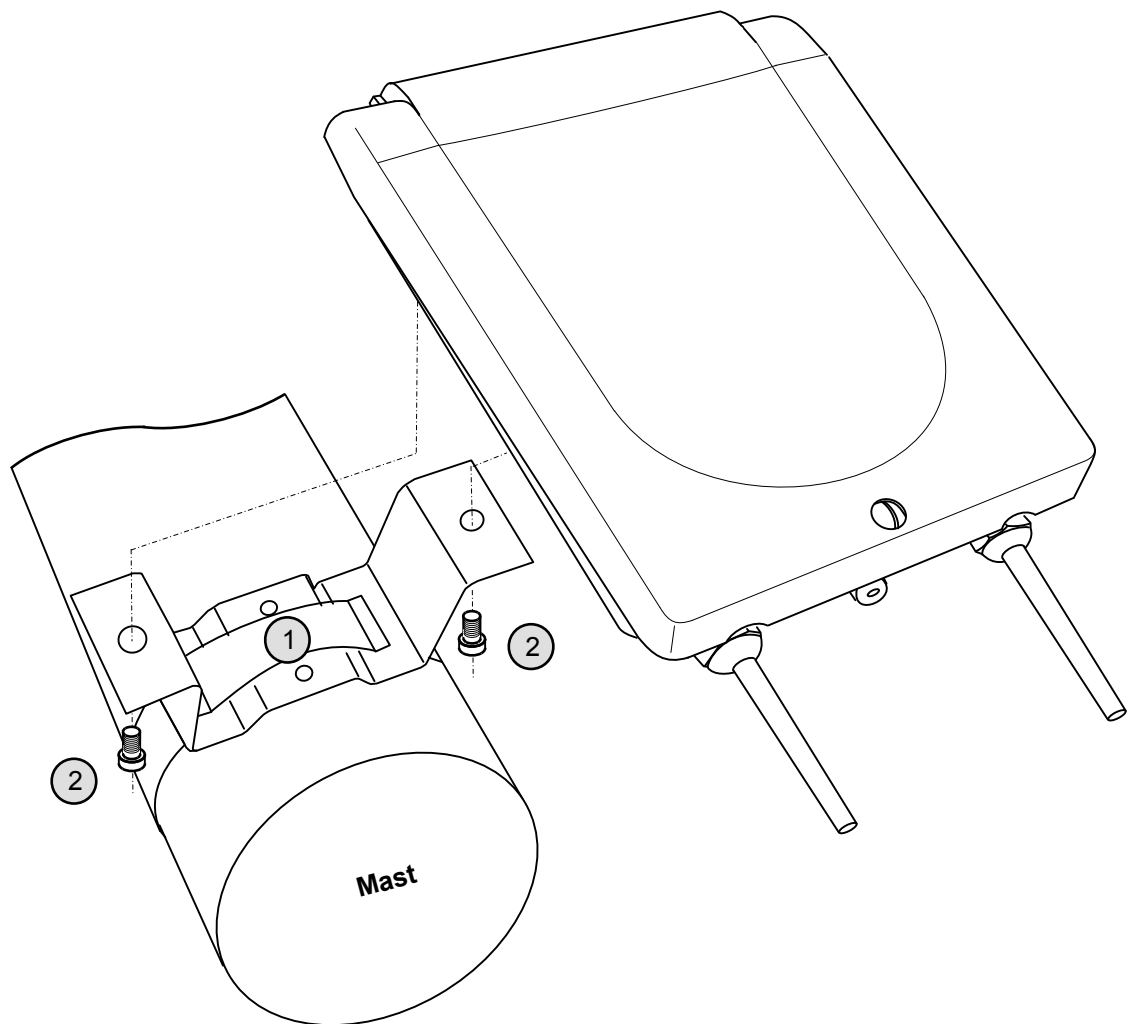


Figure 2.3: Mast Attachment for a 4070 EO Base Station

1. Attach the mast support to the mast with a pipe-collar (not provided)
2. Attach the outdoor base station to the support with the two screws provided

2.6.2.2.2 Wall offset mounting kit

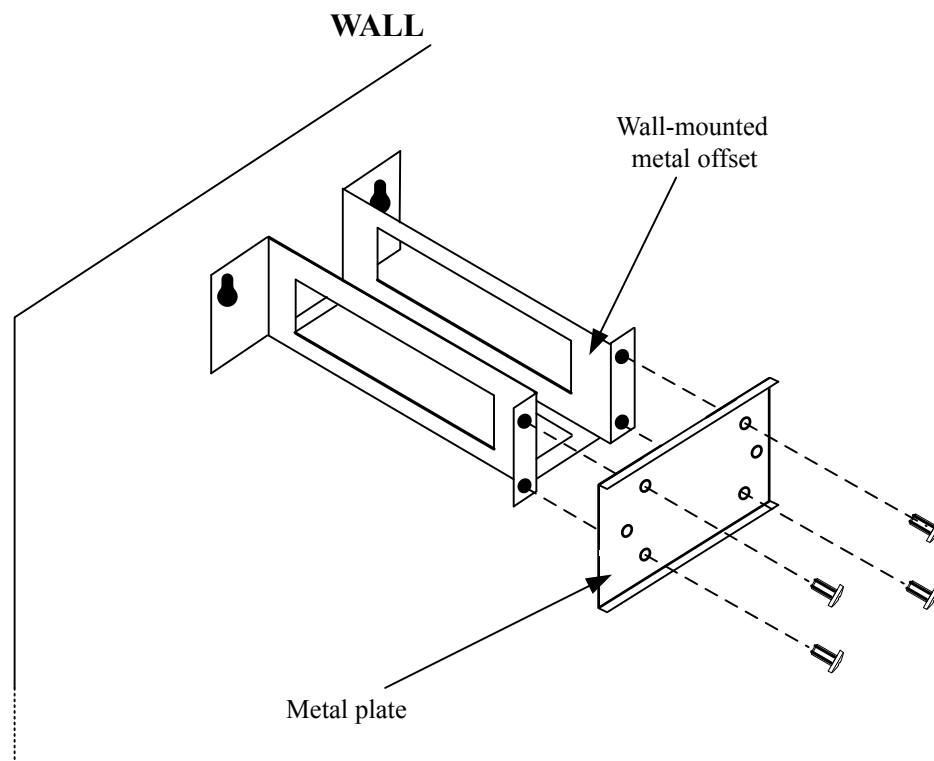
This kit is not included in standard delivery of the outdoor base station. It must be ordered separately.

The base station is mounted as follows:

1. Position the metal plate on the offset and attach it with the screws:

Remark:

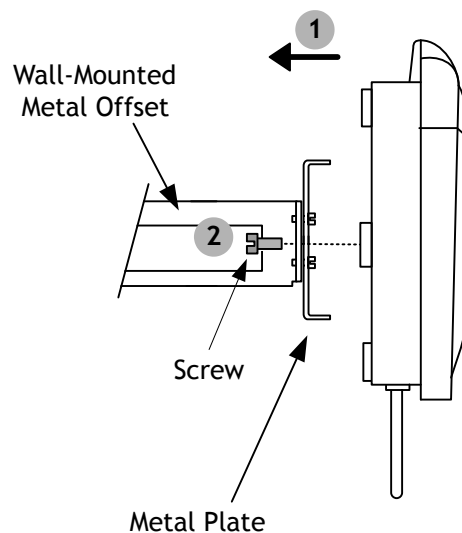
screws to be used: Ø3.5 x 25 mm.



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:

use the 2 hex head screws provided with the kit.



2.6.3 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.

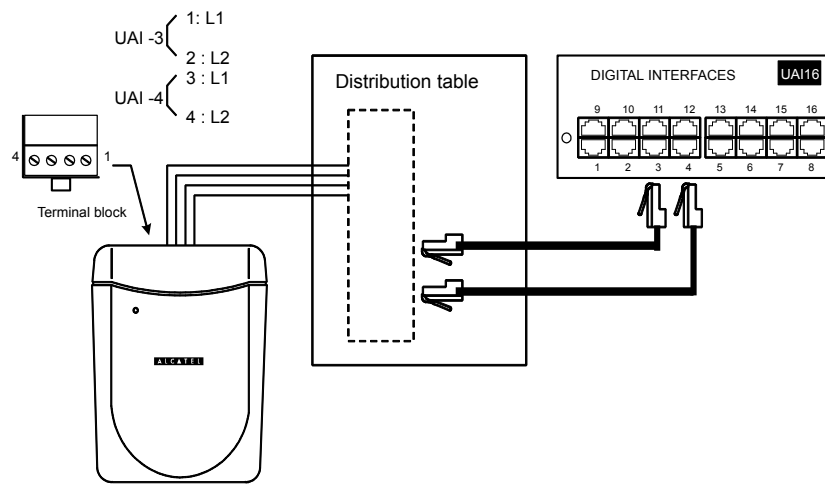
If there is a two-cable connection:

- use two neighboring 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.

2.6.4 Configuration

Note:

Differences between 4070, 4070 NG, and 8379 DECT IBS 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 and 8379 DECT IBS 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 becomes too weak.

2.6.4.1 Configuring the DECT frequency range used by IBS base stations

Select and configure the DECT frequency range used by IBS base stations when they communicate with DECT handsets. The DECT frequency range must be configured on PBX. It is sent to IBS base stations at initialization.

1. In OMC, go to: **System Miscellaneous > DECT/PWT Frequencies**
2. Select the **DECT** radio button
3. According to your geographical area, use the drop-down menu to select the corresponding DECT frequency range (**Europe**, **LATAM** (South America), **Asia**, **US** or **Thailand**)

The DECT frequencies are displayed on screen. Except for US, all frequencies are available and selected.

4. If necessary, you can limit the DECT frequencies used by IBS base stations. In this case, clear the corresponding check boxes
5. Click **OK** to validate

The base stations automatically reboot and run in the DECT frequency range selected on PBX

2.6.4.2 Configuring the IBS base station settings

After initialization, the IBS base station is detected by the PCX and displayed in the **Subscribers/Base stations List** available from OMC. The PBX retrieves information from the IBS base station such as:

- Boot software version
- Firmware version
- RF board number
- Serial number
- Part number

The following settings can be displayed/modified via OMC:

1. In OMC, select **Subscribers/Basestations List**
2. Select the IBS base station and click the **Details** button
3. Review/modify the following fields:

Firmware version	Displays the firmware version of the base station (read-only)
Boot software version	Displays the boot software version of the base station (read-only)
RPN	Use the browser button to select the Radio Part Number (RPN) of the base station. Each base station has its own RPN, which is an hexadecimal two digit number (value between 0 and 79). <i>Note:</i> <i>Values between 80 and 254 are reserved for the base stations associated xBS system.</i>
Line Length	Select one of the following values according to the length of the cables used between the IBS base station and the UA board: • Short line: 0 to 400 m (default value) • Medium line: 400 to 800 m • Long line: 800 to 1200 m
Antenna Diversity	If necessary, select Diversity to allow the base station to receive calls on either of its two antennas according to the reception quality (same for transmission) (default value: No diversity)
RF Board Number	Displays the RF board number of the base station (read-only)
Serial Number	Displays the serial number of the base station (read-only)
Part Number	Displays the part number of the base station (read-only)

4. Click **OK** to validate

After modification, the base station reboots (regardless of any call in progress).

2.7 DECT configuration

Configuring the system's DECT 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 configuration, the dialing plan must be defined and the hardware configuration (installing interface boards, recognizing sets, etc) completed.

2.7.1 Configuring the 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 OXO Connect, a type-B ARI is assigned by the DECT protocol (ARC = 1, non modifiable)
- the EIC (Equipment Installer Code) is the number assigned by ETSI to each maker or distributor offering DECT system
- 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.

1	0	0	0	0	4	3	6	0	7	4
001	000	000	000	000	100	011	110	000	111	1
ARC	EIC					FPN			FPS	
ARI										

To enter the system ARI number with OMC (Expert View):

Select: **DECT > DECT/PWT/ARI/GAP->** enter the ARI number (the system deduces the EIC, FPN and FPS fields automatically).

Important:

The ARI number must be modified by the installer (following the above rules) before registering any DECT sets.

2.7.2 Configuring GAP authentication

This service allows to secure communications between the DECT system and GAP handsets. This requires to configure the following parameters on the PCX:

- The GAP authentication feature must be activated
- An authentication code (AC) must be entered on the PCX. By default, the AC is set to 0000 for all GAP handsets when the GAP authentication feature is activated.

The AC code is sent to the mobile during the registration procedure. It is identical for all GAP handsets and must not be entered manually in the GAP handsets after registration. If this the case, the administrator must delete the GAP handset and make a new registration to retrieve the current AC.

After download, the AC is automatically changed to a User Authentication Key (UAK) that is stored internally in GAP handsets. This changes also occur on the DECT base stations. After the change has been done on both sides, the AC is deleted and only the UAK is used for GAP authentication.

Authentication takes place when the GAP handset establishes a call. A cryptographic challenge/response mechanism is started between the GAP handset and the DECT system using the UAK. This code is then compared with the one configured in the DECT system. If it matches, the GAP handset is authenticated and the call can continue; if not, it is stopped.

- To enable GAP authentication and define an authentication code with OMC (Expert View):

Select: **DECT > DECT/PWT/ARI/GAP**

Select the **Activate GAP Authentication** check box

Enter an authentication code of between 4 and 8 digits in the **Authentication code** parameter.

2.7.3 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: **Subscribers/Base stations List -> Add ->** add the required number of DECT accesses by selecting **IBS/xBS** and the number of devices, then validate by clicking **OK**

Select **Subscribers/Base stations List -> GAP Reg. ->** The GAP registration procedure is under way when the **Register GAP Handsets** window appears.

Note:

*If the **GAP registration selection** pop-up opens, select the **DECT IBS/DECT xBS** radio button and click **OK**.*

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

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**.

2.8 DECT traffic counters

The OXO Connect PCX manages a set of DECT traffic counters. These specific counters are mainly used to ascertain that there are enough DECT 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 counters are available from the web-based tool (DECT menu).

3.1 Detailed description

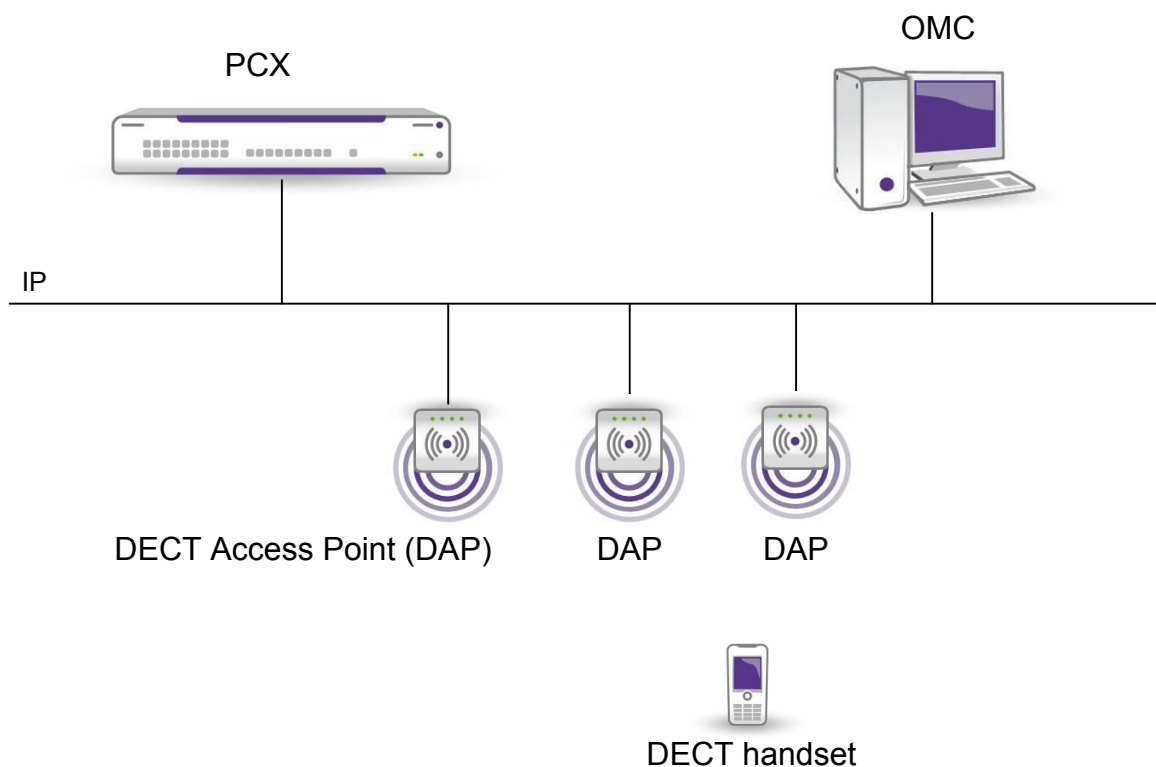
3.1.1 Overview

The IP-DECT solution combines IP and DECT technologies to provide a wireless telephony solution on IP networks.

Unlike DECT base stations, IP-DECT base stations are connected to the IP network and use the SIP protocol to communicate with the OXO Connect. However, DECT handsets connect to the IP-DECT base stations via radio links complying with the DECT protocol.

A mixed system of DECT and IP DECT base stations, can be deployed. This configuration is named Dual DECT.

The following figure provides a schematic view of an IP-DECT solution:



The IP-DECT solution is based on the following components:

- IP-DECT base stations also called DECT Access Point (DAP), see: [DECT Access Point \(DAP\)](#) on page 36
- A DAP Configurator integrated in the OMC, see: [DAP Configurator](#) on page 35
- Managed DECT handsets, see: [Handset management](#) on page 38

3.1.2 Description

3.1.2.1 DAP Configurator

DAP Configurator is used to configure and manage the IP-DECT system. It is integrated in the OMC.

3.1.2.2 DECT Access Point (DAP)

DECT Access Points (DAP) are connected to the IP network and provide interface for DECT over IP to handle DECT handset registration and calls to/from the OXO Connect.

- DAPs act as DECT/SIP gateways.
- Up to 16 DECT Access Points (DAP) can be connected.
- Supported DAPs:
 - 4080 IP-DECT
 - 8340 Smart IP-DECT
 - 8340-C Smart IP-DECT

DAPs require a configuration file to be downloaded via TFTP protocol at each startup/reboot. This configuration file is generic for all the DAPs. It is generated by DAP Configurator,

Note:

At installation, a first file is created by OXO Connect with a GK (Gatekeeper) section containing the IP address of the PBX and the SIP port used. These parameters are updated by the OXO Connect if they are changed in the system.

Once connected to the LAN, DAPs startup and are automatically discovered by the OXO Connect.

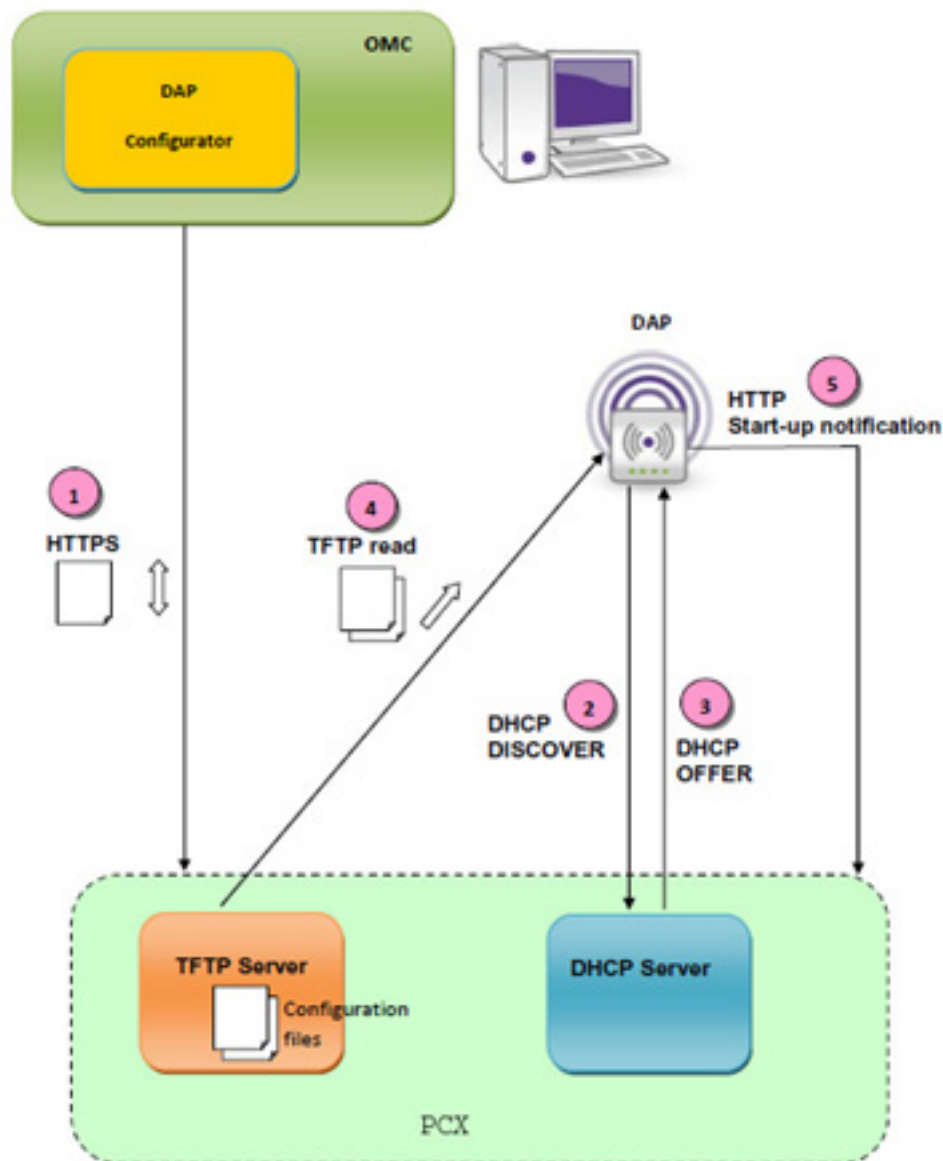


Figure 3.1: DAP discovery process

1. **Step 1:** The IP-DECT configuration file is updated by the OMC (DAP Configurator) and pushed back to the OXO Connect
2. **Step 2-3:** The DAP gets its network configuration (IP address / TFTP server address) from the DHCP server. This DHCP server is either the DHCP server of the OXO Connect or another DHCP server configured to return the IP address of the OXO Connect's TFTP server. DAPs give the preference to the ALU DHCP offer. To allow DHCP configuration, the network must support broadcast.
3. **Step 4:** The DAP gets its configuration file from the OXO Connect via TFTP. The IP-DECT configuration file cannot be exported to another server.
4. **Step 5:** Once up and running, the DAP sends a notification to the OXO Connect via HTTP for auto-discovery by the system.

DAPs are designed to support:

- Up to eleven simultaneous calls per DAP

- A maximum of twenty-five DECT handsets registrations per DAP

Each DECT handset registers on a dedicated DAP during its installation phase. This DAP operates as the **registration DAP** for the DECT handset.

The registration DAP operates as the entry point for DECT handsets on the IP network. The registration DAP also ensures registration of DECT handsets on the OXO Connect via the SIP protocol. The registration DAP is not necessarily the DAP to which the DECT handset is currently connected to.

3.1.3 Quality of Service (QoS)

DAPs support differentiated Quality of Services (QoS) on layer 3 (optional).

The DSCP value can be configured with the OMC. When the Call Server quality of service is modified with OMC, the DSCP setting, available in the DAP configuration file (**dapcfg.txt**), is automatically updated. All DAPs automatically reset to take this modification into account.

The default DSCP value is 46 (Expedited Forwarding).

3.1.4 Using VLAN Ids and Priority (IEEE 802.1q and IEEE 802.1p)

The DAPs optionally support:

- Priority on Layer 2 (IEEE 802.1p): The default setting is 5 (Voice, < 10 ms latency). This setting can be set to any value between 0 and 7.
- VLAN Tagging on Layer 2 (IEEE 802.1q)

The VLAN ID and priority must be set on the switch port manually ("Port Based" option configured).

The switch port must not accept any IEEE 802.1q tagging from the DAP.

3.1.5 Handset management

Handset management is done via OMC using HTTP requests sent from OXO Connect to the DAP. These HTTP requests are protected by a basic HTTP authentication.

The password is generated by OXO Connect and can be regenerated via OMC.

The IP-DECT solution supports different handset models:

- 8212 DECT (in GAP mode), 8232 DECT (in GAP mode) and 8242 DECT (in CAT-iq mode)
- GAP handsets (seen as generic IP-DECT handsets)

The DECT handsets subscribe to a DAP, which register them in the OXO Connect as SIP phones.

Note:

A-GAP protocol is not supported

3.1.6 Dial by name

The dial by name feature is available on the handsets connected to the DAPs (except for generic GAP handsets).

This feature provides the ability to make a call entering the first characters of the last name of a user listed in:

- The internal directory of the OXO Connect
- An external LDAP server if defined in the configuration via OMC

3.1.7 Emergency calls

When an emergency call is set up from a remote site, the location associated to the OXO Connect (with public network access) may be wrong. It is recommended not to make emergency calls with IP-DECT handsets located on a remote site.

3.1.8 Security

3.1.8.1 SIP password

The SIP password used to register the IP-DECT handset into the OXO Connect is configured in the **dapcfg.txt** file that is retrieved by the DAP via TFTP protocol. This password can be reset by the OMC (IP-DECT Subscriber details, in the SIP parameters) and is common to all the IP-DECT handsets. Once modified, a new **dapcfg.txt** file is automatically generated by invoking the DAP Configurator in silent mode. This will trigger the reset of the DAP.

As this information is confidential, the SIP password is encrypted by the DAP Configurator with a secret shared with the DAP's.

3.1.8.2 SIP-TLS and SRTP

SIP-TLS and SRTP are not supported.

3.1.8.3 HTTP connection

The OXO Connect makes HTTP requests to the DAP for handset management. Those HTTP requests are protected by a basic HTTP authentication. The password set by the OMC is transferred to the DAP by the **dapcfg.txt** file after having been encrypted by the DAP Configurator.

3.1.9 Limits and restrictions

- Windows Vista is not supported for the OMC when the IP-DECT solution is deployed
- The maximum number of DAPs that can be connected to the IP-DECT solution is fixed. For more information, see the document [1]
- The maximum number of IP DECT handsets that can be configured for the IP-DECT solution is fixed. For more information, see the document [1]
- Up to 170 DECT handsets (120 IBS DECT handsets + 50 IP-DECT handsets) in case of dual DECT topology
- DAPs are designed to support:
 - Up to eleven simultaneous calls per DAP
 - Channel 12 is used for clock synchronization when required
 - A maximum of twenty-five DECT handsets registrations per DAP
 - G.711 and G.729 codecs

Note:

The 8340-C Smart IP-DECT does not support G.729

- SIP-TLS and SRTP are not supported
- Only DECT GAP handsets are supported (no A-GAP protocol)
- The DAP configuration file cannot be exported to another TFTP server. It is only available on the OXO Connect server
- Only digits are allowed for handsets dialing numbers (# and * are forbidden)
- Call recovery is not supported
- For IP-DECT sub system (in the cases of single or dual topology), it is not possible to restrict the frequency plan. This entails that it is impossible to deploy IP-DECT in the countries for which the frequency plan must be restricted (legal constraints) compared to all frequencies available for the country localization

- Definition of the frequency plan in OMC is only applicable to IBS-DECT sub system

The following restrictions apply only to dual DECT systems:

- Roaming between IP-DECT and IBS-DECT sub systems is not possible. Roaming is only possible within the DECT sub system where the DECT handset has been registered to.
- IP-DECT and IBS-DECT sub systems are not synchronized. Handover is only possible between synchronized base stations, thus, within each DECT sub system but not between IP-DECT and IBS-DECT.
- The level of service and user interface may be different for a same type of DECT handset when attached either to IBS-DECT or IP-DECT sub system (Example: 8232 DECT runs in A-GAP mode when connected to IBS-DECT, and in GAP when connected to IP-DECT).
- One given DECT subscriber can only use either IBS base stations or IP-DECT base stations. Nevertheless, the registration of a given handset on both IP-DECT and IBS base stations is possible, by using 2 different subscribers (two licenses required for the same phone - one DECT user and one IP-DECT user), but the level of service and user interface are different.

3.2 Topologies

3.2.1 IP network deployment rules

The following requirements are mandatory for all topologies:

- **DAPs must get their configuration file from the OXO Connect (file cannot be exported). TFTP exchanges must be allowed between all DAPs and the OXO Connect.**
- **All DAPs must be in the same subnet.**
- **Multicast with a TTL fixed to value 1 must be always possible between all DAPs.**
- **A DHCP server is mandatory. DAPs give preference to ALU DHCP offer.**
 - The minimum required signal strength for synchronization (DAP to DAP communication) is - 80 dBm.
 - The ceiling (Minimum RSSI level between an Alcatel-Lucent DECT handset and a DAP) is - 70 dBm in Easy coverage and - 60 dBm in Tricky coverage.

3.2.2 DAPs synchronization, roaming and handover

Radio synchronization of DAPs over the air is the prerequisite for seamless handover.

Handover is possible within one cluster. A cluster is a group of contiguous base stations with overlapping radio coverage. See: [Figure 1](#).

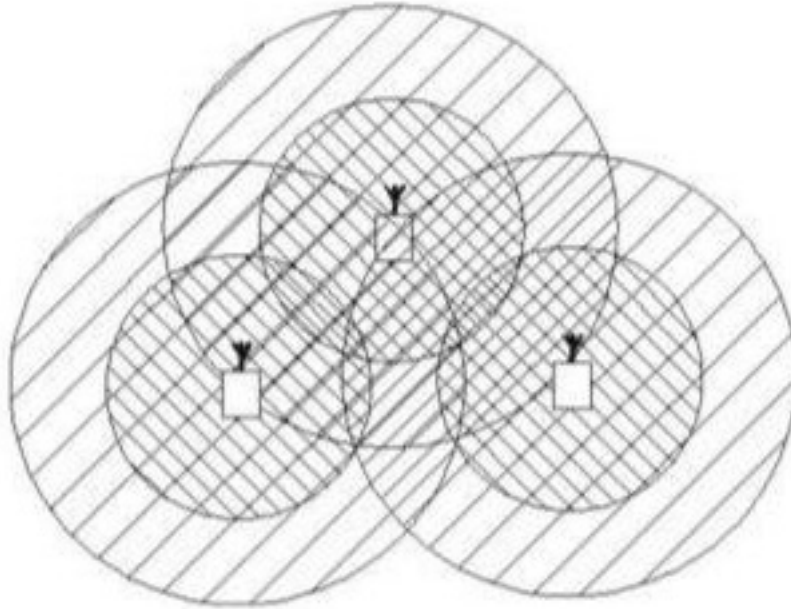
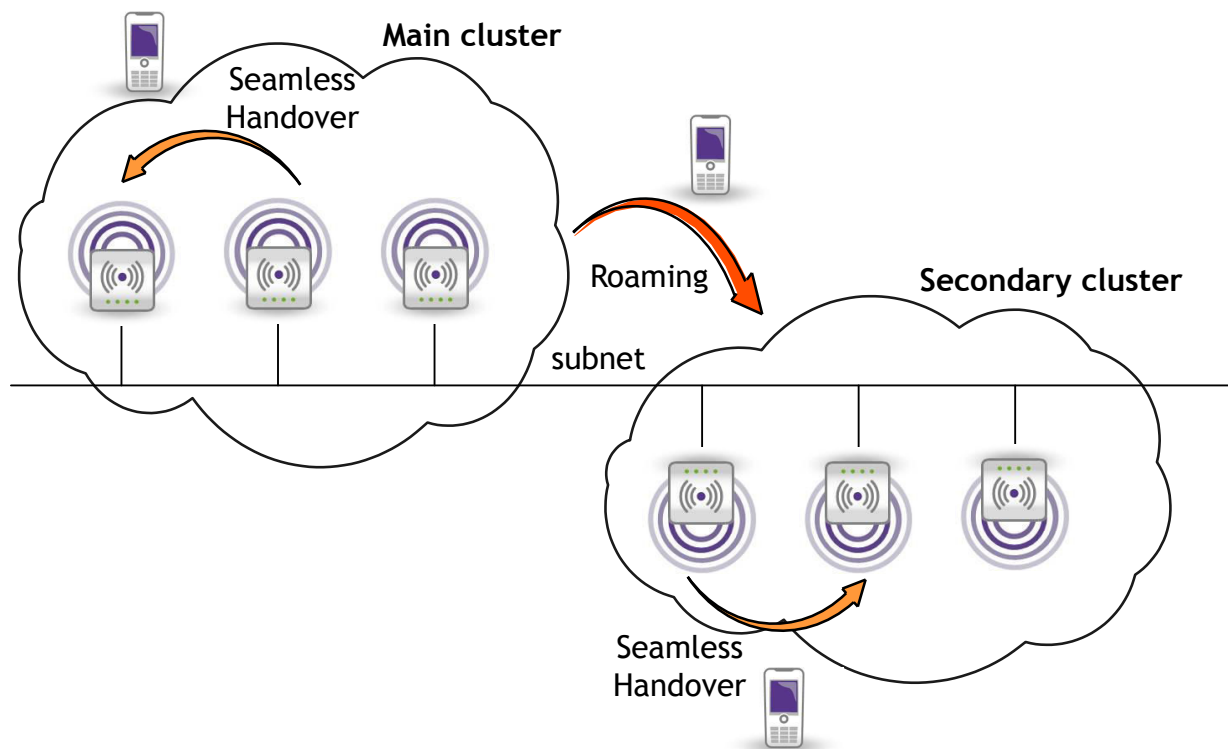


Figure 3.2: Base station cluster example

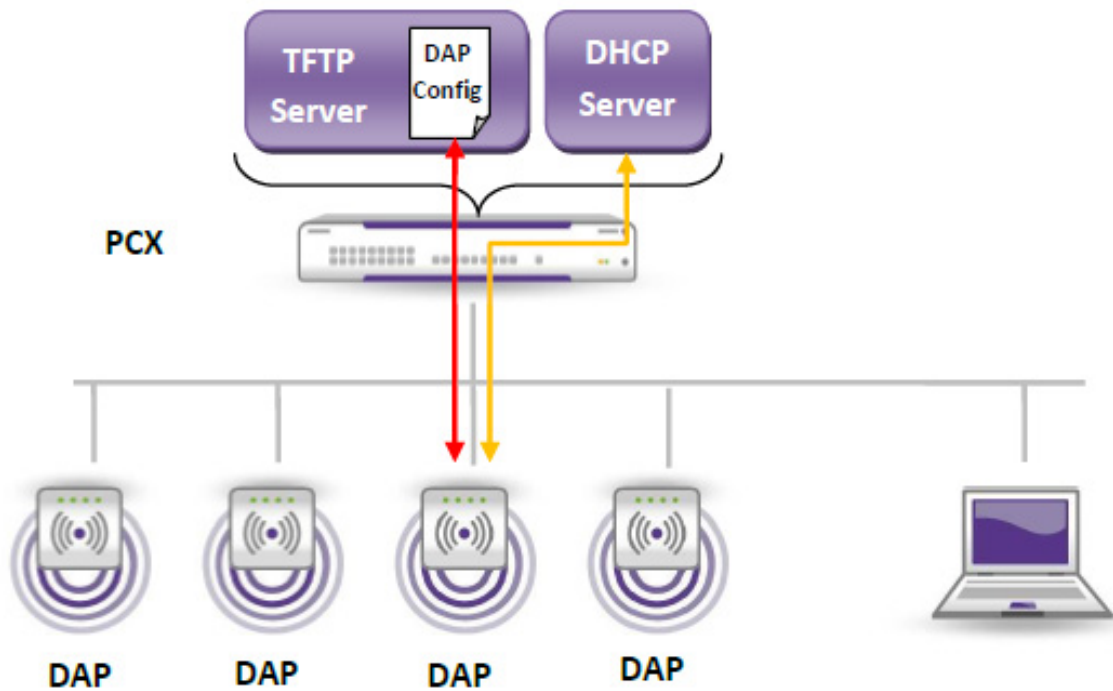
The split RPN is supported, which entails that only two clusters are allowed: main and secondary clusters. The two clusters must be in the same IP subnet. In this case, seamless handover is not possible between the clusters and the calls are released. Only roaming is possible (handover is possible within one cluster).



In case of separated DECT clusters, each cluster has a synchronization master DAP for clock synchronization. On the main cluster (lowest DAP RPN), the LED of the master DAP is fixed, whereas on the secondary cluster the LED of the synchronization master DAP is blinking.

3.2.3 IP-DECT only topology

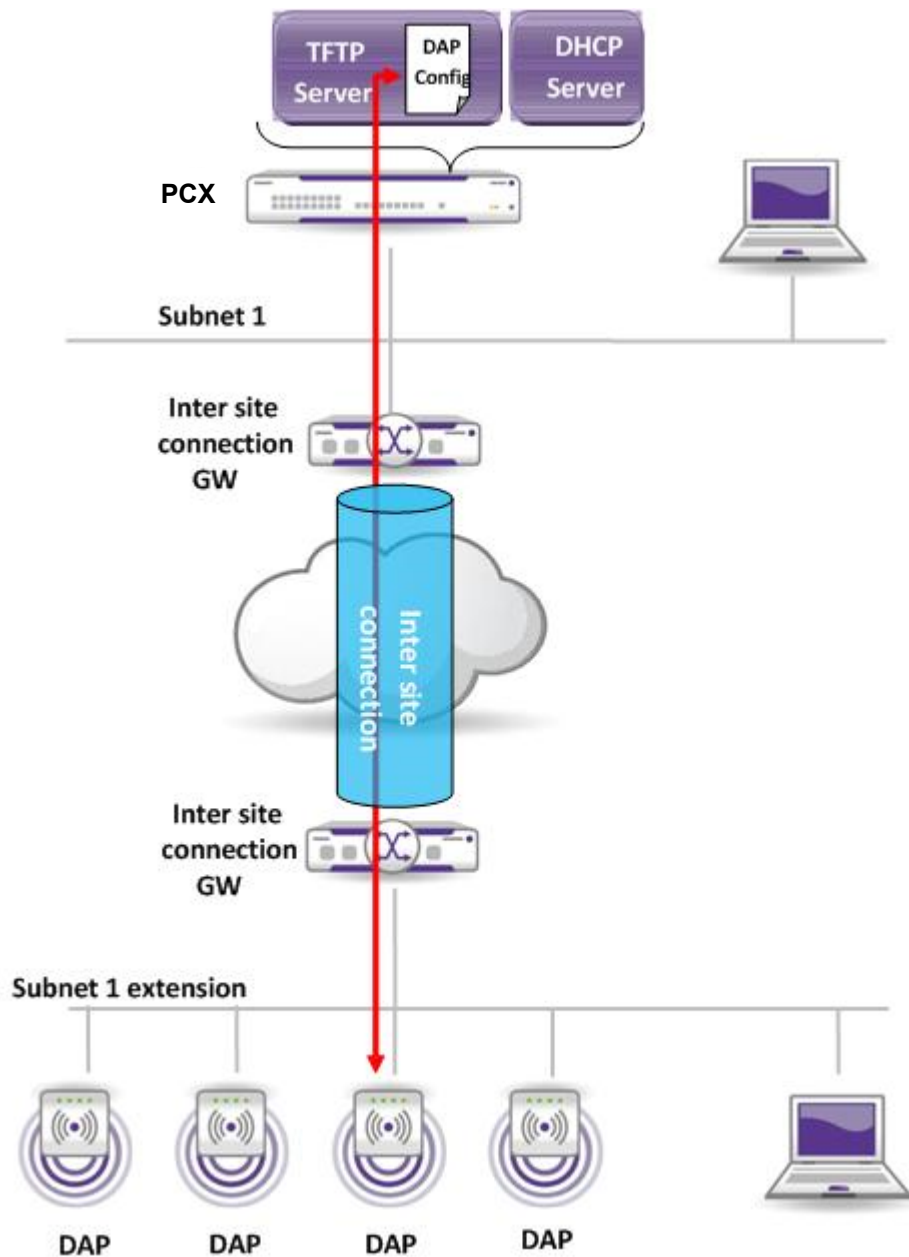
3.2.3.1 OXO Connect and DAPs in the same subnet using OXO Connect DHCP server



Reminder:

IP deployment rules are defined in [IP network deployment rules](#) on page 40

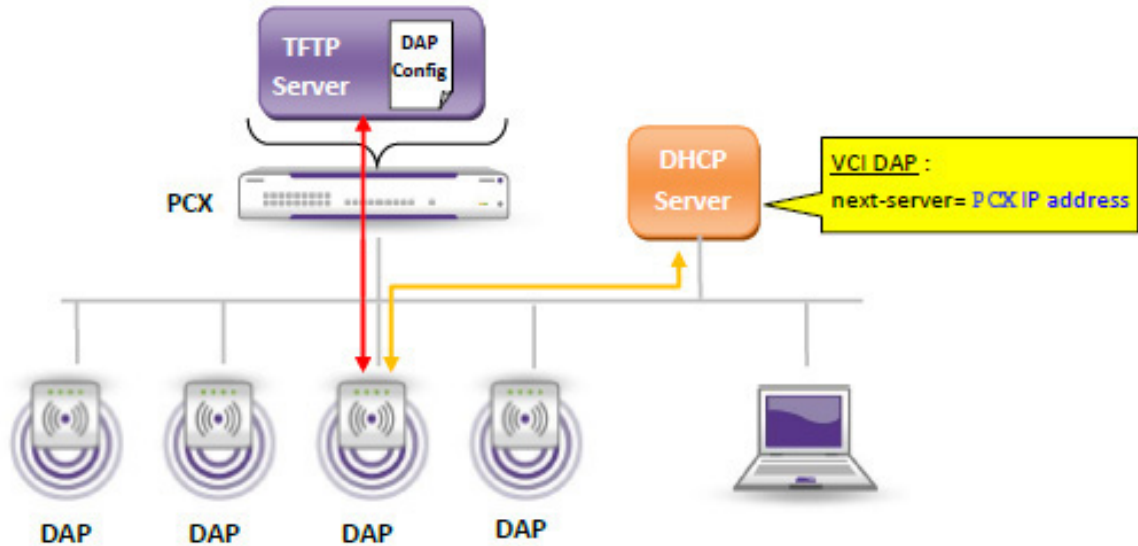
3.2.3.2 DAPs located on remote site with OXO Connect DHCP server



Reminder:

IP deployment rules are defined: [IP network deployment rules](#) on page 40

3.2.3.3 OXO Connect and DAPs in the same subnet with external DHCP server



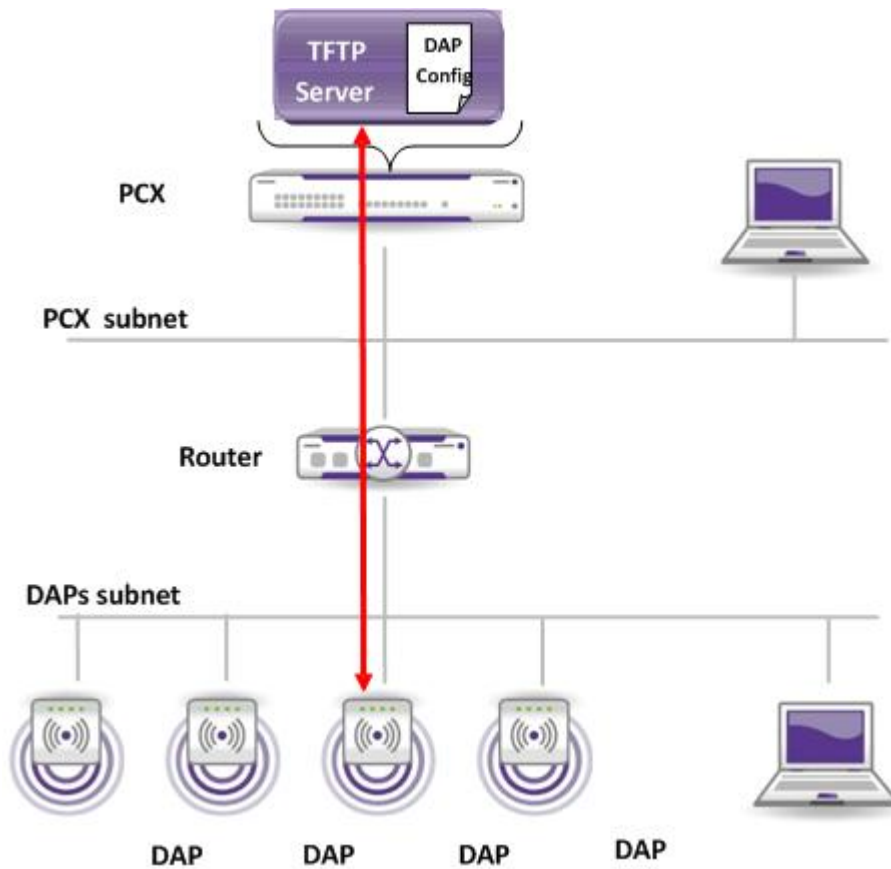
Reminder:

IP deployment rules are defined: [IP network deployment rules](#) on page 40

Moreover:

- The OXO Connect DHCP server must be deactivated
- An external DHCP server must be configured for:
 - Provisioning of IP phones provided by ALE International (IP network settings and device management)
 - DAPs

3.2.3.4 OXO Connect and DAPs in different subnets



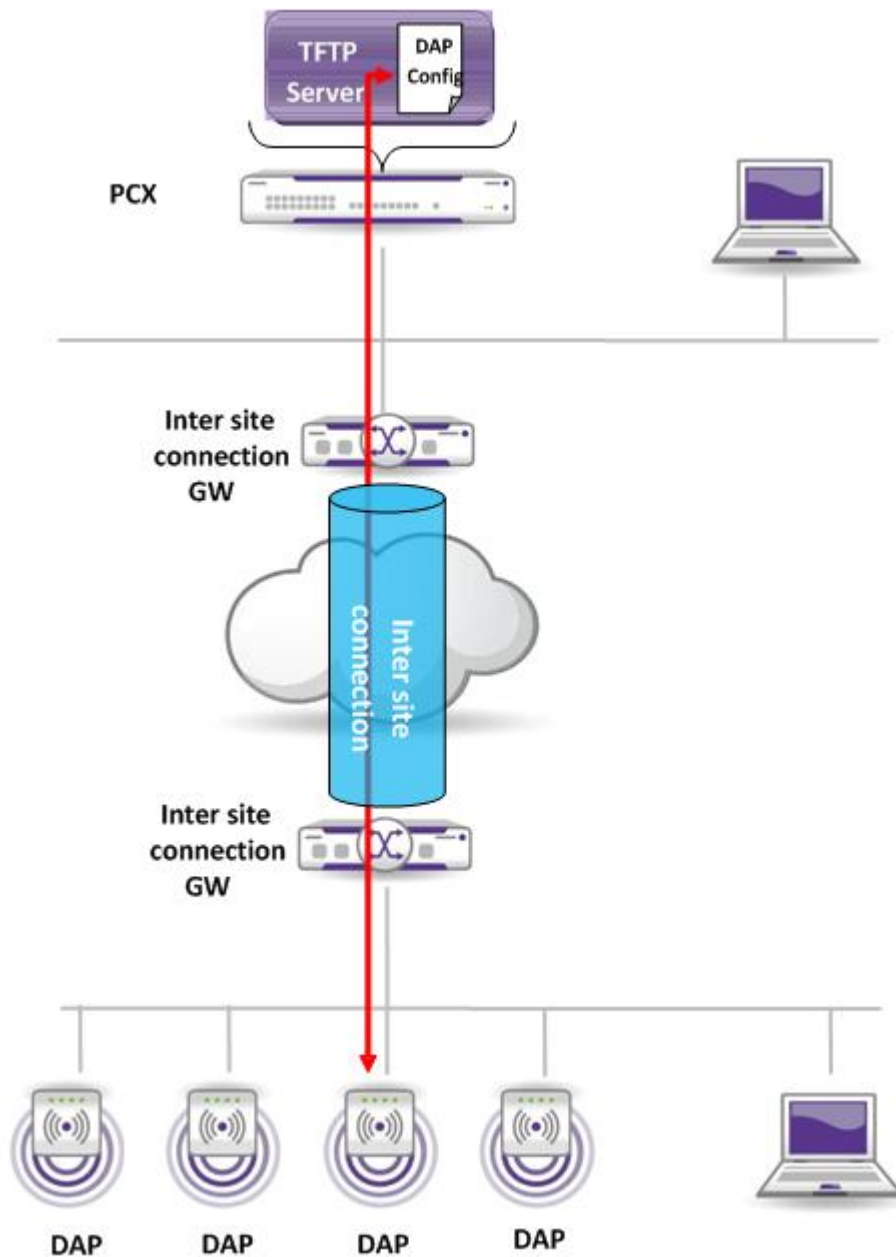
Reminder:

IP deployment rules are defined: [IP network deployment rules](#) on page 40

Moreover:

- The DHCP service must be ensured by an external DHCP server.
- According to DHCP location, the router configuration has to filter or not the DHCP protocol between subnets.

3.2.3.5 DAPs located on a remote site



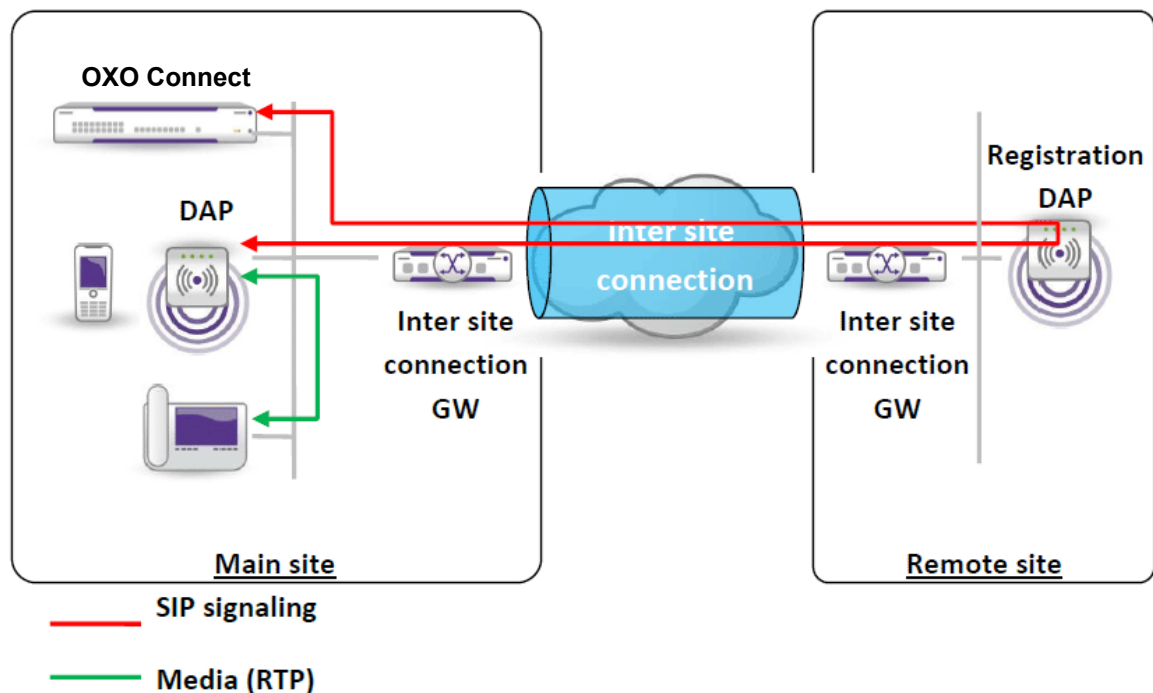
Reminder:

IP deployment rules are defined: [IP network deployment rules](#) on page 40

- Moreover, the DHCP service must be ensured either by the embedded OXO Connect DHCP server or by an external DHCP server according to:
 - The inter site connection, which can filter or not the DHCP protocol.
 - DAPs, which manage the ALU DHCP offer preference

3.2.3.6 Subnet extensions

IP-DECT is deployed on both main and remote sites:



Reminder:

IP deployment rules are defined: [IP network deployment rules](#) on page 40

In a topology with a main site and one secondary site, split RPN must be used to ensure that handsets register to the DAPs on the main site.

Even if the conditions for the IP-DECT solution are satisfied, these topologies can encounter some operating faults depending on the network topology and configuration. Included in these conditions, the inter site connection robustness, quality and bandwidth are important.

Possible issues:

- **Tromboning**

SIP signaling for a DECT handset always goes through its registration DAP. But media (RTP) is directly exchanged with the DAP where the handset was synchronized at time of call setup.

Consequently, in some cases, SIP signaling can be sent back and forth through the inter site connection (tromboning).

- **Inter site connection down**

When the inter site connection is down, provided split RPN is used, only handsets on the remote site cannot receive or make calls (handsets on the main site are not impacted).

Reminder:

Regarding inter site connection:

- Data transmitted through the inter site connection may be encrypted: this may also add some significant delay to the media transmission.
- No specific codec (e.g. reduced bandwidth codec) used for calls going through the inter site connection: the same codec is used for all calls.

3.2.4 Dual DECT topology

DECT handsets are managed differently by the Call Server whether connected to IP-DECT sub system or IBS DECT sub system:

- On IP-DECT sub system, DECT handsets are seen by the Call Server as SIP phones
- On IBS DECT sub system, DECT handsets are managed directly by the Call Server.

In the case of Dual DECT topology:

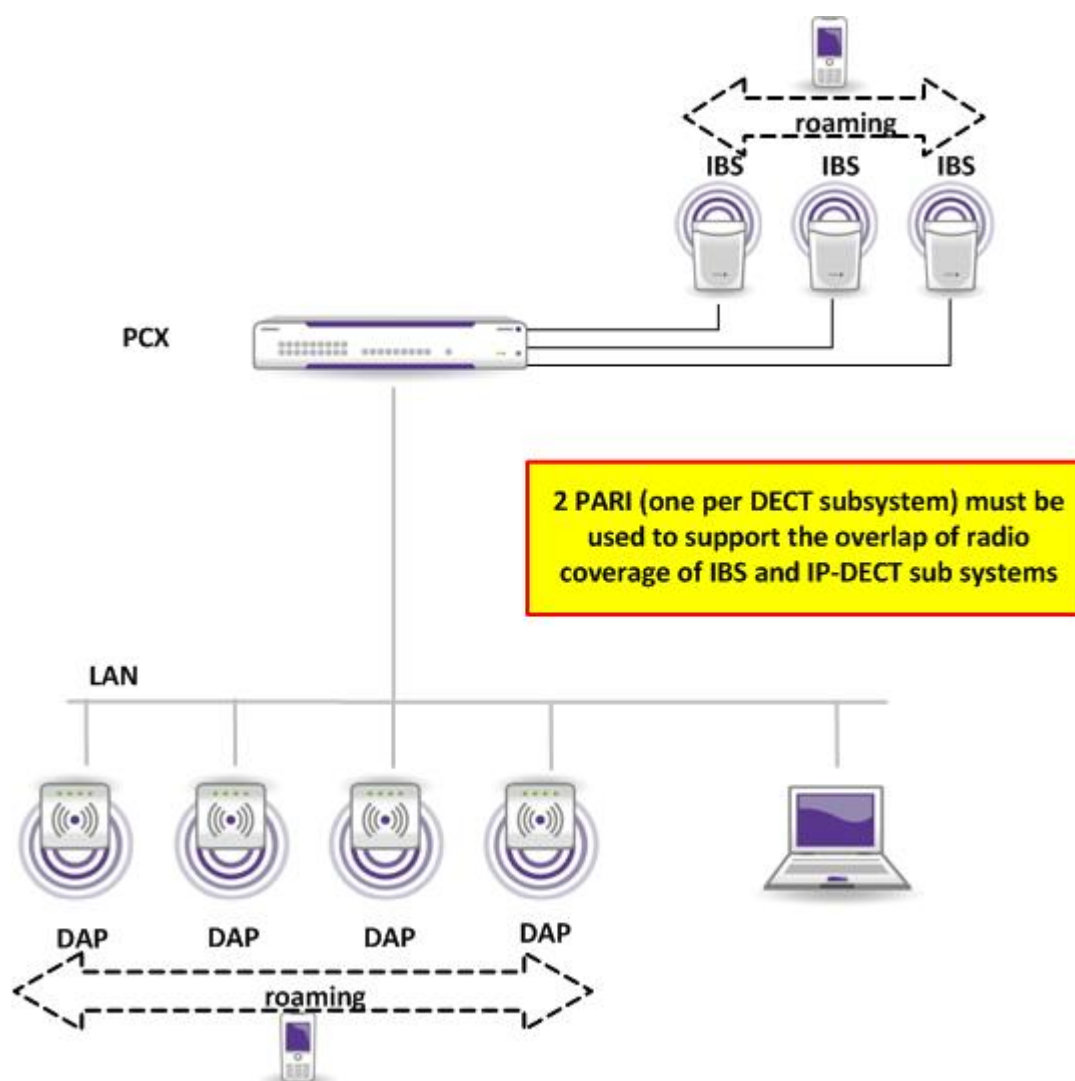
- Two PARI must be used (one per DECT sub system)
- Roaming is only possible within the DECT sub system in which the DECT handset is registered.

There is no roaming between IBS DECT and IP-DECT sub systems.

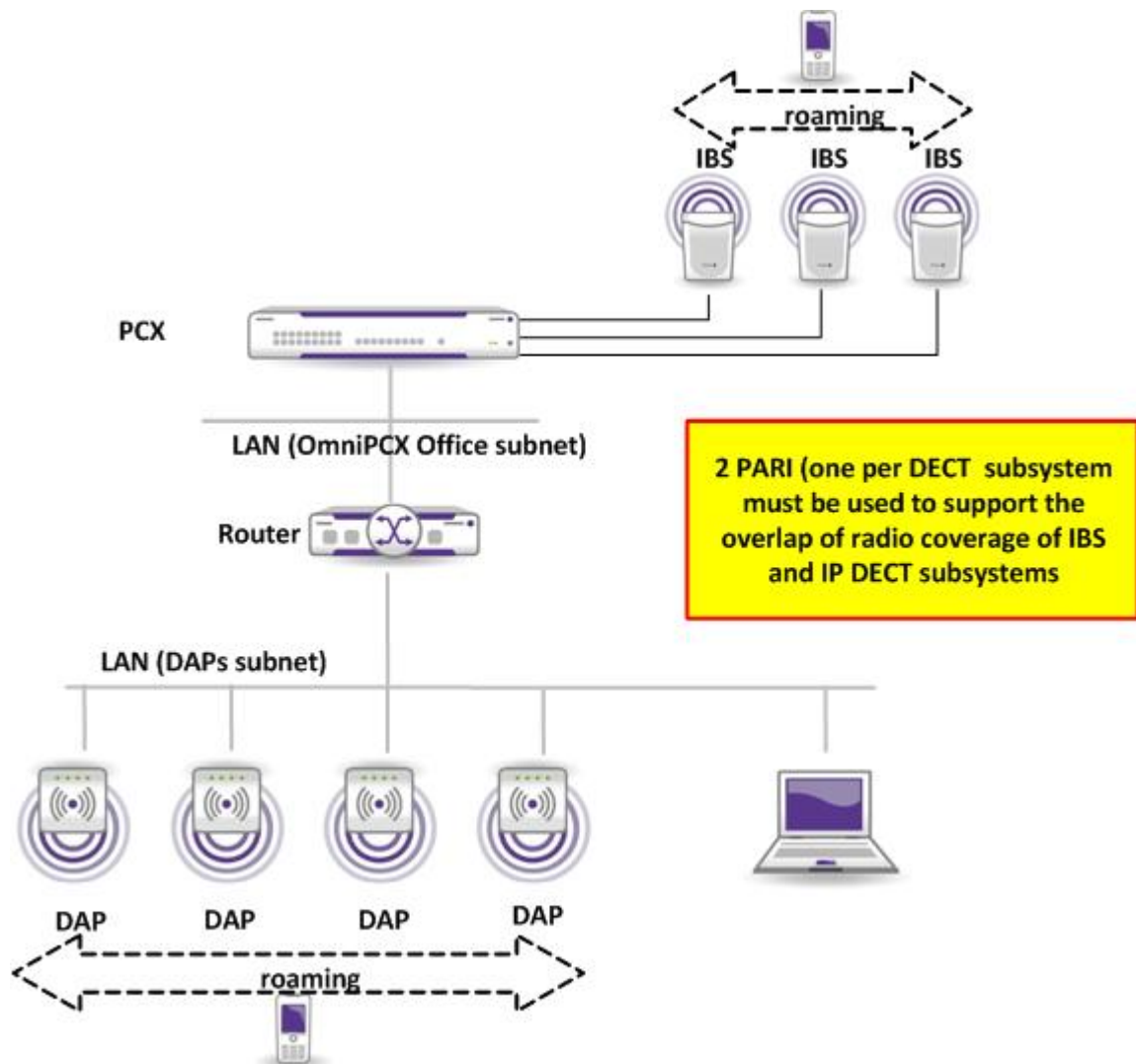
Reminder:

For IP DECT subsystem, deployment rules are defined: [IP network deployment rules](#) on page 40

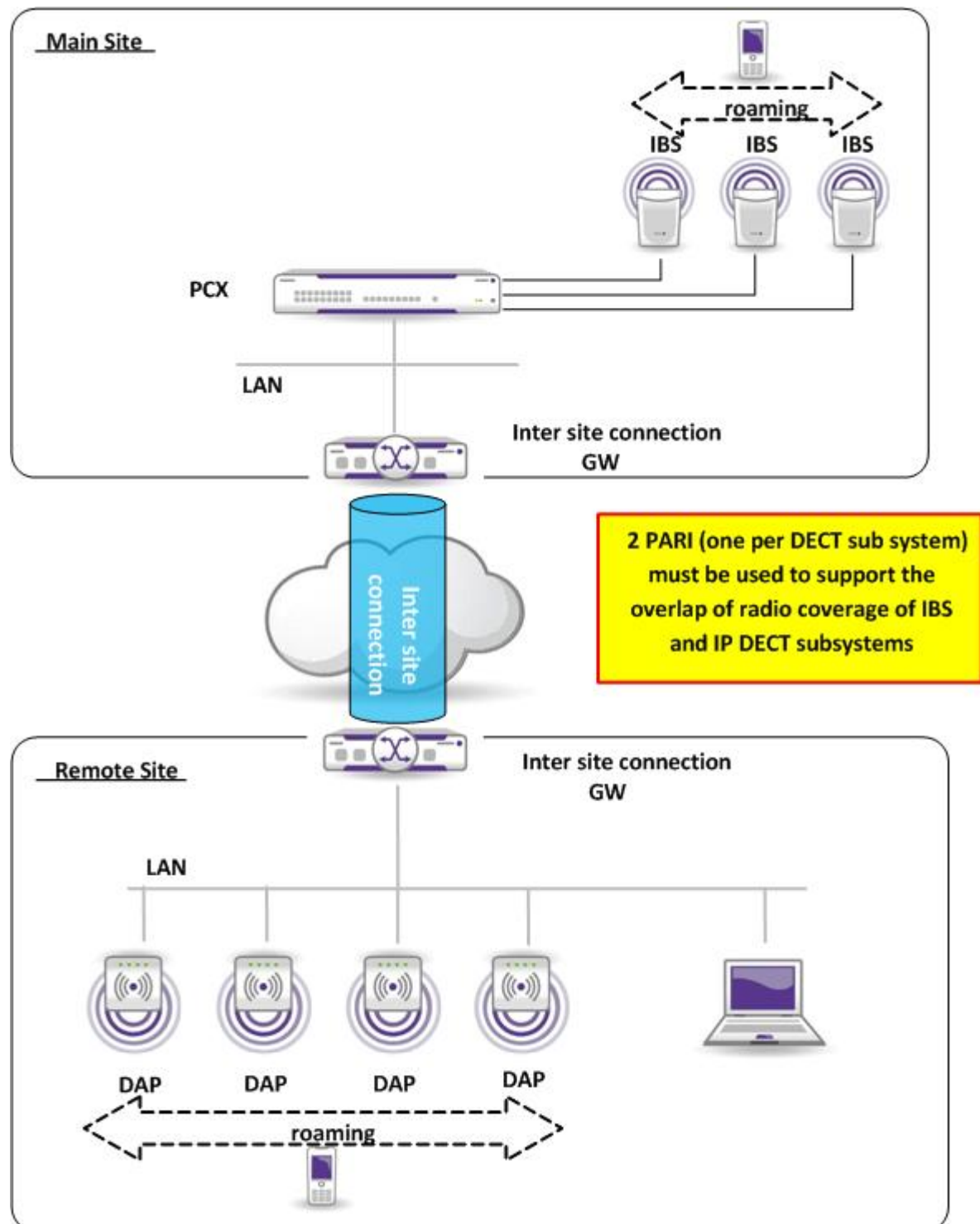
3.2.4.1 OXO Connect and DAPs in the same subnet



3.2.4.2 Routed network



3.2.4.3 Remote site



3.3 Configuration procedure

3.3.1 Overview

This chapter describes the configuration operations to perform on the OXO Connect to use IP-DECT solution.

The basic operations to configure the IP-DECT solution are:

- [Deploying the IP-DECT solution](#) on page 52:
 - [Configuring DHCP server](#) on page 52
 - [Running DAP configurator](#) on page 52
 - [Plugging DAPs](#) on page 53
- [Managing IP-DECT handsets](#) on page 54:
 - [Declaring IP-DECT handsets](#) on page 54
 - [Removing IP-DECT handsets](#) on page 54
 - [Replacing IP-DECT handsets](#) on page 54
 - [Modifying IP-DECT handsets phone number](#) on page 55
- [Managing DAPs](#) on page 56:
 - [Removing a DAP](#) on page 56
 - [Replacing a DAP](#) on page 56
 - [Synchronizing DAPs](#) on page 56
 - [Removing all subscriptions in DAPs](#) on page 57
 - [Modifying DAP web administration page password](#) on page 57

3.3.2 Deploying the IP-DECT solution

3.3.2.1 Configuring DHCP server

DAPs use, by default, the embedded DHCP server of the OXO Connect to get their IP parameters. For more information, please refer to [14] DHCP configuration.

Note:

As the DAP does not give any preference to the DHCP server of the OXO Connect, if there is another DHCP server in the subnetwork, the DAP may retrieve invalid IP network settings from this other server. If this takes place, the DAPs are not able to retrieve their configuration file and thus reboot continuously. This is why ALE International strongly advised against having several DHCP servers on the subnetwork of the OXO Connect.

If an external DHCP server is used, it must be configured to serve both **ALU IP phones** and DAPs:

- The next-server option has to be set to the IP address of the OXO Connect
- The DAP vendor class identifier is D(ECT)AP 49.

Note:

If the DAPs are in a voice VLAN, the voice VLAN ID has to be set at port level in the network equipment configuration (switch).

3.3.2.2 Running DAP configurator

DAPs require a configuration file to be downloaded at each start-up/reboot via TFTP protocol. This configuration file is generic for all the DAPs and generated by the DAP Configurator.

Note:

At installation, a first file is created by OXO Connect with a GK (Gatekeeper) section containing the IP address of the PBX and the SIP port used. These parameters are updated by the OXO Connect if changed in the system.

To run DAP configurator:

- In OMC, select **DECT > IP Dect (old) > DAP configurator**
- Select the **Misc. Settings** tab.
- In the **PARI** field, enter the **PARI** of the system.

Note:

The PARI assigned to your IP-DECT system can be retrieved from the eBay web site via the following URL:

https://ebuy.businesspartner.alcatel-lucent.com/CodePari/Install_List.aspx

Note:

In case of dual DECT topology, It is mandatory that this value is different from the PARI of the IBS network.

- Click **Save & Exit**

When the DAP Configurator is running, the configuration file is downloaded from the OXO Connect to the PC running the OMC. When the DAP Configurator is closed with the **Save & Exit** button, the modifications are saved in the configuration file and the file is uploaded in OXO Connect. A reboot request is then sent to the DAPs so that they can retrieve the new configuration file.

Note:

*Each time the DAP Configurator is closed with the **Save & Exit** button, a reboot of the DAPs will be requested, even if nothing has been modified. To avoid the reboot of the DAPs, the **Cancel & Exit** button has to be used instead.*

Note:

DAP Configurator allows the modification of the PARI of the system. This modification removes all the DECT handsets subscribed on the DAPs.

3.3.2.3 Plugging DAPs

Once connected to the LAN, the DAP get its IP parameters from the DHCP server.

In a second step, the DAP makes a TFTP request to OXO Connect to download its configuration file. Each DAP gets an RPN (from 0 to 15, in order of appearance) and the one with the lowest RPN has a specific role in the IP-DECT solution: Master DAP. By default, the master DAP is the DAP plugged first. RPNs can be changed afterwards via the DAP Configurator.

The split RPN concept is supported. For example, when the connection between the main site and remote site fails, some DAPs can no longer handle handset registration, and handsets may be out of service on both sites. The Split RPN concept allows to secure handset registration on the main site.

All DAPs below this split RPN are considered to be located in the main site and the DAPs greater or equal to the split RPN are associated to the remote site. In this configuration, all registrations are allocated to DAPs associated to the main site. DAPs associated to the remote site cannot handle registrations. This means that the DAPs associated to the main site must be enough to host all registrations (maximum of twenty-five handset registrations per DAP).

By default, the split RPN is disabled and there is only one location for DAPs.

To manage RPNs:

- In OMC, select **DECT > IP Dect (old) > DAP configurator**
- Click the **Network Settings** button.
- Enter MAC addresses in the corresponding RPN lines.
- Click **Save & Exit**

Note:

*The **Network Settings** tab of the DAP Configurator has to be used only to modify the RPN of DAP that already appeared in the system. It cannot be used to modify a MAC address of an existing DAP in case of DAP replacement.*

Note:

The Master DAP has a special role in the IP-DECT solution and it must be located in a central position of the DAP topology.

3.3.3 Managing IP-DECT handsets

3.3.3.1 Declaring IP-DECT handsets

Important:

In case a DAP has been unplugged just before declaring IP-DECT handsets, make sure to wait two minutes before proceeding to the registration else the GAP registration is rejected.

To declare an IP-DECT handset:

1. In the OMC:

- a. Select **Users/Base stations List**
- b. Click the **Add** button
- c. Select the **4080/8340 IP DECT** radio button
- d. Select a directory number
- e. Confirm your entries.
- f. Click the **GAP Reg.** button

If the **GAP registration selection** pop-up opens, select the **4080/8340 IP DECT** radio button and click **OK**.

The **IP-DECT Registration** window is displayed.

- g. Select the IP-DECT handset and click the **Register** button.

The PARK code, a PIN code, and a registration status is displayed.

2. On the mobile:

- a. Launch the registration procedure on the handset (refer to the accompanying documentation).
- b. Enter the PIN code

Note:

The DECT registration period is limited to 2 minutes for security reasons.

Once the set is registered, the terminal type is updated and the status is set to **Registered**.

3.3.3.2 Removing IP-DECT handsets

To remove an IP-DECT handset:

1. In OMC, select **Users/Base stations List**
2. From the list, select the handset to remove
3. Click the **Delete** button

Note:

Delete sends a request to remove the handset data from the DAP and remove all the data in the PBX:

- If the handset is connected to the DAP, the registration is also removed in the handset.
- If the handset is out of coverage or turned off, the registration remains in the handset and has to be removed manually.
- If the DAP is not reachable when the handset is deleted in OMC. A warning message is displayed in OMC, the registration remains in the DAP and has to be removed (see [Synchronizing DAPs](#) on page 56).

3.3.3.3 Replacing IP-DECT handsets

To replace an IP-DECT handset with the same type of handset:

1. In OMC:

- a. Select **Users/Base stations List**
- b. From the list, select the handset to replace
- c. Click the **GAP Reg.** button

The **IP-DECT Registration** window is displayed.

- d. Select the IP-DECT handset and click the **Unregister** button.
- e. Click the **GAP Reg.** button
- f. Select the IP-DECT handset and click the **Register** button.

The PARK code, a PIN code, and a registration status is displayed.

2. On the mobile:

- a. Launch the registration procedure on the handset (refer to the accompanying documentation).
- b. Enter the PIN code

Note:

The DECT registration period is limited to 2 minutes for security reasons.

To replace an IP-DECT handset with a different type of handset:

- The first handset has to be deleted in OMC and a new one created (see [Declaring IP-DECT handsets](#) on page 54)

3.3.3.4 Modifying IP-DECT handsets phone number

To modify an IP-DECT handset phone number:

1. In OMC:

- a. Select **Users/Base stations List**
- b. From the list, select the handset
- c. Click the **GAP Reg.** button

The **IP-DECT Registration** window is displayed.

- d. Select the IP-DECT handset and click the **Unregister** button.
- e. Click the **Return** button.
- f. In the **Users/Base stations List** window, enter the new phone number and click the **Modify** button.
- g. Click the **GAP Reg.** button

The **IP-DECT Registration** window is displayed.

- h. Select the IP-DECT handset and click the **Register** button.

The PARK code, a PIN code, and a registration status is displayed.

2. On the mobile:

- a. Launch the registration procedure on the handset (refer to the accompanying documentation).
- b. Enter the PIN code

Note:

The DECT registration period is limited to 2 minutes for security reasons.

Note:

The modification of phone numbers can only be done individually in the list of subscribers. Any global modification by changing the numbering plan are not taken into account. IP-DECT handsets must be deleted before numbering plan modification and re-created afterwards, as for any SIP phone.

3.3.4 Managing DAPs

3.3.4.1 Removing a DAP

To remove a DAP:

1. Unplug the DAP

Note:

The time for detecting the unplugged DAP is 2 minutes.

IP-DECT handsets registration cannot be done during this time.

2. In OMC, select **Users/Base stations List**
3. From the list, select the DAP to remove
4. Click the **Delete** button

Note:

*The **dapcfg.txt** file is then updated and the remaining DAPs restarted. If the removed DAP is the master DAP, the remaining DAP with the lowest RPN will become the new master DAP.*

3.3.4.2 Replacing a DAP

To replace a DAP:

1. Unplug the DAP

Note:

The time for detecting the unplugged DAP is 2 minutes.

IP-DECT handsets registration cannot be done during this time.

2. In OMC, select **Users/Base stations List**
3. From the list, select the DAP to remove
4. Click the **Detail** button
5. Click the **IP/SIP** button.
6. Enter the MAC address of the new DAP in the **MAC address** field.
7. Confirm your entry.
8. Plug the new DAP.

Note:

The list of registered handsets is then retrieved from the other DAPs.

Note:

*When a DAP is replaced by a 8340-C Smart IP-DECT in the system, check that G.729 mode in DAP configurator is **G729 not supported** (The 8340-C Smart IP-DECT does not support G.729). In this case, all DAPs (with or without G.729 support) in the system work using G.711 codec.*

3.3.4.3 Synchronizing DAPs

The DECT handsets are registered in both the OXO Connect and the DAP. If the DAP is unavailable, some handsets can remain in the DAP after being removed from the OXO Connect.

To synchronize OXO Connect and the DAPs:

1. In OMC, select **DECT > IP Dect (old) > IP DECT commands**
2. Select **Synchronize all**
3. Confirm your entry.

Note:

This command keeps all IP-DECT handsets that are in the Subscriber list of OMC. All other handsets in the DAPs are removed.

3.3.4.4 Removing all subscriptions in DAPs

To remove all subscriptions in DAPs:

1. In OMC, select **DECT > IP Dect (old) > IP DECT commands**
2. Select **Terminate all**
3. Confirm your entry.

3.3.4.5 Modifying DAP web administration page password

The DAP has a Web administration page which needs a password for access. For IP-DECT DAP administrator password there is no default password and the password can only be reset.

To modify this password:

1. In OMC, select **System miscellaneous > Passwords > Device Administrator Password**
2. Click the **Reset** button for **IP-DECT DAP Web Administrator**
3. Confirm the reset action.
4. Enter the current OMC session password to activate the reset.

3.4 Maintenance

3.4.1 Cold reset

The data stored locally on the DAPs (list of registered handsets) are not deleted by a cold restart of the OXO Connect. A warning message is displayed.

To remove the registered handsets, a specific cold restart of the DAPs have to be requested via OMC, refer to [Removing all subscriptions in DAPs](#) on page 57.

3.4.2 Save/restore

The save mechanism includes the DAPs configuration file (dapcfg.txt).

When restoring a saved configuration, the saved dapcfg.txt file overwrites the one on the OXO Connect.

The OXO Connect has to check the consistency between the restored configuration file (DAP binary version in the dapcfg.txt) and the DAP binary version available on OXO Connect (dap_binary.txt file included in the OXO Connect delivery).

After restore, the OXO Connect requests a reboot of all the DAPs so they can get their restored configuration file. This reboot is requested after the OXO Connect restart.

The list of handsets are stored both on OXO Connect and DAP side.

The OMC restore does not restore any handset in the DAP. It only restores the configuration file. Any missing handset has to be re-registered via OMC.

An OMC restore restores the handsets on the OXO Connect only. As the DAPs keep their handsets list locally (if no cold reset of the DAPs is requested), the list of handsets could be different between OXO Connect and the DAPs (case of handsets removal/addition after the OMC save).

A synchronization command should be requested in that case, refer to [Synchronizing DAPs](#) on page 56.

In case of restore requested by a swap with data saving, the list of handsets in the DAP remains consistent with the one in OXO Connect.

3.4.3 Software upgrade

DAPs binary is part of the OXO Connect software package and downloaded to the PBX via the OMC software download tool.

The version of the binary is included in the configuration file that the DAPs get at each restart. If the binary hosted on OXO Connect is different from the running one, DAPs upgrade/downgrade to that version.

So after each OXO Connect reboot, DAPs are automatically reset so they can manage an upgrade/downgrade if necessary.

DECT handsets firmware are upgraded individually via a specific tool and a wired connection.

3.4.4 Incidents

If a DAP is no more reachable, the handsets that have subscribed on that DAP are no more accessible. After a period of ten minutes, the other DAPs discovers that the DAP is down and manage an automatic distribution of the concerned handsets. This automatic distribution is not done if more than one DAP are not reachable at the same time. In that situation, a network issue is probably the cause of the DAPs disappearance (example: reboot of the switch where the DAPs are connected). If a DAP becomes reachable again after the automatic distribution of its handsets, this DAP does not retrieve its handsets.

When the master DAP is no more reachable, the DAP with the lowest RPN becomes the new master DAP.

The handsets that cannot be distributed to the remaining DAPs are out of service (SIP registration timeout).

As long as a DAP is not reachable, handset registration/deregistration is not possible. The DAP issue can be either a network issue or a DAP failure. In that situation, the issue has to be solved in order to allow again handset registration/deregistration. If the DAP failure is hardware, it must be replaced or removed.

4.1 xBS overview

The OXO Connect offers a wireless telephony solution with xBS deployed on the company IP network (LAN). xBSs combine DECT and IP technologies:

- xBSs are connected to the LAN and use the UA over UDP/IP protocol to communicate with the OXO Connect.
- DECT handsets connect to the xBSs via radio links complying with the DECT protocol.

The 8378 DECT IP-xBS solution (xBS solution in the rest of the document) is made up of xBSs synchronized together on the air (DECT synchronization). xBSs generally support the same mobility features as legacy DECT system.

An xBS solution can be deployed along with the IBS DECT solution, on the same OXO Connect. DECT handsets can roam between the xBSs and IBSs. Handover between the xBS and IBS DECT solutions is not possible.

An xBS solution cannot be deployed along with an IP-DECT system on the same PBX.

The xBS solution does not require any license.

The following figure provides an example of xBS solution:

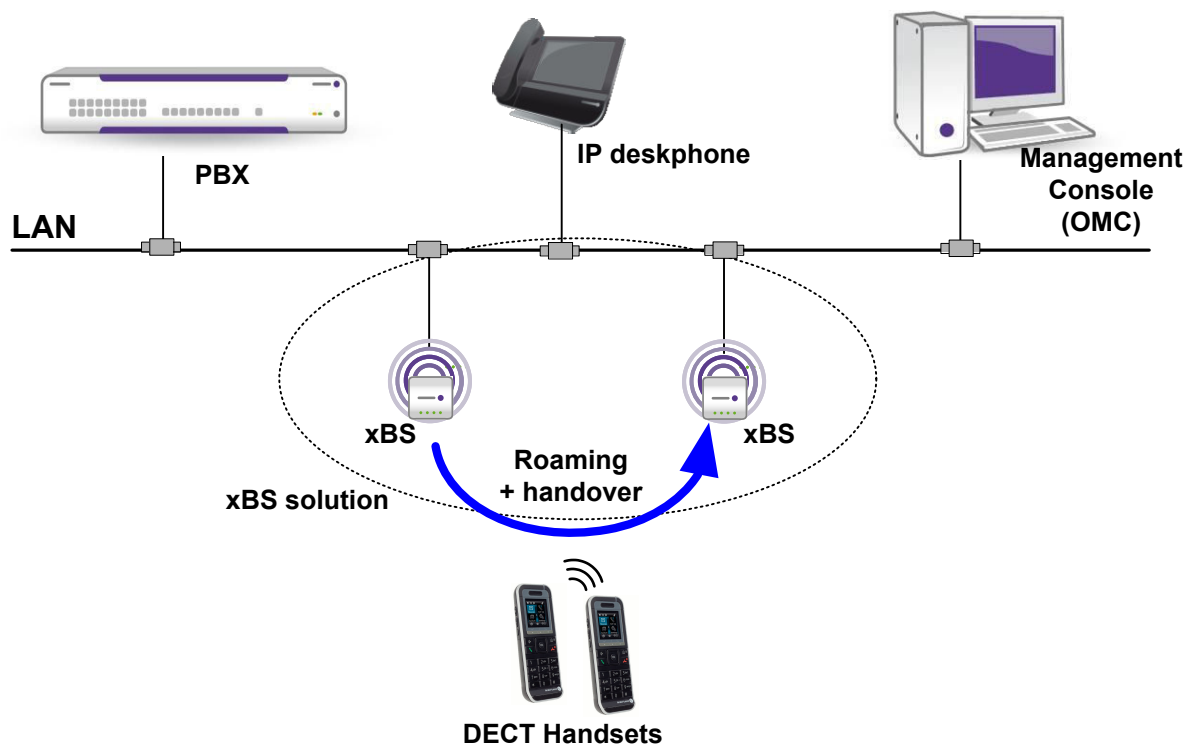


Figure 4.1: xBS solution view example

4.2 xBS components

The xBS solution relies on:

- **xBSs** (identified as 8378 DECT IP-xBS), connected to the IP network (LAN) operating as entry points for DECT handsets. xBSs handle mobility features (roaming and handover) and communications to/from DECT handsets.

Once connected to the LAN, xBSs start up and connect to the OXO Connect at initialization. xBSs use the UA over UDP protocol to communicate with the OXO Connect.

xBSs retrieve their IP configuration and binary from the PBX. Base station initialization is similar to IP NOE phone initialization. It can be static or dynamic (default option). In static, IP configuration is performed on xBSs using their web management interface (HTTP connection).

xBSs support:

- Twelve DECT radio slots, with eleven radio slots reserved for communications. xBSs can manage up to eleven simultaneous calls (nine simultaneous calls when two slots are reserved for the alarm feature). One slot is used for clock synchronization
- Ethernet connectivity 10/100 baseT (IEEE802.3) and PoE
- IPv4 addressing
- IP unicast routing (not IP multicast)
- G711 and G729A codecs
- VLAN Tagging on Layer 2 (IEEE 802.1q)
- Quality of Services (QoS) on layers 2 and 3 (QoS value is sent to the xBS at initialization)
- NTP for clock synchronization and Daylight Saving Time (DST) (NTP and DST values are sent to xBS at initialization)
- **DECT handsets**, connected to the xBSs via radio links complying with the DECT protocol. At initialization, DECT handsets register to the PBX through xBSs, and communicate through the xBS solution. In an xBS/IBS DECT mixed configuration, DECT handset can register either through an xBS or an IBS.

The xBS solution supports:

- 8212 DECT handsets in GAP mode
 - 8232 DECT, 8242 DECT, 8262 DECT, and 8262 DECT EX in A-GAP mode
 - **The OXO Connect**, which manages:
 - Settings of the xBS solution, including base station and DECT handset configuration (via the OMC application)
 - Registration of xBSs and DECT handsets. For xBS registration, the PBX provides:
 - A DHCP server to provide xBSs with their network configuration (IP address/TFTP server IP address) when they initialize in dynamic mode (default mode)
- Note:*
An external DHCP server can also be used instead of the internal PBX DHCP server.
- A TFTP server to provide xBS with their configuration file and binary
 - Connection with xBSs for signaling and media
 - Supervision of xBSs and DECT handsets (maintenance purposes)
 - Supervision of xBSs for "keep-alive" dialog

4.3 xBS synchronization and mobility

4.3.1 Site

A site is a group of xBSs located in the same geographical location where handover is possible (see: [Handover](#) on page 64). By default, one site is configured for the entire PBX, and all xBSs belong to this site, which is identified as site 1 in PBX configuration.

Up to twenty sites can be configured in PBX. This organization per site allows to minimize the data traffic between xBSs, especially in case of xBSs located on different offices. For example, a company can include a headquarter and distant branch offices, each represented by a site. Between sites, handover is not possible, only roaming is possible.

xBSs can be moved from the default site to another site in PBX configuration (see: [Declaring the xBS on PBX](#) on page 88).

4.3.2 Sync Cluster

A SYNC Cluster is a set of xBSs which are synchronized (time aligned) together at DECT radio interface (see: [Clock synchronization](#) on page 61). Two xBSs, that do not belong to a same Sync Cluster, cannot have the same clock synchronization.

All xBSs belonging to the same Sync Cluster must synchronize together. An xBS may belong to several Sync Clusters in a same SITE. If an xBS belongs to two different Sync Clusters, the two Sync Clusters are chained together (time synchronized). A chain of Sync Clusters allows to force the way in which xBSs are synchronized (time aligned) together.

The PBX can include up to 8 Sync Clusters per site. By default, all xBSs belong to the same Sync Cluster, which is identified as Sync Cluster 1 in PBX configuration. Each xBS can belong up to 8 Sync Clusters: Sync Cluster 1 to Sync Cluster 8 in PBX configuration (see: [Configuring Sync Clusters and clock synchronization in a site](#) on page 90).

4.3.3 Data synchronization

Data synchronization in the xBS solution is ensured by an xBS acting as a data synchronization source (identified as `Data Sync Primary`). This `Data Sync Primary` is an xBS in charge of synchronizing data between all the xBSs belonging to the same site (including the time synchronization tree). Its role is to centralize all data and to copy them to all xBSs attached to it.

For each site defined in the PBX, the first xBS detected by the PBX acts as the `Data Sync Primary` for all others belonging to the same site. Its IP address is transmitted by the PBX to all other xBSs at initialization. There is one `Data Sync Primary` per site.

Handover is only possible between the xBSs connected to the same `Data Sync Primary`. The xBSs must also share the same clock synchronization.

xBSs are supervised by the PBX (keep-alive dialog). If the `Data Sync Primary` fails, the PBX selects another xBS as `Data Sync Primary`, and notifies all other xBSs of this change. The failure detection by the PBX may take two minutes.

After reboot, each xBS communicates with the new `Data Sync Primary`.

4.3.4 Clock synchronization

4.3.4.1 Automatic clock synchronization

xBSs require a stable and accurate clock synchronization to operate correctly and provide handover (see: [Handover](#) on page 64). Clock synchronization is transmitted on the air.

A clock synchronization is performed between the xBSs belonging to a same Sync Cluster. By default, a clock synchronization tree is automatically built with the information provided by each xBS belonging to the same Sync Cluster. The synchronization master is the xBS root of the synchronization tree (identified as `Sync Master` in the rest of the document). This xBS transmits a signal on the air to all other xBSs located in its radio coverage area. In turn, these xBSs become the synchronization source for the located in their radio coverage area. Only the xBSs that can receive a synchronization signal become synchronized. If the current `Sync Master` fails, a new xBS is automatically selected as `Sync Master`.

xBSs of different clusters can be synchronized if there is an xBS belonging to the two clusters (see: [Example of clock synchronization \(one site, several Sync Clusters and one Sync Master\)](#) on page 63).

If some xBSs cannot be attached to the main synchronization tree (no radio signal between xBSs), additional secondary synchronization trees are automatically created. These secondary synchronization trees are independent and have their own `Sync Master`. This case is not recommended when the different synchronization trees have overlapping radio coverage: additional xBSs may be needed to link the different synchronization trees.

The creation of the clock synchronization tree does not require any configuration on the PBX. The criteria used to build the clock synchronization tree are:

- Link quality/Received Signal Strength Indications (RSSI)
- Optimization of the number of hops to the root of the clock synchronization tree (that is the `Sync Master`)

4.3.4.2 Manual clock synchronization

Automatic configuration of clock synchronization is preferred, but in specific cases, clock synchronization may be configured manually for each site defined in the PBX by selecting:

- The xBS acting as master of the clock synchronization for all xBSs belonging to the site (identified as **Master** in PBX configuration).

Only one synchronization master is defined per site, which means that there is only one clock synchronization tree in the site.

- The xBS acting as second (backup) master of the clock synchronization (identified as **Backup Master** in PBX configuration)
- The xBS acting as synchronization source for a dedicated xBS of the site (identified as **Sync Source** in PBX configuration).

An xBS running as `Sync Master` can act as **Sync Source** for another xBS. It is not possible to force the **Sync Source** of an xBS running as `Sync Master`.

When clock synchronization was manually configured and both `Master` and `Backup Master` fail, the xBSs of the site are no longer operational, as there is no more clock synchronization. A new `Master` must be defined in PBX configuration.

The manual configuration of the clock synchronization is performed from the **IP DECT Clock Synchronization** menu in PBX configuration (see: [Configuring Sync Clusters and clock synchronization in a site](#) on page 90).

4.3.4.3 Example of clock synchronization (one site, one Sync Cluster and one Sync Master with automatic synchronization)

The following example of clock synchronization relies on one site, with one Sync Cluster including ten xBSs (XBS-1 to XBS-10), and XBS-1 acting as `Sync Master`. All xBSs have the same clock synchronization.

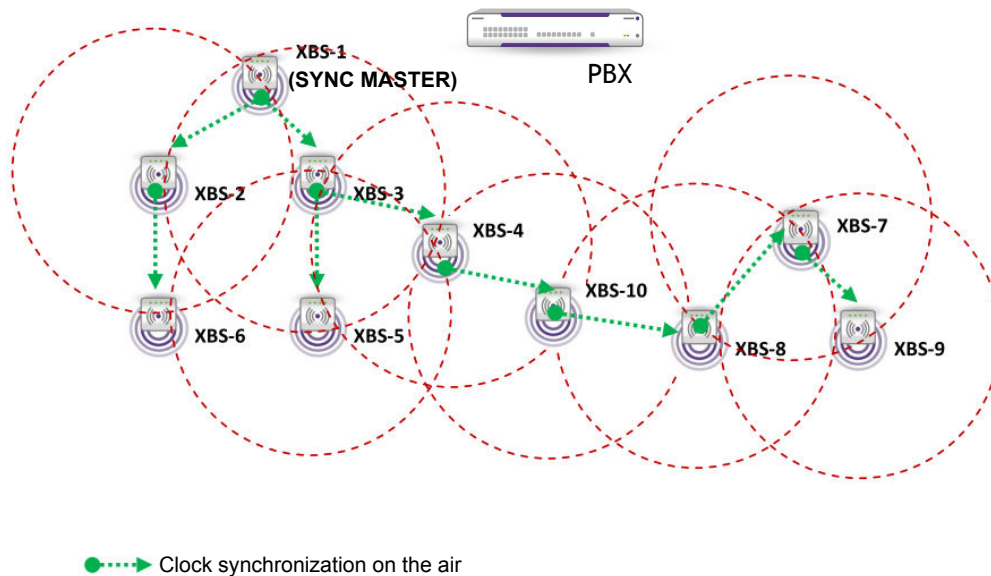


Figure 4.2: Example of clock synchronization (one site, one Sync Cluster and one Sync Master)

In this configuration, roaming and handover are possible in the Sync Cluster.

The Sync Master may change in case of modification of the radio coverage or failure. In this case, the xBS solution automatically creates a new clock synchronization tree, including a new Sync Master.

4.3.4.4 Example of clock synchronization (one site, several Sync Clusters and one Sync Master)

The following example describes the clock synchronization in a building with three floors and an elevator shaft.

There is one site including four SYNC Clusters:

- XBS-1 to XBS-6 belong to Sync Cluster 1
- XBS-8 to XBS-13 belong to Sync Cluster 2
- XBS-15 to XBS-20 belong to Sync Cluster 3
- XBS-5, XBS-7, XBS-12, XBS-14 and XBS-19 belong to Sync Cluster 4
- XBS-5 belongs to Sync Clusters 1 and 4
- XBS-12 belongs to Sync Clusters 2 and 4
- XBS-19 belongs to Sync Clusters 3 and 4

Alls have the same clock synchronization provided by XBS-12 acting as synchronization source (Sync Master). This entails that the radio signal between xBSs of a same Sync Cluster is strong and stable while the radio signal between xBSs of different Sync Clusters is not stable. Thus xBSs are grouped in Sync Clusters in order to force synchronization between xBSs with stable signal.

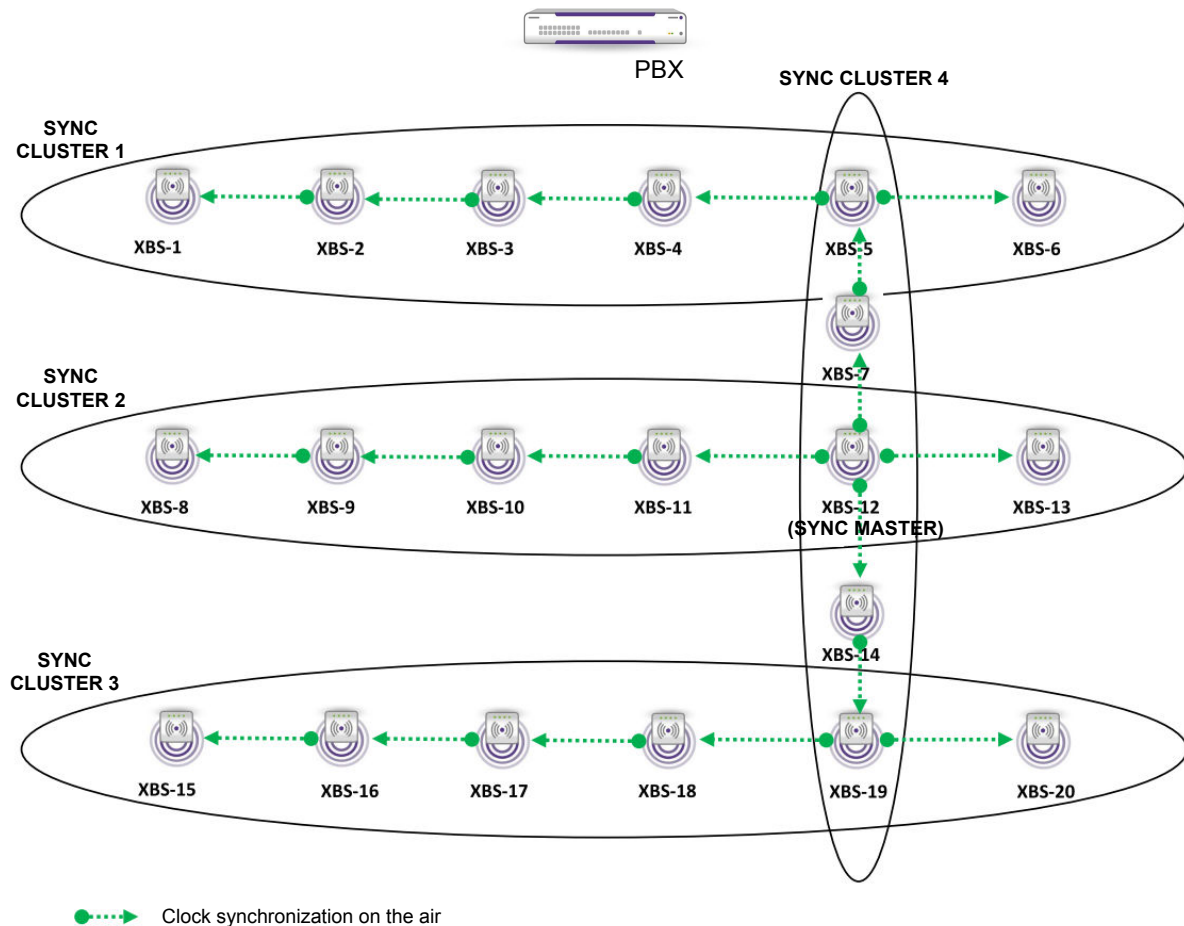


Figure 4.3: Example of xBS configuration with one site, several Sync Clusters and one synchronization source

Roaming and handover are possible in this configuration.

4.3.5 xBS mobility

4.3.5.1 Roaming

The roaming feature allows DECT handset users to make or receive calls from any location in the xBS solution coverage area.

Roaming is possible between all xBSs whatever the site and Sync Cluster to which they belong.

4.3.5.2 Handover

The handover feature allows DECT handset users to move from one xBS to another one during a call. Transfer to the other xBS does not affect users (seamless handover): there is no interruption of the call.

Handover can take place between two xBSs provided that:

- They are synchronized (time aligned) (see: [Clock synchronization](#) on page 61).
- They have the same Data Sync Primary (see: [Data synchronization](#) on page 61)

4.3.5.2.1 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 synchronize 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 recognize 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 synchronized with the system, the handset decides on the most appropriate channel for a call. It chooses the least disrupted of the free channels.

4.3.5.2.2 Inter- and intra-cell handover procedures

The radio coverage of a base station forms a "cell".

Intercell handovers 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 handover is performed on the same base station towards a higher quality channel.

4.3.5.3 Call recovery

When a communication with a DECT handset is interrupted due to a problem (for example: out of service), the xBS solution offers the call recovery feature, allowing the call to be automatically resumed.

Call recovery is possible for DECT handsets connected to an xBS.

4.4 xBS signaling and voice flows

A call from a DECT handset requires a signaling and media connection between the PBX and the initial xBS to which the DECT handset is connected (XBS-1 in step 1 below). The xBS system manages all signaling and media redirection between its xBS (connection handover). The media flow (RTP) is direct between an IP phone (or trunk) and an xBS.

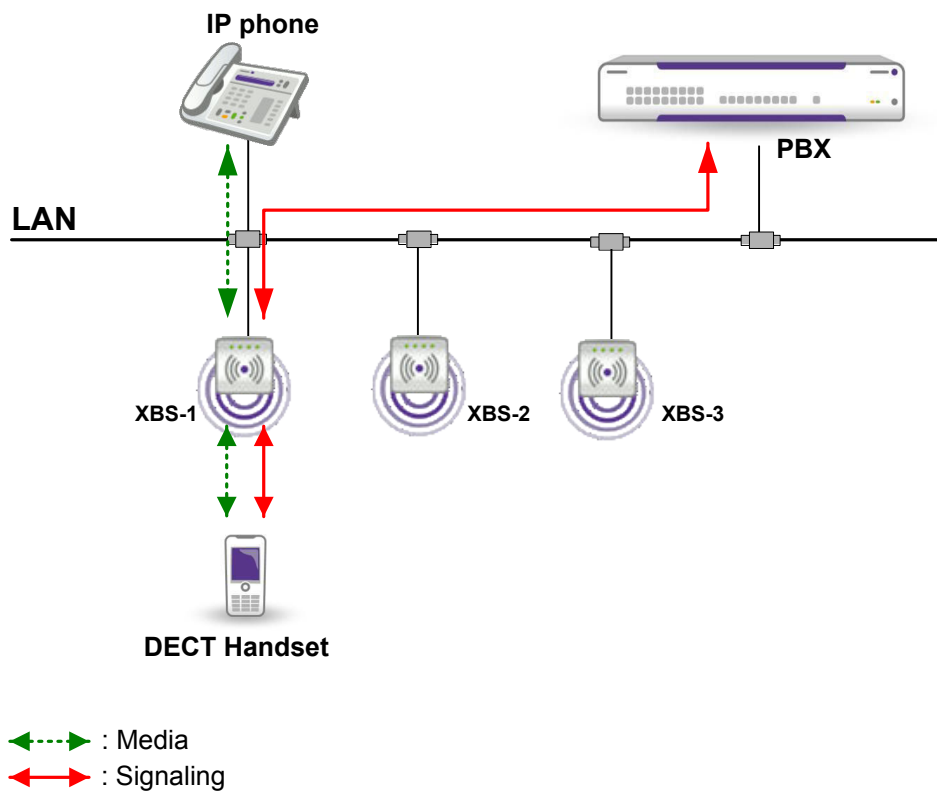


Figure 4.4: Step 1

In case of connection handover, the initial media connection is maintained with the distant IP phone. Media is rerouted between the xBSs (XBS-2 in step 2, and XBS-3 in step 3 below). Signaling and media commands are always sent by the PBX to the initial xBS.

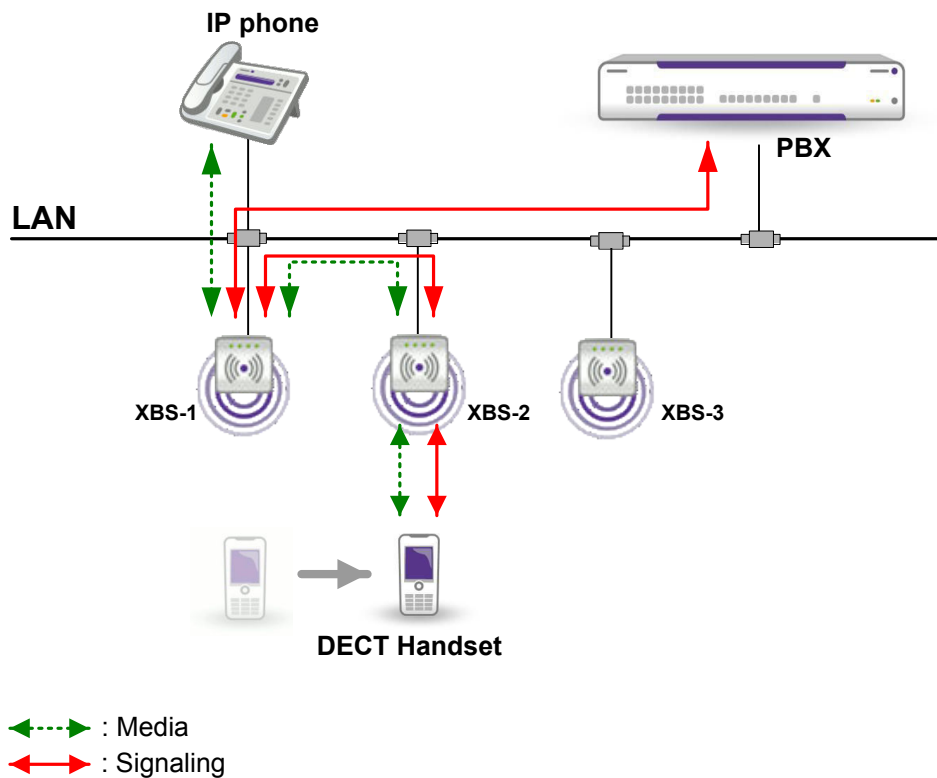


Figure 4.5: Step 2

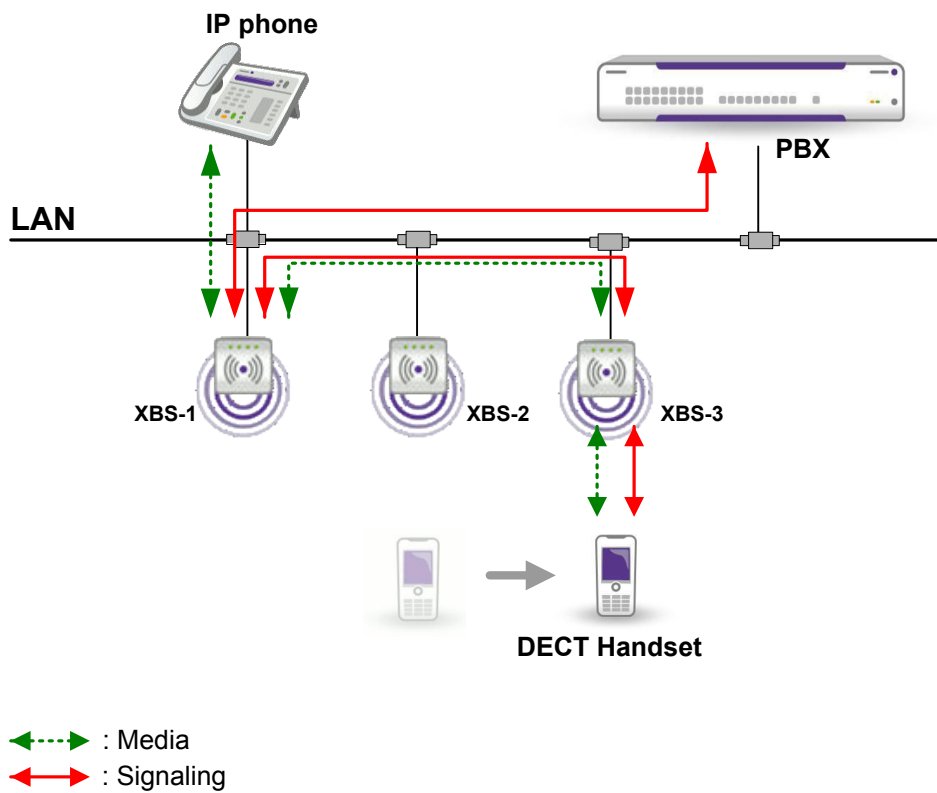


Figure 4.6: Step 3

The connection established between the PBX and xBS does not support neither 802.1x authentication nor encryption.

4.5 xBS and IBS DECT

xBS and IBS DECT can be deployed on the same PBX node.

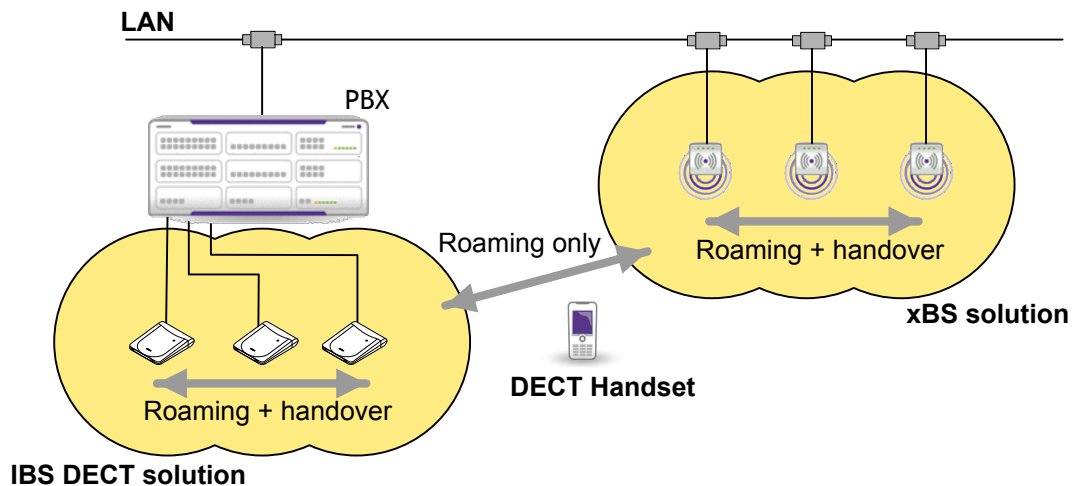


Figure 4.7: Example of mobility with xBS and IBS DECT solutions

DECT handsets can roam between xBS and IBS DECT. According to their location, DECT handsets can register to the PBX, either through the xBS or IBS DECT solution (only one subscriber per DECT handset is defined on PBX).

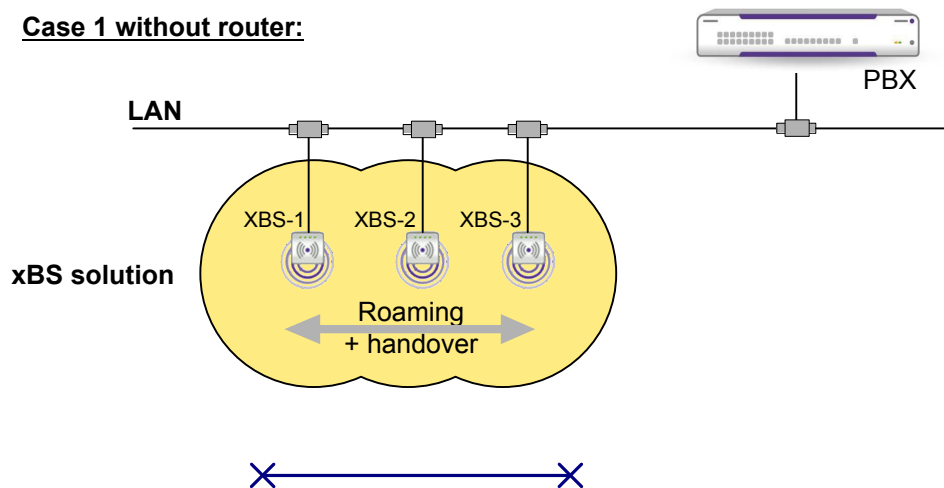
It is recommended to deploy xBS and IBS DECT solutions in two different locations: radio coverage of the two systems must not overlap (no clock synchronization). The xBS Sync Cluster is never clock synchronized with IBS DECT: handover is not possible between the two solutions. In case of overlapping, a DECT handset can be in the radio coverage of an IBS and always in communication with an xBS.

Call recovery is possible between xBS and IBS DECT. In case of connection failure on xBS solution, the call recovery can be performed on the IBS DECT solution, and vice-versa.

4.6 xBS topologies

4.6.1 xBS topology with one site and one Sync Cluster

Case 1 without router:



Case 2 with router:

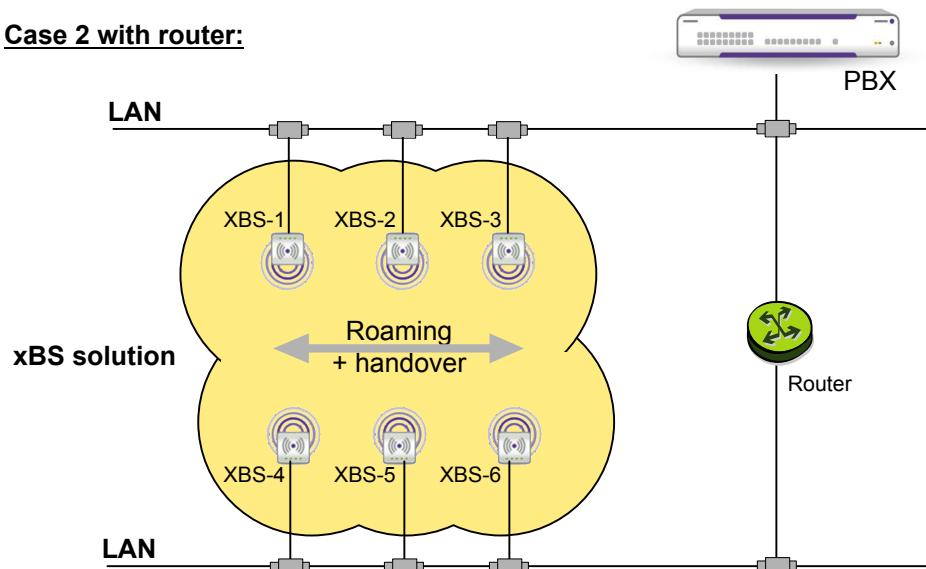


Figure 4.8: Examples of xBS topologies with one site and one Sync Cluster

In the two configurations (with and without router):

- All xBSs within the Sync Cluster have the same clock synchronization, provided by an xBS acting as **Sync Master**
- Roaming and handover are possible within the Sync Cluster

4.6.2 xBS topology with one site and multiple Sync Clusters

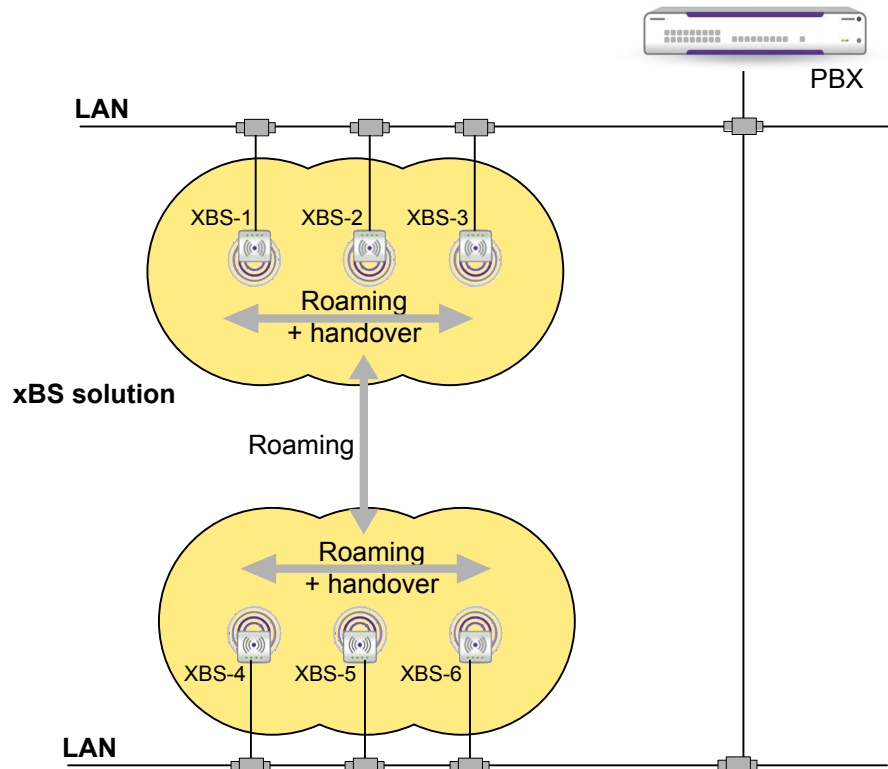


Figure 4.9: Example of xBS topology with one site and two Sync Clusters

The XBS-1, XBS-2 and XBS-3 belong to Sync Cluster 1.

The XBS-4, XBS-5, and XBS-6 belong to Sync Cluster 2.

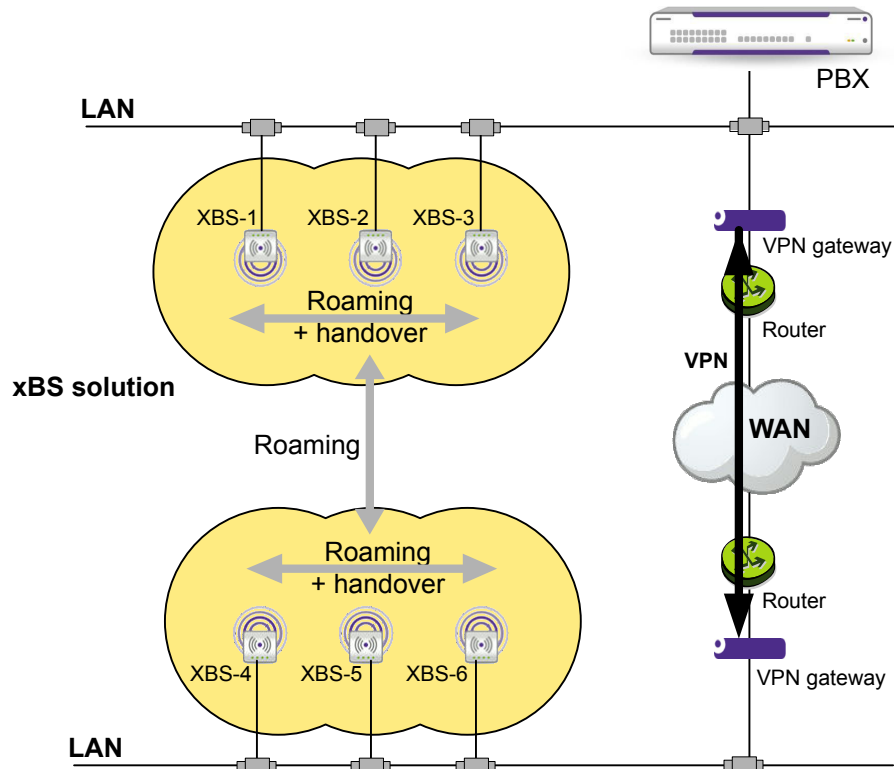
In this configuration:

- Each Sync Cluster has its own **Sync Master**
- There is no clock synchronization between Sync Cluster 1 and Sync Cluster 2
- Roaming is possible between the two Sync Clusters
- Handover is only possible within each Sync Cluster

It is not necessary to define two Sync Clusters if the radio coverages of the two groups of base stations do not overlap. All base stations can be grouped in the same Sync Cluster. In this case, the xBS solution automatically defines two independent clock synchronization trees: one for XBS-1, XBS-2 and XBS-3, and another one for XBS-4, XBS-5 and XBS-6. Handover is not possible between the two groups of base stations.

The radio coverages of the two groups of base stations may overlap, but not enough to provide a stable clock synchronization. In this case, the two groups can be separated in several Sync Clusters to prevent any risk of unwanted synchronization between those groups.

4.6.3 xBS topology with multiple sites



The remote site is connected to the main site with a LAN to LAN VPN connection through the IP network.

xBSs are split into two sites with possibility of multiple Sync Clusters on each site.

In this configuration:

- Each site has its own **Sync Master**
- There is no clock synchronization between the Sync Cluster of the main site and the Sync Cluster of the remote site
- Roaming is possible between the two Sync Clusters
- Handover is only possible within each Sync Cluster

When clock synchronization and handover is not required or not possible between groups of xBSs, it may be useful to define a site for each of these groups to avoid unnecessary data exchanges especially over a low data rate connection. Data are then only exchanged between base stations of a same site. Typical use case is a main site and one or several remote sites.

4.7 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.

ALE International 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 catalog and approval zone.

table 4.1: DECT list of countries and regions

Country or zone of registration	Corresponding region denomination	ALE International DECT availability	
		Approval	Catalog
All CE countries	1	Eur	Eur
US+Canada	2	US	US
APAC/ ASIA			
Australia	1	Eur	Eur
Bangladesh (2T)	1	Eur	Eur
Bhutan (2T)			
Cambodia	1	Eur	Closed
China	4	Asia	Asia
Hong Kong	1	Eur	Eur
India	1	Eur	Eur
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

Country or zone of registration	Corresponding region denomination	ALE International DECT availability	
		Approval	Catalog
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
Peru	3	Latam	Closed

Country or zone of registration	Corresponding region denomination	ALE International DECT availability	
		Approval	Catalog
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

Country or zone of registration	Corresponding region denomination	ALE International DECT availability	
		Approval	Catalog
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
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

Country or zone of registration	Corresponding region denomination	ALE International DECT availability	
		Approval	Catalog
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
Belorussia (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
Hungary	1	Eur	Eur

Country or zone of registration	Corresponding region denomination	ALE International DECT availability	
		Approval	Catalog
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

4.8 DECT traffic counters

The OXO Connect PCX manages a set of DECT traffic counters. These specific counters are mainly used to ascertain that there are enough DECT 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 counters are available from the web-based tool (DECT menu).

4.9 DECT engineering rules

The DECT engineering rules are described in the document: **DECT and IP-DECT Engineering Rules and Site Survey Kit Manual** (reference: 8AL90874).

4.10 xBS solution deployment

This chapter describes the installation and configuration of an xBS solution on the OXO Connect.

All the requested files and binaries are included in the OXO Connect software delivery. All xBS solution configuration is performed via OMC application.

It consists in:

- [Installing the xBS hardware](#) on page 78
- Configuring the PBX settings relating to xBS solution (see: [Configuring the xBS solution](#) on page 86)
- [Deploying xBS](#) on page 87
- [Configuring Sync Clusters and clock synchronization in a site](#) on page 90
- [Deploying DECT handsets](#) on page 91

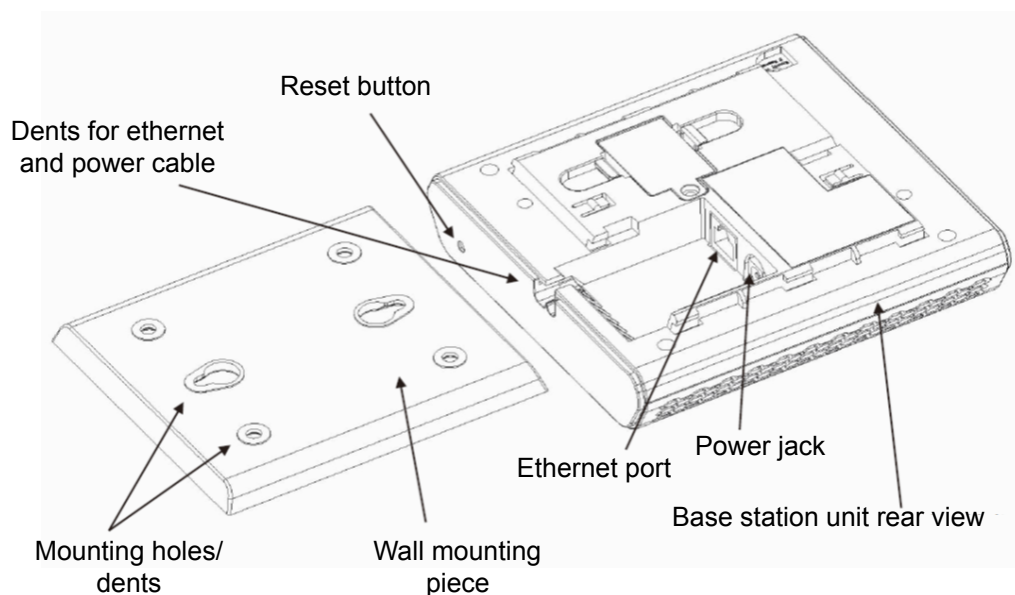
4.10.1 Installing the xBS hardware

The following paragraphs describe the hardware installation of an xBS on the OXO Connect.

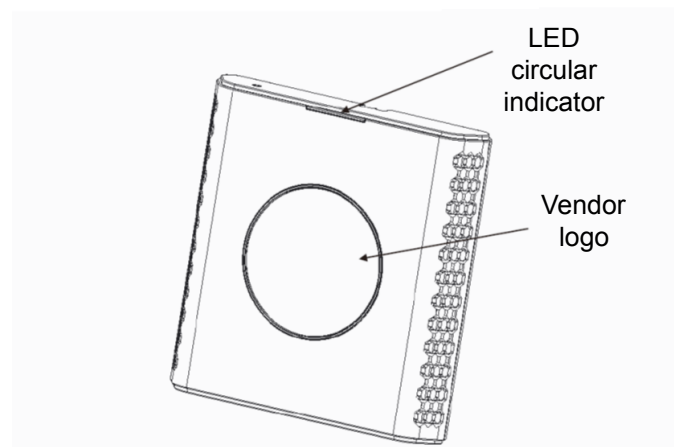
4.10.1.1 Hardware package description

Every shipped base unit package/box contains:

- 2 mounting screws and 2 anchors
- 1 plastic wall mounting piece
- 1 base unit



The base station front end shows an LED indicator that signals different functional states of the base unit and occasionally of the overall network. The indicator is off when the base unit is not powered.



4.10.1.2 Installing the base station

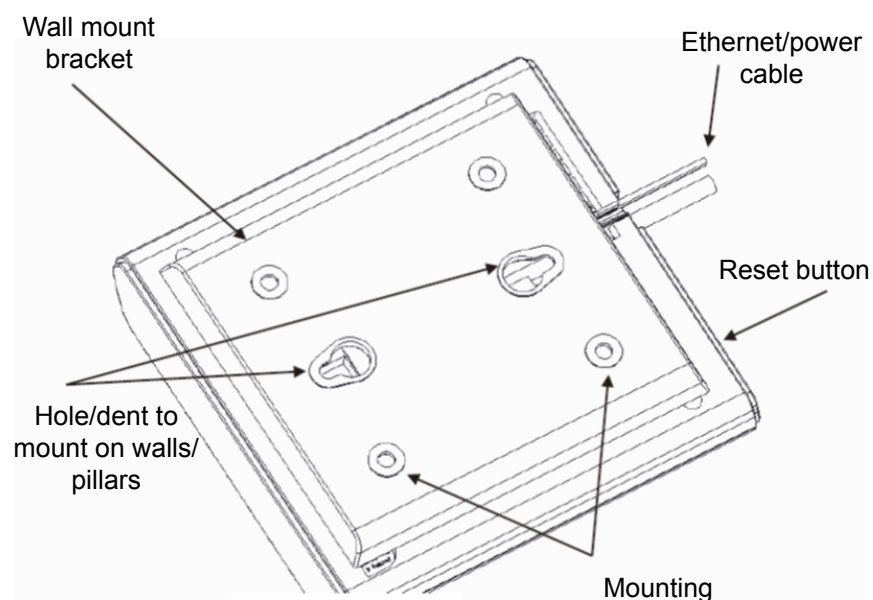
Determine the best location that will provide an optimal coverage taking account the construction of the building, architecture, and choice of building materials.

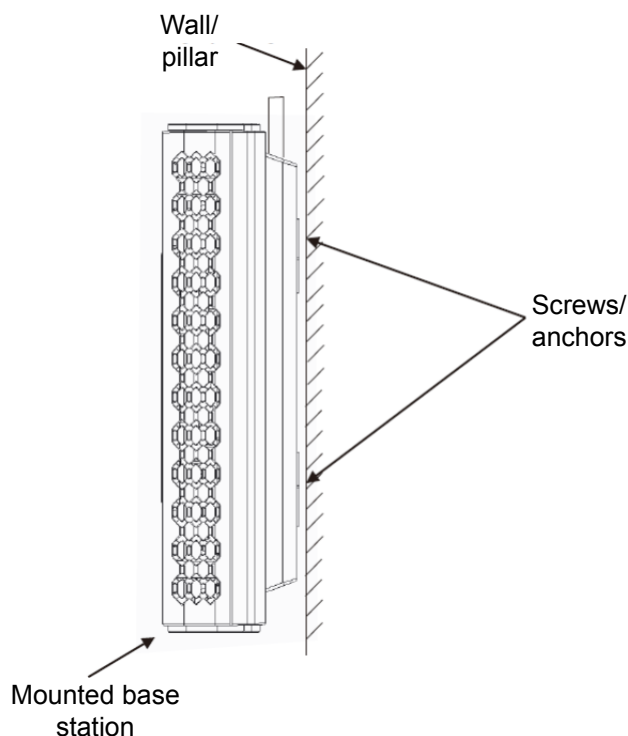
4.10.1.2.1 Installing an indoor base station

The base station is best mounted at an angle other than vertical on both concrete/wood/plaster pillars and walls for optimal radio coverage. Avoid mounting the base unit upside down as this would significantly reduce radio coverage.

Mount the base unit as high as possible to clear all nearby objects (e.g. office cubicles, cabinets, etc.).

Make sure that when you fix the base stations with screws, the screws do not touch the PCB on the unit. Avoid all contacts with any high voltage lines.





4.10.1.2.2 Installing an outdoor base station

Installation recommendations:

- To ensure water tightness, the unit must be installed with the antennas pointing down
- If installing in damp conditions, take the necessary steps to prevent any water from entering the unit when the unit must be opened
- The functional part of the base station (electronic part) must not have any electrical contact with an electrical pylon

Lightning protection:

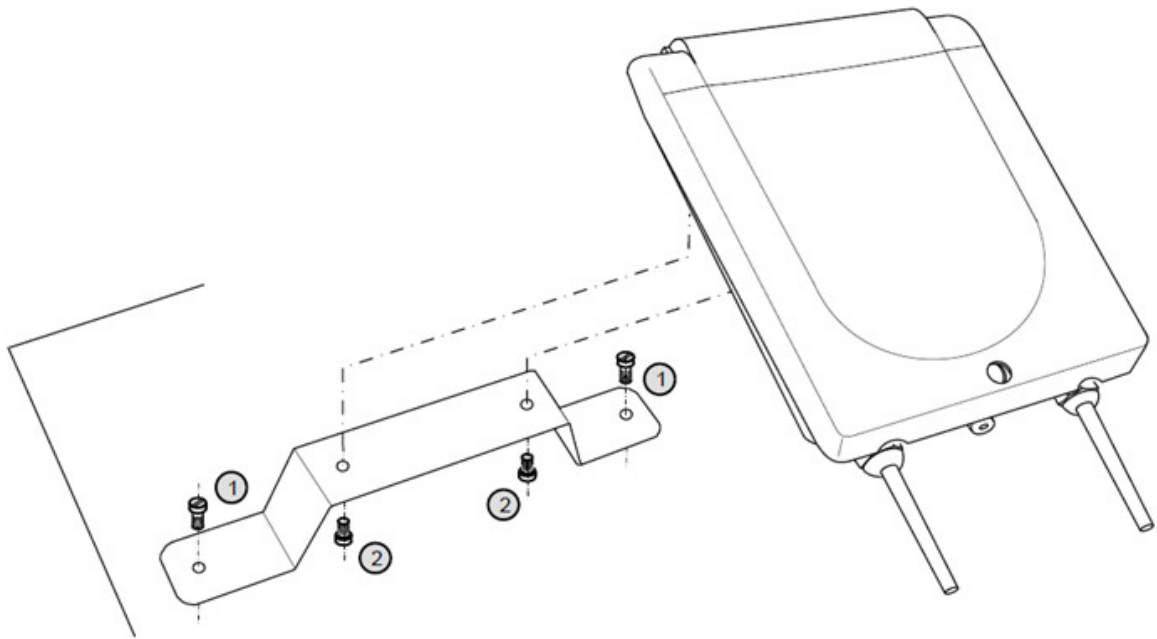
A lightning arrester is not required:

- If the base station is installed less than 1.50 m from a wall and more than 2 m below the roof
- if the base station is installed on another building with connection via an underground cable and the conditions outlined above are met.

4.10.1.2.2.1 Attaching the outdoor base station

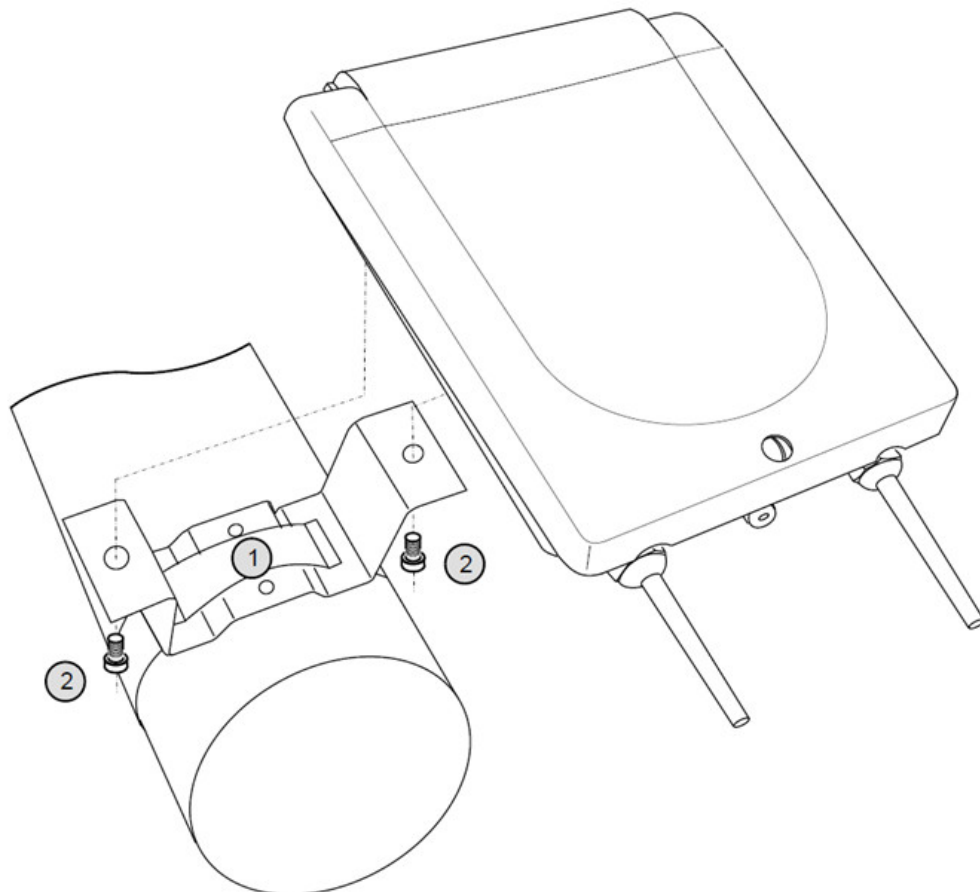
If attaching the base station to a wall:

- Attach the wall support to the wall with two screws (not provided)
- Attach the Outdoor xBS to the support with the two screws provided



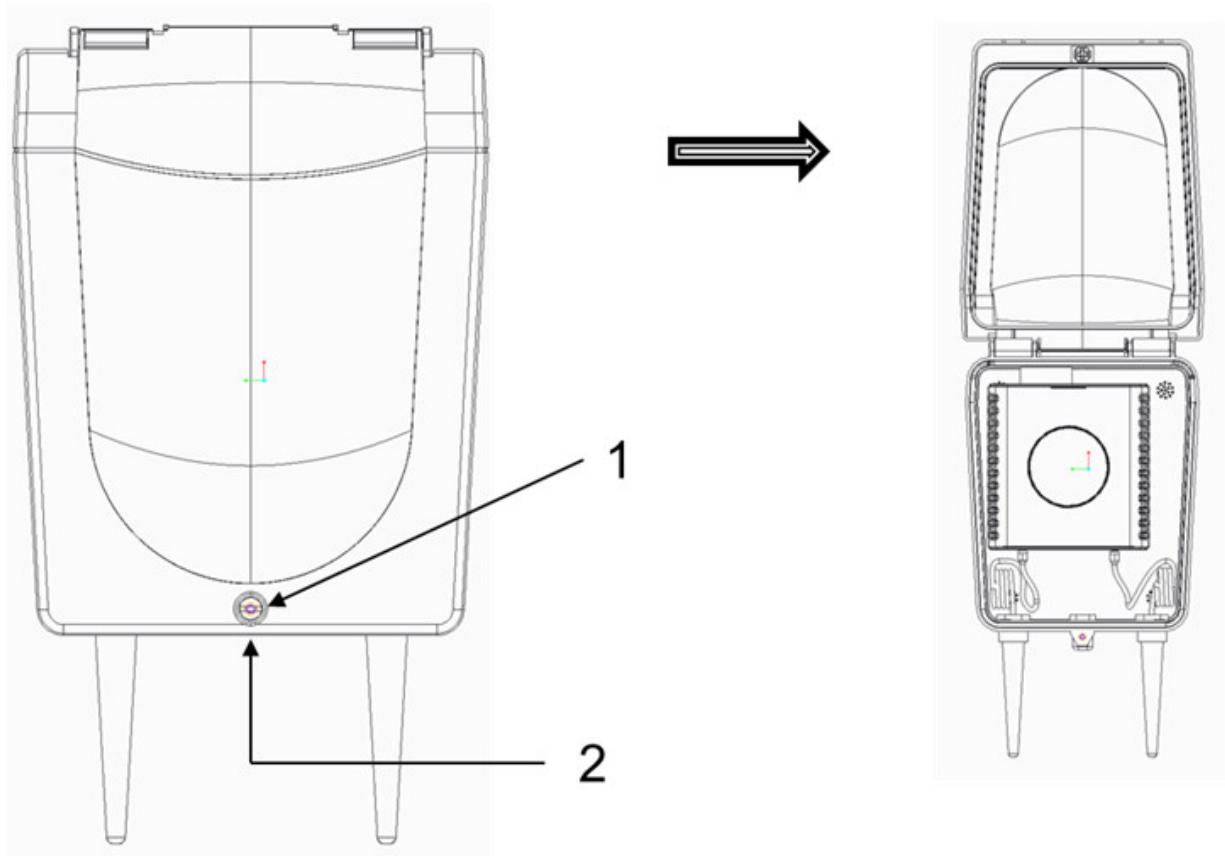
If attaching the base station to a mast:

- Attach the mast support to the mast with a pipe-collar (not provided)
- Attach the Outdoor xBS base station to the support with the two screws provided



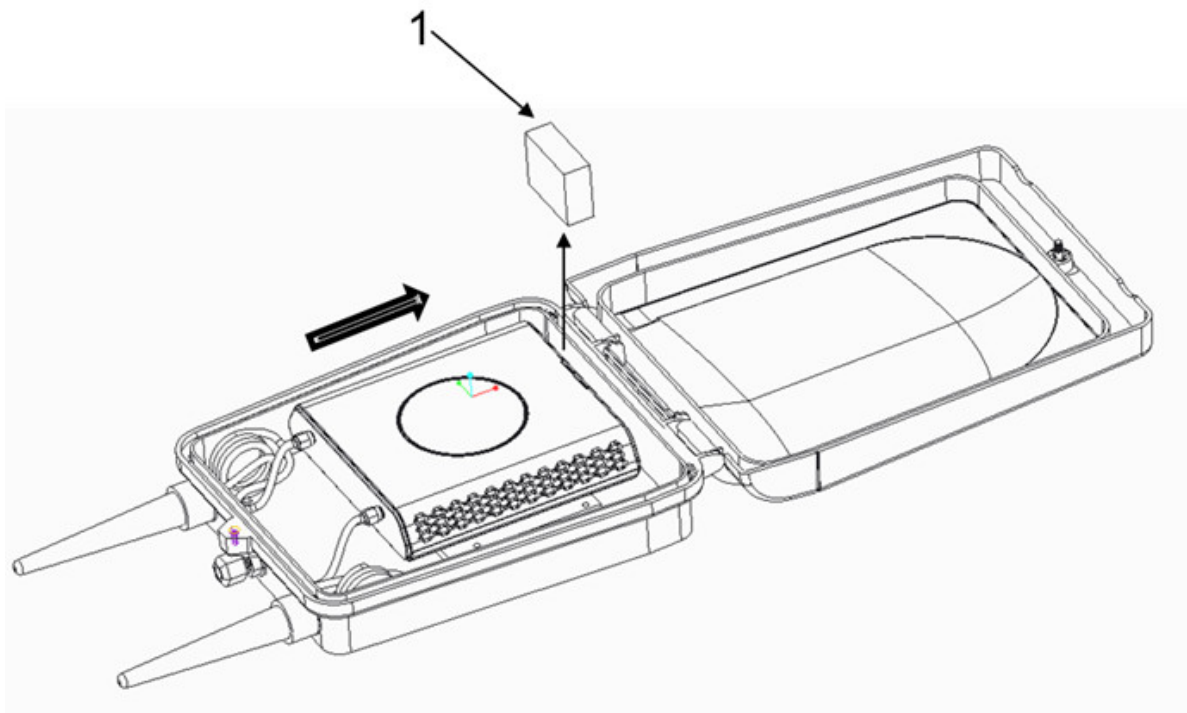
4.10.1.2.2.2 Wiring the base station

- After fixing the position, unfasten the screw and open the outdoor box (see 1 in the figure below)
- Untighten the cable gland and insert the RJ45 cable through the cable gland. (see 2 the figure below)



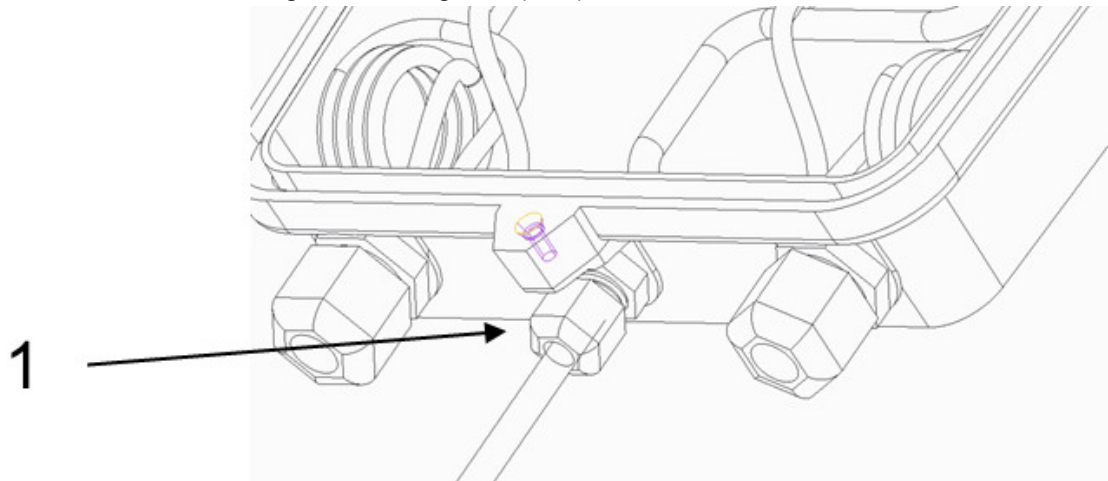
When the cover has been opened, wire the base station:

1. Remove the foam (used for transportation only)
2. Lift up the base station
3. Take out the base by sliding the base station upward.

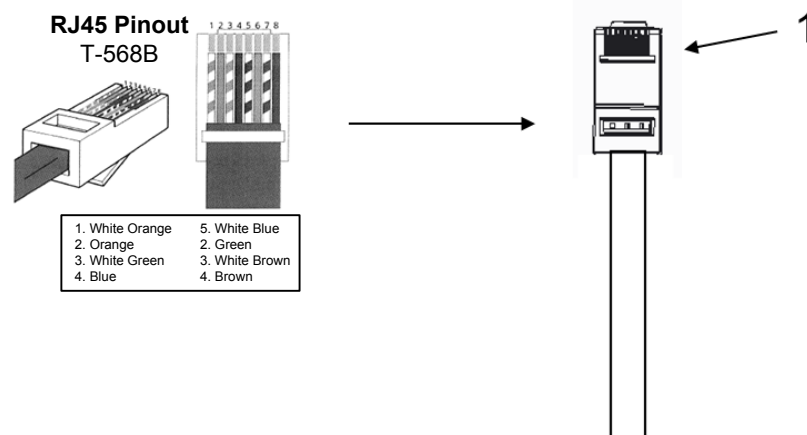


4. When the cover has been opened, wire the base station:

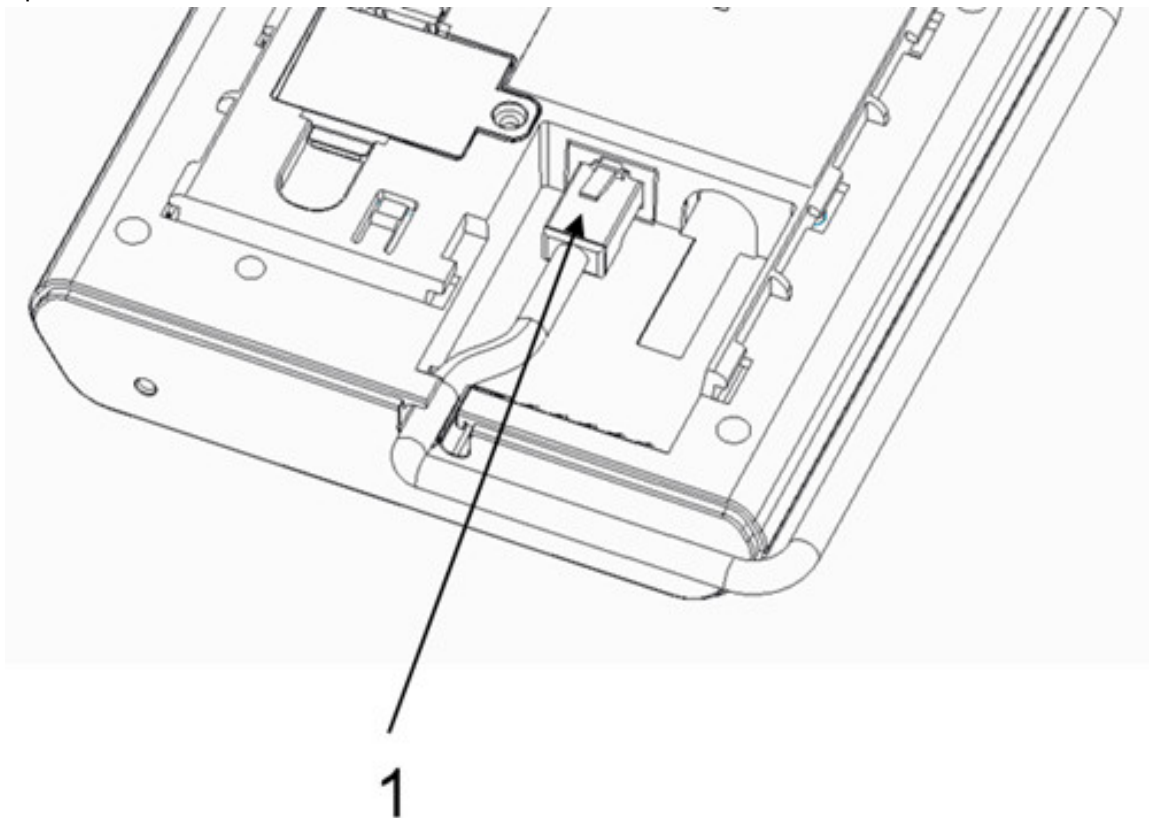
- a. Insert the RJ45 cable through the cable gland. (in 1)



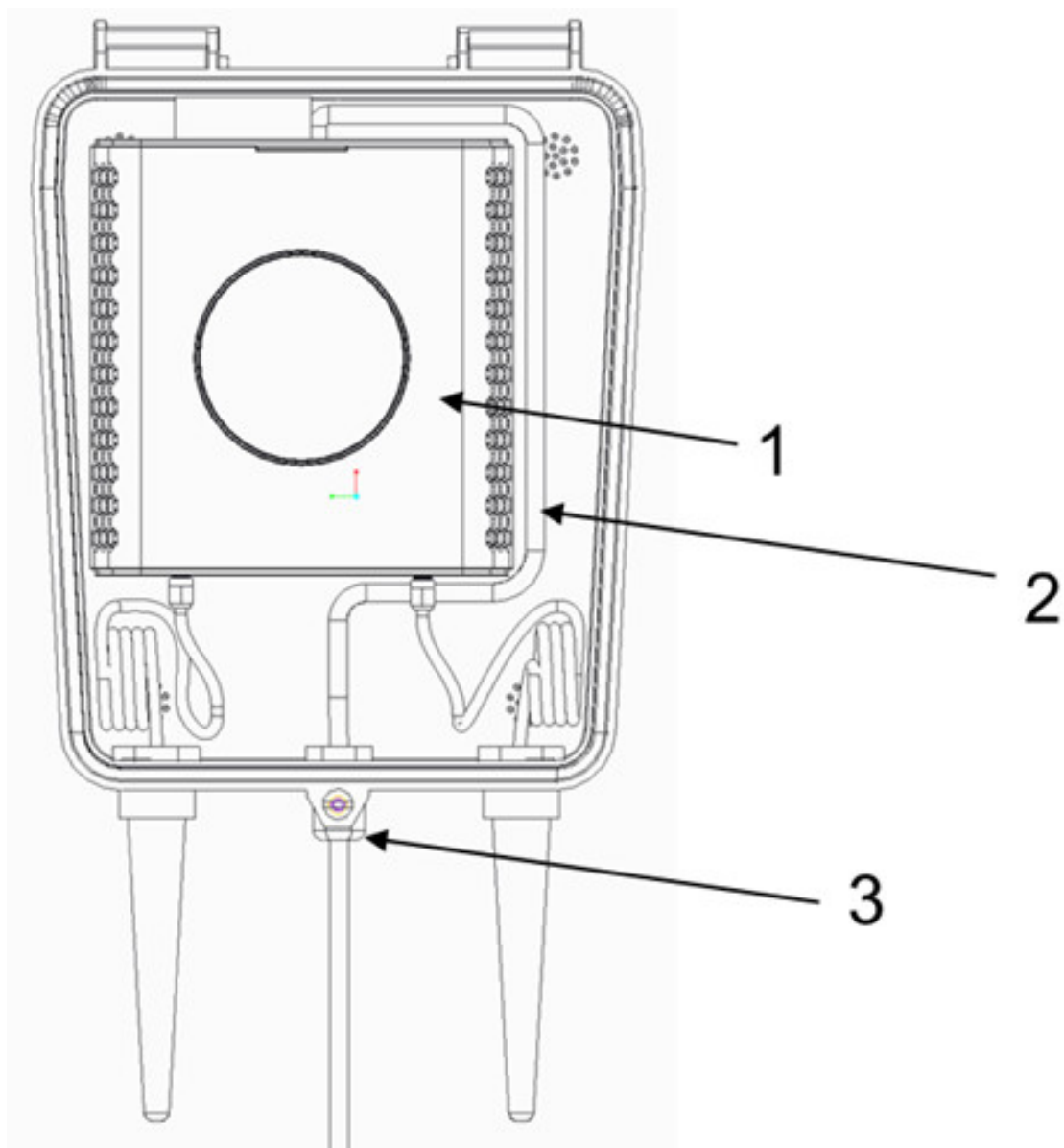
- b. Insert the cable into a transparent RJ45 socket following the TIA-568B. Then use the clamping tools to clamp the socket



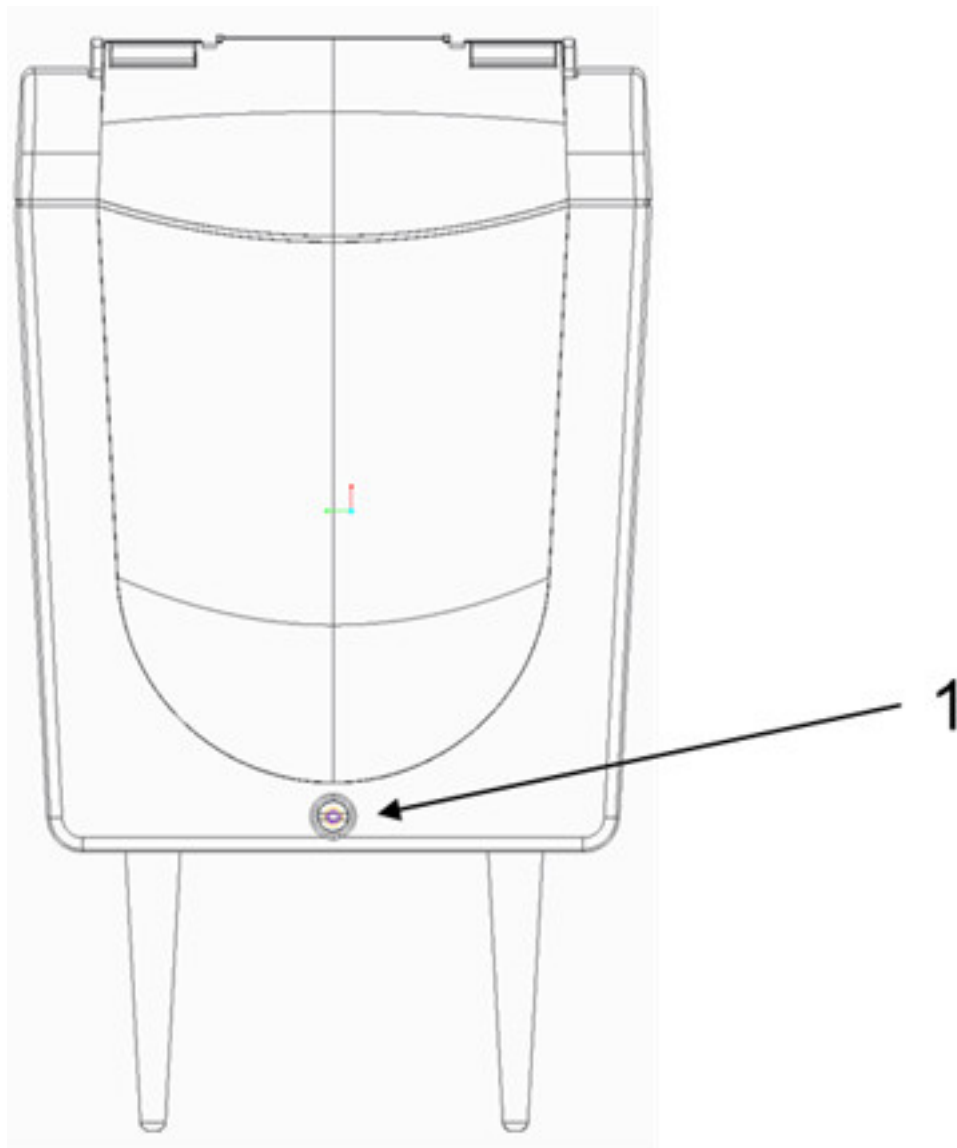
- c. Upside down the Base station. Put the cable into the RJ45 Connector



- d. Place the base station back to the bracket. Slide the base station bottom to top (see 1 in the figure below)
- e. Position the cable around the right side of the unit as shown in the diagram below. (see 2 in the figure below)
- f. Adjust the Ethernet cable and tighten the cable seal (see 3 in the figure below)



5. Close the box and screw to lock the top cover (see 1 in the figure below):



4.10.2 Configuring the xBS solution

4.10.2.1 Configuring DHCP server

At initialization in dynamic mode, xBSs use either the embedded DHCP server of the PBX (OXO Connect) or an external DHCP server to get:

- An allocated IP address
- The default router IP address
- The Subnetmask
- The next server IP address (PBX TFTP IP address)
- The DNS server (PBX IP address)
- The TFTP server name (PBX IP address)
- NTP (Network Time Protocol) (PBX IP address)

To configure the embedded DHCP server of the PBX, refer to the **DHCP configuration** section of document [14].

If an external DHCP server is used, it must be configured to serve xBSs and IP phones declared on the PBX:

- The **next-server** option has to be set to the IP address of the PBX
- The base station Vendor Class Identifier (VCI) is `alcatel.ipxbs.0`

4.10.2.2 Configuring the Access Right Identifier (ARI)

An Access Right Identifier (ARI) number must be assigned to the xBS solution on PBX. This ARI number must be defined on PBX before DECT handset registration. The ARI number allows to link DECT handsets to the xBS solution.

There is only one ARI number defined on the PBX. In an xBS/IBS DECT mixed configuration, the ARI number is used by the base stations of the two xBS and IBS DECT solutions.

To configure the ARI number:

1. In OMC, select **DECT > DECT/PWT/ARI/GAP**
2. In the **ARI** field, enter the ARI number of the xBS solution

4.10.2.3 Configuring auto provisioning

To allow xBSs to initialize in dynamic mode, the auto provisioning must be activated on PBX (same operation as for IP NOE phones). For more information, refer to the **Auto provisioning** section of document [13].

To configure auto provisioning:

1. In OMC, select **Subscribers/Basestations List > Auto Provision**
2. Select **Activate temporarily**

The automatic provision is temporarily activated for a predefined period (8 hours)

3. Close and reopen the screen to see the status change

The current status of auto provisioning configuration is indicated at the bottom of the **Subscribers/Basestations List** screen: **Automatic provisioning temporarily activated** or **Automatic provisioning deactivated**

4.10.2.4 Configuring the administrator password to access the base station settings

Each xBS includes a management tool accessible from a web browser (HTTP connection). This tool offers remote configuration of xBSs on the network (LAN).

Access to the base station management tool is protected by an administrator password common to all xBSs. This password is configured on PBX and sent to the xBSs during their initialization.

To configure the administrator password:

1. In OMC, select **System Miscellaneous > Passwords > Device Administrator Password**
2. In the **xBS Web Administrator** field, click the **Set** button and change the password (`Admin00!`)

4.10.3 Deploying xBS

4.10.3.1 Deploying xBSs in dynamic mode (auto provisioning)

By default, xBSs initialize in dynamic mode when they are connected to the LAN:

- They make a request to the DHCP server to get their network configuration (see: [Configuring DHCP server](#) on page 86)
- They make a TFTP request to the PBX to download their configuration file

xBSs are automatically declared in the PBX when requesting their configuration file (`startipxbs-<MAC address>`). xBSs are declared on PBX with the MAC address provided in the request of the

`startipxbs-<MAC address>` file and their IP address. Once declared on PBX, xBSs are listed in the **Subscribers/Basestations List** menu on OMC (with the **8378 DECT IP-xBS** label). Their parameter can be reviewed on OMC (see: [Declaring the xBS on PBX](#) on page 88).

Before connecting an xBS to the LAN, ensure that:

- A DHCP server is configured (see: [Configuring DHCP server](#) on page 86)
- Auto provisioning is selected in the PBX settings (see: [Configuring auto provisioning](#) on page 87)

4.10.3.2 Deploying xBSs in static mode (manual provisioning)

By default, xBSs initialize in dynamic mode when they are connected to the LAN. Skip this section if xBSs must be deployed in dynamic mode.

The static mode allows to configure manually an xBS. It consists in:

- [Declaring the xBS on PBX](#) on page 88
- [Configuring IP parameters on the xBS](#) on page 89

Once connected to LAN, the xBS makes a TFTP request to the PBX to download its configuration file (`startipxbs-<MAC address>`).

4.10.3.2.1 Declaring the xBS on PBX

To declare an xBS on PBX:

1. In OMC, select **Subscribers/Basestations List**
2. Click the **Add** button
3. Select the **xBS** radio button and click the **OK** button

The xBS is displayed in the list of subscribers with the **xBS** label

4. Select the xBS and click the **Details** button
5. Review/modify the following fields:

Site	Use the drop-down menu to select the site number to which the base station must belong (default value: 1)
RPN	Use the browser button to select the Radio Part Number (RPN) of the base station. Each base station has its own RPN, which is an hexadecimal two digit number (value between 80 and 254) <i>Note:</i> <i>The values between 0 and 79 are reserved for the base stations associated to the IBS DECT solution.</i>
Firmware version	Displays the firmware version of the base station (read-only)
RF Power (in dBm)	If needed, modify the RF power for the base station (in dBm)
Out of Service	If set to Yes , the base station is put out of service
Antenna diversity	If needed, select Diversity to allow the base station to receive calls on either of its two antennas according to reception quality (same for transmission) (default value: Diversity)
Location	If needed, select the location for emergency calls (default value: Default description (Location 0))
Serial Number	Displays the serial number of the base station (read-only)

Part Number	Displays the part number version of the base station (read-only)
Noisy audio environment	Select the radio button if the base station must operate in a noisy environment

6. Click **OK** to validate

7. Click the **IP settings** button and review/modify the following fields:

MAC address (hex)	Enter the MAC address of the base station
Voice Coding/Decoding	Use the drop-down menu to select the audio codec used for calls going through the base station (G711 or G729)
Voice Active Detection	If needed, select the Voice Activity Detection (VAD) which allows to reduce the bandwidth used (silence suppression)
(v4) IP address	This field displays the IP address of the base station when the equipment is connected.

8. Click **OK** to validate

When the xBS is connected to the LAN and detected by the PBX, the label identifying the base station in the list of subscribers changes: **xBS** label is replaced by **8378 DECT IP-xBS**.

4.10.3.2.2 Configuring IP parameters on the xBS

The following IP parameters must be defined on the xBS:

- Base station IP address
- Subnetwork mask
- Router IP address
- TFTP1 server IP address (PBX IP address)
- If needed, static VLAN number
- If needed, DHCP user class

Each xBS includes a management tool accessible from a web browser (HTTP connection). This tool offers remote configuration of xBS on the network (LAN).

To access the xBS management tool and configure its IP parameters:

1. Connect directly a computer to the xBS using a straight or crossed Ethernet cable
2. Press the xBS reset button and keep your finger on the button for at least 6 to 10 seconds
3. From a computer, open a web browser, and enter the xBS IP address:

`http://<base station IP address>`

Note:

- IP address is 192.168.0.2 when the xBS is implemented for the first time.
- Once the xBS has connected to the OXO Connect, you can retrieve its IP address via WebDiag, from the RPN or MAC address (written on the xBS).

4.10.3.3 xBS reset

4.10.3.3.1 Reset

The reset restores the xBS parameters to their default value, except the following parameters:

- IP configuration mode (DHCP, Static)
- IP static parameter, VLAN ID
- Customer certificate, self-generated certificate, CTL certificate
- Survivability data

- Main CS CPU and secondary
- Admin password

To reset an xBS, press its reset button (short press) or the `SW Reboot` button on the xBS web home page.

4.10.3.3.2 Reset to test and debug mode

This is a temporary mode: the configuration is only valid until the next reset.

This reset performs the following actions:

- Set the IP address to 192.168.0.2 (no VLAN, QoS parameters are applied in this mode)
- Web server is ready for login (unlocked even if the PBX has locked its access)
- The xBS runs in test mode, with access to software commands only available for some specific tests
- The web server password is set to its default value

To reset an xBS in test and debug mode, press its reset button and keep your finger on the button for at least 5 seconds.

4.10.3.3.3 Reset to factory

Reset to factory is intended to cope with situations in which the administrator can no longer access the base station configuration because the administrator password has been lost, and the base station is configured in static mode. Reset to factory can also apply when a base station, configured in static mode, must switch to a new xBS solution. A reset to factory is required before moving the base station to another system. Reset to factory is not needed when a base station is configured in dynamic mode.

The reset to factory performs the following actions:

- Restore the administrator password to its default value (`Admin00!`)
- Restore the configuration and settings to their default values (DHCP and dynamic mode)
- Remove all customer certificate, CTL server certificate, and self-generated certificate
- Remove survivability data
- Remove main and secondary CPU IP addresses in Flash

To reset an xBS to factory, press its reset button and keep your finger on the button for at least 15 seconds

Note:

This operation can also be performed from its web management interface.

4.10.4 Configuring Sync Clusters and clock synchronization in a site

Prerequisite: The xBSs must be configured on PBX (see: [Deploying xBS](#) on page 87).

For each site defined in PBX, it is possible to:

- Select the Sync Clusters to which the xBSs belong. By default, all xBSs belong to Sync Cluster 1.

This operation can be performed whatever the clock synchronization mode (manual or automatic).

- Configure manually the clock synchronization for all xBSs belonging to the site. By default, the clock synchronization is automatically managed by the xBS solution.

Note:

This operation must only be performed under the control of ALE International Technical Support.

To perform these operations:

1. In OMC, select **DECT > IP DECT Clock synchronization**
2. In the **Site** field, use the drop-down menu to select the site for which the clock synchronization and/or Sync Clusters must be configured

3. Click the **Manual** radio button
4. In the **Master** field, use the drop-down menu to select the xBS acting as master of the clock synchronization (default option: **Auto**)

In **Automatic** mode, this field is set to **Auto**, and it cannot be modified.

5. In the **Backup Master** field, select the xBS acting as second (backup) master of the clock synchronization (default option: **Auto**).

It is not possible to select the same xBS in **Master** and **Backup Master** field. The **Master** field must be configured before the **Backup Master** field.

In **Automatic** mode, this field is set to **Auto**, and it cannot be modified.

6. For each xBS listed in the **Clusters/Synchronization path** table, you can select:

- The Sync Cluster(s) to which they belong
- Their synchronization source (default option: **Auto**)

The xBS and its synchronization source always belong to the same Sync Cluster.

The synchronization source for the xBSs acting as **Master** and **Backup Master** is set to **Auto** and it cannot be configured.

In **Automatic** mode, the synchronization source for all xBSs is set to **Auto**, and it cannot be modified.

7. Click **OK** to validate

4.10.5 Deploying DECT handsets

In an xBS/IBS DECT mixed configuration, the DECT handset deployment can be performed either on the xBS solution or IBS DECT solution (this operation is identical on the two solutions). A DECT handset registered on the xBS solution can operate on an IBS DECT solution and vice-versa.

The DECT handset deployment consists in:

1. Declaring the handset on the PBX:
 - a. In OMC, select **Subscribers/Basestations List** and click the **Add** button
 - b. Click the **DECT IBS/DECT xBS** radio button and click **OK**
 - c. In the **Number of devices**, select the number of DECT handsets to create (default: 1)
 - d. In the **No** field, keep the proposed number or select another free number (grayed if there are several DECT handsets to create)
 - e. Click **OK**
2. Select the entry corresponding to the created set in the list and click the **GAP Reg** button
3. Launch the registration on the DECT handset
4. In OMC, select the entry corresponding to the created set in the **Unassigned Handsets list**
5. When the IPUI of the device registering appears in the list, select it
6. Click the **Assign** button
7. Click the **Return** button

4.10.6 xBS initialization with LED states

A three-color LED (green, red, and orange) is visible on the xBS front panel.

This LED provides information at the xBS initialization:

Initialization step	LED state
Step 0: Self-test and OS initialization	Unlit, or solid red displayed if error detected
Step 1: Network initialization	Red blinking (100 ms on /3000 ms off)
Step 2: IP parameters acquisition	Red blinking (100 ms on /400 ms off /100 ms on /3000 ms off)
Step 3: Configuration file download	Red blinking (100 ms on /400 ms off /100 ms) * 2 and 100 ms on /3000 ms off)
Step 4: Software download	Orange blinking (100 ms on and 3000 ms off)
Step 5: PBX link setup	Orange blinking (100 ms on /400 ms off /100 ms on and 3000 ms off)
Step 6: Base configuration by PBX	Orange blinking (100ms on /400 ms off/ 100 ms) * 2 and 100 ms on and 3000 ms off)
Base station active, and configuration is complete	Green blinking (400 ms on /100 ms off)
Base station in service, and synchronization is done	Green blinking (1 s on /1 s off)

8212/8232/8242/8262 DECT Handset Registration

5.1 Registering the Handset

5.1.1 Prerequisite

Before making a call the Handset must be registered to a DECT system.

The message **System 1 Auto install ?** is displayed on the screen in case of no registration.

The Handset can operate with a maximum of five DECT systems.

To register the Handset the following information must be available:

- PARK code: required if more than one DECT system overlaps in your location
- DECT system name
- Phone number allocated to the Handset

5.1.2 Service Level offered on IBS and IP-DECT systems

A same DECT handset can have a different level of service depending on which DECT system (IBS or IP-DECT) it is connected to.

A same service may be also implemented differently and invoked with a different user interface depending on which DECT system it is connected to.

table 5.1: Service Level offered on IBS/xBS and IP-DECT systems

Service	IBS/xBS mode	IP-DECT mode
	A-GAP	GAP (8212 DECT/8232 DECT) or CAT-iq (8242 DECT) + SIP
Phonebook	Centralized CS driven UI	Centralized Local UI
Contacts	Centralized (10 numbers)	Local
Call log	Partial (same as Premium DeskPhone) • Dial list • Incoming call log not supported	Yes Local
Text messages	Yes	No
Internal/external ringing melody selection	Yes	No
Conference	Yes	No

Service	IBS/xBS mode	IP-DECT mode
	A-GAP	GAP (8212 DECT/8232 DECT) or CAT-iq (8242 DECT) + SIP
PBX services	Yes	Partial Poor UI (service codes)
Nomadic mode	Yes	No
PIMphony	Yes	No
My IC Web	Yes	Yes

5.1.3 Registering Procedure

To register the Handset:

1. Declare the handset on the PCX, see: [Declaring the Handset on the OXO Connect](#) on page 94
2. Configure the handset, see: [Registering the handset](#) on page 94

5.1.4 Declaring the Handset on the OXO Connect

To declare the handset:

1. In OMC, select **Subscribers/Base stations List**

The **Subscribers/Base stations List** window is displayed

2. Click **Add**

The **Add Subscriber/Base station** window is displayed

3. Select **IBS/xBS** (IBS solution) or **4080/8340 IP DECT** (IP-DECT solution)
4. Select the **number of device** to create (default: 1)
5. Keep the proposed number or select another free number
6. Click **OK**

5.1.5 Registering the handset

To register the Handset:

1. In OMC:

- a. Select the entry corresponding to the created set in the list and click the **GAP Reg** button

The **Register GAP handset** window opens

- b. For IBS/xBS DECT solution:

- a. Launch the registration on the handset: see [Registering the handset](#) on page 94
- b. Select the entry corresponding to the created set in the **Unassigned Handsets** list
- c. When the IPUI of the device registering appears in the list, select it
- d. Click the **Assign** button
- e. Click **Return**

- c. For IP-DECT solution:

- a. Select the IP-DECT handset and click the **Register** button.

The PARK code, a PIN code, and a registration status is displayed.

- b. Launch the registration on the handset: see [Registering the handset](#) on page 94

Once the set is registered, its status change to **Registered** in the **IP-DECT Registration** window.

2. On the handset:

- a. The message **System 1 Auto install ?** is displayed, press the **OK** button.
- b. The message **Register** is displayed, press the **OK** button.
- c. Enter the pin code (0000 by default) and press the **OK** button.
- d. Select a system (it is recommended that the first empty system is selected).
- e. Enter the PARK code and confirm your entries.
- f. Enter the access code and confirm your entries.
- g. select the power mode and press the **OK** button.

Note:

You are advised not to select the 50 mw power mode unless required. The 50 mw power mode is intended for hazardous sites such as nuclear plants where it is requested that emissions do not exceed the maximum value.

The registration operation can last up to 2 minutes.

If the operation has been done correctly (subscription accepted), the telephone is ready to be used and the radio reception quality icon is displayed.

If the registration operation has not been successful, the station proposes launching the subscription again.

Note:

To register the handset on more than one system, refer to the constructor documentation.

An SD card can be inserted into the 8242 DECT/8262 DECT handsets to increase the number of local contacts and messages. This SD card can also store the handset configuration data and subscription data. The data stored depends on the system (IBS/xBS DECT or IP-DECT) on which the handset is registered:

- When the handset is registered on an IBS/xBS DECT system (8242 DECT/8262 DECT handsets), the SD card only stores the handset configuration data
- When the handset is registered on an IP-DECT system (8242 DECT handsets), the SD card stores the handset configuration and subscription data

5.1.6 Internal/external ringing tune

This feature allows the user to configure separate ringing melodies for internal and external incoming calls.

See the user guide for the concerned set for more information.

5.2 FAQ and troubleshooting tips

5.2.1 Can I use the 50 mW low power mode: probably NOT

The 50 mW low power mode is intended for hazardous sites, such as nuclear power plants, where emissions must not exceed the maximum value of 50 mW. This mode applies only when requested. Its use implies a specific site survey and base station deployment. If used inappropriately, it can cause problems, such as call drops, audio noises and poor quality transmissions in the areas covered by this system.

5.2.2 Economy mode versus 50 mW low power mode

5.2.2.1 Economy mode

The aim of the ECO mode (or Economy mode) is to decrease power consumption and radiations whenever possible. It is intended to be nature friendly and automatically minimize, whenever possible, the radio frequency power to 25 mW peaks, as opposed to the 250 mW peaks (or 210 mW peaks in the US) of the standard power mode.

The Economy mode is selected by the end-user in the DECT settings menu.

When the Economy mode is active, RF emission switches automatically:

- From normal power to economy mode when approaching a DECT base station -60 dBm for at least 1.6 seconds
- From Economy to normal mode when going away from a base station RF field -70 dBm for at least 1.6 seconds

Caution:

In strong interference environments, when the ECO mode is active, transmission conditions can degrade resulting in bad quality of the audio channel and possibly call cuts.

5.2.2.2 50 mW mode

The 50 mW mode is required for hazardous sites, such as nuclear power plants, where emissions must not exceed the maximum value of 50 mW.

The 50 mW mode is selected at DECT registration and, as selected mode, it is permanent.

Caution:

The 50 mW mode must be used ONLY in systems specifically deployed for this use.

5.2.2.3 How do I know which mode is (Economy or 50 mW) active?

The status of these two modes is reflected in the Signal Strength Icon (vertical bars).

	Economy mode disabled	Economy mode enabled	
		inactive	active
Standard power mode			
50mW power mode			

50 mW power mode

=> icon with 3 bars

Standard power mode

=> icon with 4 bars

ECO mode disabled:

normal field strength, 3 or 4 bars

ECO mode enabled and inactive:

field strength with a white E letter on the top left corner

ECO mode enabled and active:

field strength with a green E letter on the top left corner

5.2.2.4 Peak transmission power according to mode

dBm	mW	Parameter
24	250	Standard power mode (Europe)
21	125	Standard power mode (US)
17	50	50 mW power mode
14	25	Economy mode enabled and active

Geolocation and Notification Management on DECT

6.1 Overview

This document details the geolocation and alarm feature available with the OXO Connect on 8242 DECT and 8262 DECT handsets in IBS and xBS deployments.

Specific alarms are triggered from the set and sent to a server to provide isolated worker protection. These alarms include location data, so that assistance can be sent to the end user with the shortest delay.

Possible types of alarms are:

- Notified by the user:
 - Alarm button: sends an alarm when the user pushes a button, after an unexpected event
 - Event button: sends an event alarm when the user pushes a button (long press in communication or idle state) to indicate a predefined event.

For DECT handset, available keys are **1, 2, 3, 4, 5, 6, 7, 8, 9**.

- Automatically initiated by the handset and transparent to the user (8262 DECT only):
 - Man down alarm: sends an alarm when the end user has lost verticality, which generally implies having fallen on the ground, because of an injury
 - No movement: sends an alarm, after a period of inactivity of the end user
 - Shock: sends an alarm when an abnormal shock is detected
 - Pull cord: sends an alarm when the pull-cord is removed from the DECT handset

The alarm and geolocation service requires the use of an alarm server to process the data sent from DECT handset.

Additionally, the Alarm server can send alarm messages or make voice calls upon trigger of external events, to ask the user to react (example: "Fire Alarm" displayed on the screen and ringing at maximum level). The list of available alarms is the following:

- Handset ringing with normal alarm
- Handset ringing with urgent alarm
- Handset ringing with very urgent alarm
- Handset automatic answer in handsfree mode

For a detailed description of the alarm feature, refer to the following documents:

- 8262 DECT Handset Alarms: Geolocation and notification (reference: 8AL900324ENAA)
- 8242 DECT Handset Alarms: Geolocation and notification (reference: 8AL900309ENAA)

6.2 Architecture

6.2.1 Alarm server architecture

Alarm processing is managed together by the OXO Connect and the third party alarm server.

The Alarm server interacts with the call server with signaling links and voice links. It is able to make or receive call to any fixed or wireless sets attached to the call server.

¹ For a complete list of supported alarm servers and their associated configuration, see the Alcatel-Lucent Applications Partner Program (AAPP) web site

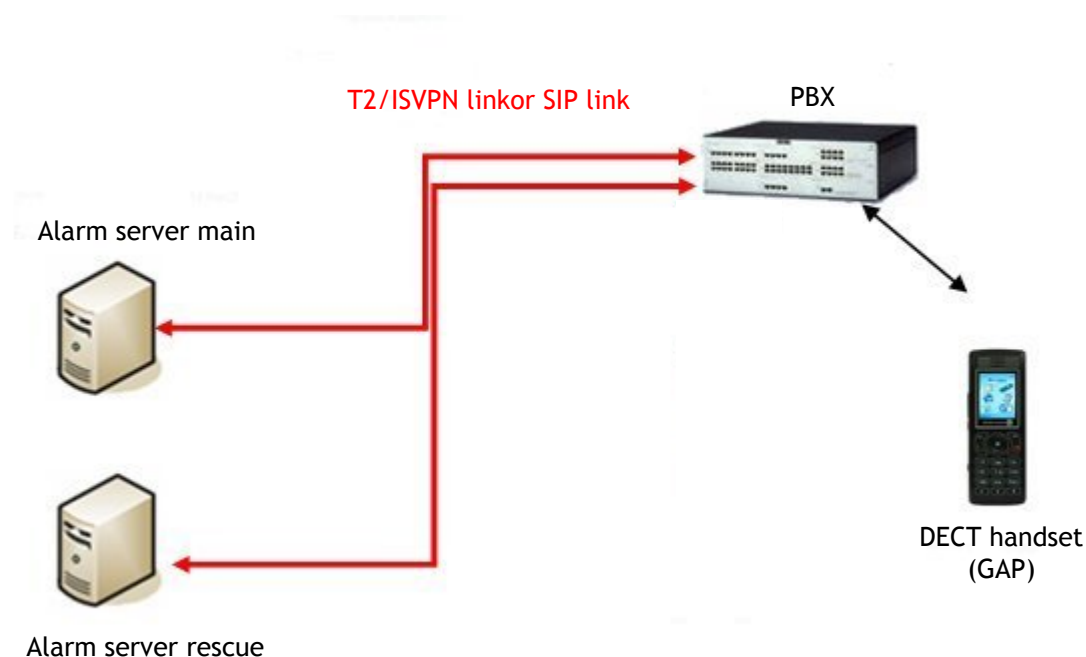


Figure 6.1: Example of Alarm Related Architecture

6.2.2 Message Mode Supported

Office mode

6.2.3 Supported Trunks

Two types of trunks can be used between the OXO Connect and the alarm server:

- T2/ISVPN
- SIP

6.3 OXO Connect Configuration

6.3.1 Configuring the T2 Trunk

6.3.1.1 Checking Hardware and Limits

1. In OMC (Expert View) select: **System > Hardware and Limits > Software Key Features > Multi-site** tab
2. Review/modify the followings attributes:

Parameter	This parameter must be set to:
Call handling ISVPN service	Enabled
Call handling QSIG + protocol	Enabled

3. Confirm your entries

6.3.1.2 Configuring External Lines

1. In OMC (Expert View): select **System > External Lines > List of Accesses**
2. Create a trunk containing a T2 access (T2 trunk group)

Note:

By default, a T2 trunk group contains one channel. This value must be increased to the desired value.

3. When the channels number has been changed, you are requested to reset the PowerCPU EE board. Reset the board
4. Select the created trunk
5. Click **Details**
6. Unselect **Public trunk** and click **OK**
7. Click **Return**
8. Select **Protocols**
9. Review/modify the following attributes:

ISDN Trunks	Select EDSS1
Digital Tie Lines	Select QSIG
ISVPN Protocols	Select ISVPN
Analog Trunks	Select 1 NDDI France
Register Signalling	Select R2 Signalling

10. Confirm your entries
11. Select **List of Trunk Groups**
12. Select a trunk group
13. Type **T2** in the **Name** field
14. Click **Modify**
15. Click **Details**
16. Click **Add**
17. Click **OK**
18. Click **Link-Cat**
19. Configure Traffic Sharing:

Traffic Sharing Mode		Barring Mode		
Mode	LC No	Mode	Voice VLC	Non V. NLC
Norm.	1	Norm.	1	1
Rest.	1	Rest.	1	1

20. Confirm your entries

6.3.1.3 Configuring Numbering

6.3.1.3.1 Declaring the Trunk Group in the Internal Numbering Plan

1. In OMC (Expert View): select **System > Numbering > Numbering Plans > Internal Numbering Plan** tab
2. Create a secondary trunk group with the following parameters:

Start	Enter the trunk group prefix
End	Enter the trunk group prefix
Base	Select ARS
NMT	Select Keep
Priv	Select Yes

6.3.1.3.2 Configuring the End of Dialing Table

1. In OMC (Expert View): select **System > Numbering > End of Dialing Table**
2. Add the T2 trunk group prefix with 20 as **Counter** value
3. Validate

6.3.1.4 Configuring the Automatic Routing

6.3.1.4.1 Configuring Automatic Routing: Trunk Group List

1. In OMC (Expert View) select: **System > Numbering > Automatic Routing Selection > Trunk Group Lists**
2. Right-click the ARS OMC windows and select **Add**.

The **Selection List** window opens

Index	Select in the list the index corresponding to the external line configured previously (see Configuring External Lines on page 100) and Click OK
No.	Enter the directory number associated to the trunk group
Provider/Destination	Select None
Access Digits	Leave blank
Auth. code ID	Select None
Tone/Pause	Select None

3. Right click and Select **Apply**

6.3.1.4.2 Configuring Automatic Routing: Prefixes

1. In OMC (Expert View) select **Numbering > Automatic Routing Selection > Automatic Routing: Prefixes**
2. Right-click the ARS OMC windows and select **Add**
3. Enter the following parameters:

table 6.1: Common fields

Activation	yes
Network	Enter priv

Prefix	Enter the trunk group prefix configured in the internal numbering plan
Substitute	Enter the trunk group prefix configured in the internal numbering plan
TrGpList	Enter the index of T2 trunk
Called (ISVPN/H450)	Enter het

4. Right-click the ARS OMC windows and select **IP Parameters**

Configure the following parameter:

table 6.2: IP parameters fields for a T2 Trunk Group

Destination	Select Not IP
--------------------	----------------------

5. Right click and select **Apply**

6.3.1.5 Configuring Installation Numbers

1. In OMC (Expert View) select: **System > Numbering > Installation Numbers**

The **Installation Numbers** window is displayed

2. Enter the **Installation Number** and click **OK**

6.3.1.6 Saving Configuration

1. In OMC (Expert View), select **Comm > Read all from the PCX** from the menu bar.

The **Read from the PCX** window is displayed

2. Select **Classic Data** and validate the **Central Services** check box
3. Click **OK** and wait until a progress bar is displayed
4. Once the progress bar disappears, select File > Save as from the menu bar

The **Save as Database** Window is displayed

5. Enter a file name and click the **Save as** button

6.3.2 Configuring the SIP Trunk

6.3.2.1 Checking Hardware and Limits

1. In OMC (Expert View) select: **System > Hardware and Limits > LAN/IP Configuration > Boards** tab
2. Check the IP addresses

6.3.2.2 Configuring External Lines

1. In OMC (Expert View): select **System > External Lines > List of Accesses**
2. Create a trunk containing VoIP trunks (SIP trunk groups)

Note:

By default, a SIP trunk group contains one channel. This value must be increased to the desired value.

3. Select the created trunk
4. Click **Details**
5. Unselect **Public trunk** and click **OK**
6. Click **Return**

7. Select **Protocols**

8. Review/modify the following attributes:

ISDN Trunks	Select EDSS1
Digital Tie Lines	Select QSIG
ISVPN Protocols	Select ISVPN
Analog Trunks	Select 1 NDDI France
Register Signalling	Select R2 Signalling

9. Confirm your entries

10. Select **List of Trunk Groups**

11. Select a trunk group

12. Type **SIP** in the **Name** field13. Click **Modify**14. Click **Details**15. Click **Add**16. Click **OK**17. Click **Link-Cat**

18. Configure Traffic Sharing:

Traffic Sharing Mode		Barring Mode		
Mode	LC No	Mode	Voice VLC	Non V. NLC
Norm.	1	Norm.	1	1
Rest.	1	Rest.	1	1

19. Confirm your entries

6.3.2.3 Configuring Numbering

6.3.2.3.1 Declaring the Trunk Group in the Internal Numbering Plan

1. In OMC (Expert View): select **System > Numbering > Numbering Plans > Internal Numbering Plan** tab
2. Create a secondary trunk group with the following parameters:

Start	Enter the trunk group prefix
End	Enter the trunk group prefix
Base	Select ARS
NMT	Select Keep
Priv	Select Yes

6.3.2.3.2 Configuring the End of Dialing Table

1. In OMC (Expert View): select **System > Numbering > End of Dialing Table**

2. Add the SIP trunk group prefix with 20 as **Counter** value
3. Validate

6.3.2.4 Configuring the Automatic Routing

6.3.2.4.1 Configuring Automatic Routing: Trunk Group List

1. In OMC (Expert View) select: **System > Numbering > Automatic Routing Selection > Trunk Group Lists**
2. Right-click the ARS OMC windows and select **Add**.

The **Selection List** window opens

Index	Select in the list the index corresponding to the external line configured previously (see Configuring External Lines on page 100) and Click OK
No.	Enter the directory number associated to the trunk group
Provider/Destination	Select None
Access Digits	Leave blank
Auth. code ID	Select None
Tone/Pause	Select None

3. Right click and Select **Apply**

6.3.2.4.2 Configuring Automatic Routing: Prefixes

1. In OMC (Expert View) select **Numbering > Automatic Routing Selection > Automatic Routing: Prefixes**
2. Right-click the ARS OMC windows and select **Add**
3. Enter the following parameters:

table 6.3: Common fields

Activation	yes
Network	Enter priv
Prefix	Enter the trunk group prefix configured in the internal numbering plan
Substitute	Enter the trunk group prefix configured in the internal numbering plan
TrGpList	Enter the index of SIP trunk
Called (ISVPN/H450)	Enter het

4. Right-click the ARS OMC windows and select **IP Parameters**
5. Configure the following parameters:

Destination	Select SIP Gateway
--------------------	---------------------------

6. Select **System > Numbering > Automatic Routing Selection > SIP Gateway Parameters**
7. Click **Create**

The **Gateway Parameters Details** opens.

8. In the **Domain Proxy** tab, review/modify the following parameters:

IP Type	Static (value determined by the system)
IP Address	Enter the Alarm Server public IP address

9. In the **Media** tab, review/modify the following parameters:

Codec/Framing	Select Default
Gateway Bandwidth	Enter 128 Kb/s

10. In the **Protocol** tab, review/modify the following parameters:

Alive Protocol	Enter SIP
Alive Timeout/s	Enter 0

11. Right click and select **Apply**

6.3.2.5 Configuring Installation Numbers

1. In OMC (Expert View) select: **System > Numbering > Installation Numbers**

The **Installation Numbers** window is displayed

2. Enter the **Installation Number** and click **OK**

6.3.2.6 Saving Configuration

1. In OMC (Expert View), select **Comm > Read all from the PCX** from the menu bar.

The **Read from the PCX** window is displayed

2. Select **Classic Data** and validate the **Central Services** check box
3. Click **OK** and wait until a progress bar is displayed
4. Once the progress bar disappears, select **File > Save as** from the menu bar

The **Save as Database** Window is displayed

5. Enter a file name and click the **Save as** button

6.3.3 Configuring Handsets

1. Declare DECT handsets on the OXO Connect as detailed: [Declaring the Handset on the OmniPCX Office](#)
2. Declare the handset number range in:
 - The **Internal Numbering Plan**
 - The **Public Numbering Plan**
 - The **Private Numbering Plan**
3. Register the DECT handset with **GAP Evo (Affi.)**
4. Configure accesses via the MMI menu:
 - Access 1: enter the trunk group prefix number of the trunk group towards the primary alarm server

- Access 2 (optional): the trunk group prefix number of the trunk group towards the secondary alarm server or of a secondary trunk group towards the primary alarm server
- 5. Select the operating mode: Office (limited to seventeen digits)
- 6. Complete the identification codes of the different levels of alarms for incoming alarms sent by the Alarm server

6.4 Other Configuration Documents

Refer to the following documents:

- Localization and notification management User documentation
- Localization and notification management Configuration documentation

7.1 Overview

7.1.1 Overview

The Advanced Cellular Extension service (ACE) is a feature of the OXO Connect, 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 OXO Connect services.

The software client can be either:

- The Ace client

Note:

The mobile device must be compliant with the Ace application. The list of compatible mobile devices is available on the Enterprise Business Portal.

- The Nokia Call Connect (NCC) for Alcatel-Lucent software

Note:

The list of compatible mobile devices is available on the Enterprise Business Portal.

Note:

*In this document, **Advanced Cellular Extension (ACE)** refers to the feature of the OXO Connect. **Ace** refers to the client software hosted on a mobile phone.*

7.1.2 Implementation

The ACE mobile phone is associated to a 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 center is called, whatever the mobile mode: ACE or private.

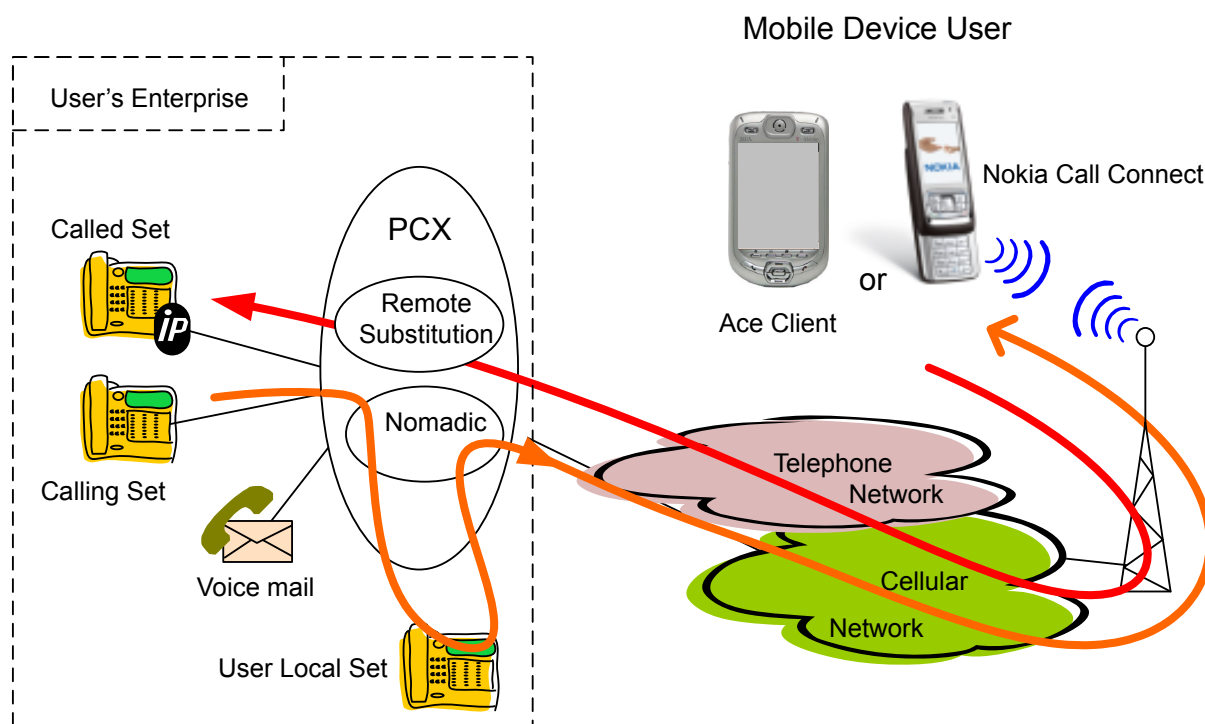


Figure 7.1: ACE Cellular Mode Architecture

7.2 Configuration procedure

This chapter details the configuration on OXO Connect to implement Advanced Cellular Extension.

7.2.1 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

7.2.2 Pre-Requisites

The Advanced Cellular Extension implementation requires:

- An OXO Connect
- An ISDN/Analog trunk group to the public network

Remark:

Analog lines also can be used for ACE

- The **DISA / DISA Transit** license

- The **Voice Mail Remote Customization** license
- A **Nomadic user** license 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)

7.2.2.1 Checking Licenses

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 license is necessary for each virtual nomadic terminal, including ACE subscribers.

7.2.2.2 Configuring DDI Numbers

If necessary, create DDI numbers:

1. In OMC (Expert View), select **Dialing > Dialing 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)

7.2.3 PCX Configuration

7.2.3.1 Configuring the Numbering Plan

It is necessary to create secondary trunk groups corresponding to the internal numbers that can be dialed 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 **Dialing > Dialing Plans > Internal Dialing 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 center is always called: this operation mode cannot be modified on the mobile phone.

7.2.3.2 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

7.2.3.3 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 attendant call number:
 - **Activation:** Yes
 - **Network:** Priv
 - **Prefix:** #9
 - **Ranges:** leave blank
 - **Substitute:** 9
 - **TrGpList:** 6 (local trunk group number)

7.2.3.4 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.

7.2.3.4.1 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

7.2.3.4.2 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.

7.2.4 Client Installation and Configuration

To install and configure the Ace client software on a mobile set, refer to the Ace Installation Manual.

To install and configure the NCC client software on a mobile set, refer to the **Nokia Call Connect Administration Guide**.

7.2.5 Nomadic Activation

Once the OXO Connect 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

Alcatel-Lucent Enterprise OpenTouch Conversation for iPhone

8.1 Introduction

Alcatel-Lucent Enterprise OpenTouch Conversation for iPhone (also called OTCV iPhone) is a software client application running on a mobile phone using the iOS from Apple. It provides an access to enterprise telephony services over a mobile Internet access or Wi-Fi network, to enable the iPhone to operate as a business phone.

OTCV iPhone provides access to business telephony features. In addition to the typical business telephony features, OTCV iPhone provides data connection to:

- Business directory
- Business call logs
- Business voice mail

OTCV iPhone:

- Interacts with native iPhone applications to enrich the communication services (local contacts)
- Can be used in remote locations, e.g. via Internet, to have access to the same level of services as in the Enterprise premises (See [13] chapter: Network configuration for remote accesses, for detailed information about network configuration from Internet/WAN)
- Can be associated to a deskphone (call routing profile configuration) or operate standalone

For information about the list of compatible devices and OS versions, see the Technical Communication TC1637, available from the Enterprise Business Portal (reference name: MIC_UC_Client_DeviceWhiteList_8AL90822AAAA).

Note:

Data connection is dependent on network availability. OTCV iPhone cannot handle any fallback mode or business services when the data connection is not available.

8.1.1 Apple hardware

The OTCV iPhone application can be used in conjunction with iPhone 4S , iPhone 5 , iPhone 5C, iPhone 5S, iPhone 6 and 6 Plus.

The iPad series is not supported.

8.2 Architecture

8.2.1 Overview

This module presents the network topologies to access the PBX services from an OTCV iPhone application.

For data communication, the OTCV iPhone accesses the PBX services using OmniTouch 8400 ICS web services implemented in the PBX (that is OXO Connect). It requires either one of these network connectivities:

- The enterprise Wi-Fi network inside the enterprise

Note:

A Wi-Fi Internet access or hot spot can be used at home for data transmission.

- An Internet/data connection provided by some cellular networks (2.5G, 3G, 3G+, 4G and GPRS) outside the enterprise. See the section **Network configuration for remote accesses** in document [13] for detailed information about network configuration from Internet/WAN

For voice communication:

- If the OTCV iPhone application is connected to the enterprise Wi-Fi network inside the enterprise, it is possible to use the VoWiFi (Voice over IP over WiFi) mode. In a Wi-Fi connected mode, the OTCV iPhone application then operates as SIP device (see [Checking the licence](#) on page 122)

Note:

When the OTCV iPhone operates in dual-mode (Wi-Fi/cellular), the application automatically uses the enterprise Wi-Fi network (also called Wireless Local Area Network (WLAN)) for call handling (VoIP calls). If the Wi-Fi is not available, the cellular network is used for call handling.

- In all other contexts, the regular cellular network (2.5G, 3G, 3G+, 4G and GPRS) and PSTN network are used for voice communications.

The OTCV iPhone application relies on the following components:

- Instant Communications web services to access the different services; including:
 - Telephony
 - Universal Directory Access (UDA)
 - Business Call Log
 - Voice mails
- The Event Server (EVS), in charge of publishing device related events and notifications, such as alarms and configurations changes in the different user applications or services. OTCV iPhone application uses the HTTP(s) protocol to connect with the servers within the enterprise. Note that the server digital certificate of the OXO Connect must be installed in the OTCV iPhone application for server authentication, and enable HTTPS connection (see the **Certificate management** section in document [13]).

8.2.2 Access Provided from the WAN/Internet

In order to set the appropriate security measures and configuration rules for connecting OTCV iPhone from the WAN/Internet, please follow with care the recommendations in the section **Network configuration for remote accesses** in document [13].

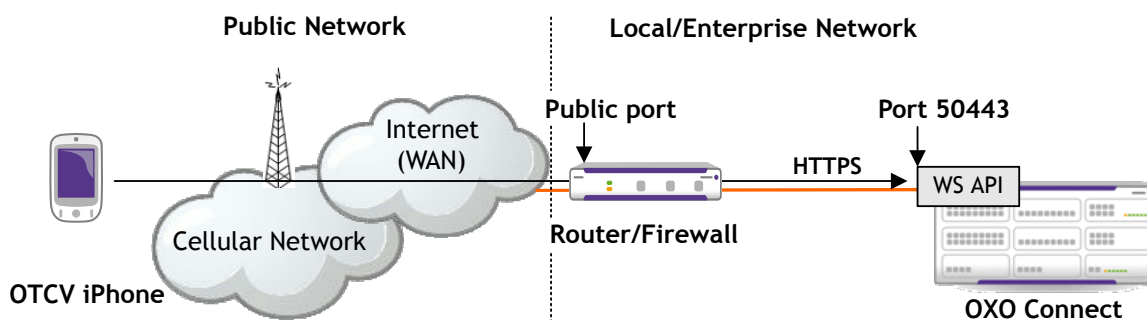


Figure 8.1: Data Transmission via a Router/Firewall

When connected from the WAN/Internet, the OTCV iPhone is seen as an external device of the enterprise network (distant access). In this configuration, the public URL of OXO Connect is used to connect. The public URL must be configured in the OXO Connect and entered in OTCV iPhone application at login.

The public URL consists of the public hostname/IP address, optionally the port (separated by colon), for example: `enterprise.loc:443`

For HTTPS connection, OTCV iPhone application must embed the authority certificate of OXO Connect server certificate. With such configuration, users are not warned that they use an HTTPS certificate issued from an unknown authority. This requires consistent DNS resolution from the outside or inside enterprise network. For more information about certificate management, see the **Certificate management** section in document [13].

8.2.3 SIP Mode

The SIP mode only occurs when the OTCV iPhone operates in dual-mode (Wi-Fi/cellular) within company premises.

The SIP mode feature adds VoIP capabilities to the OTCV iPhone application. Its embedded SIP client connects to OXO Connect through the Wi-Fi network of the enterprise. The voice and signaling (RTP and SIP) are carried over Wi-Fi (VoWi-Fi) instead of the cellular network. When the mobile is out of reach of the enterprise Wi-Fi network, it uses the cellular network for voice and data.

Following connectivity modes are supported:

- In the enterprise network coverage, OTCV iPhone application is connected to the OXO Connect by its private IP address with one of the following configurations:
 - Voice over IP and data over Wi-Fi network
 - Voice over cellular network and data over Wi-Fi network
- Outside of the enterprise network coverage, OTCV iPhone application is connected to the OXO Connect with one of the following configurations:
 - Voice and data over cellular network
 - Voice over cellular network and data over a Wi-Fi network (public or private) connecting to the Internet Access Device public IP address of OXO Connect

The operating mode VoWi-Fi or cellular is controlled by the OTCV iPhone application, based on the network connectivity available and the routing profile selected in the application settings (see: [Call Routing Profiles](#) on page 118).

The application switches the mobility destination to the mobile phone number when the **Mobility** profile is selected and the SIP option is set to off.

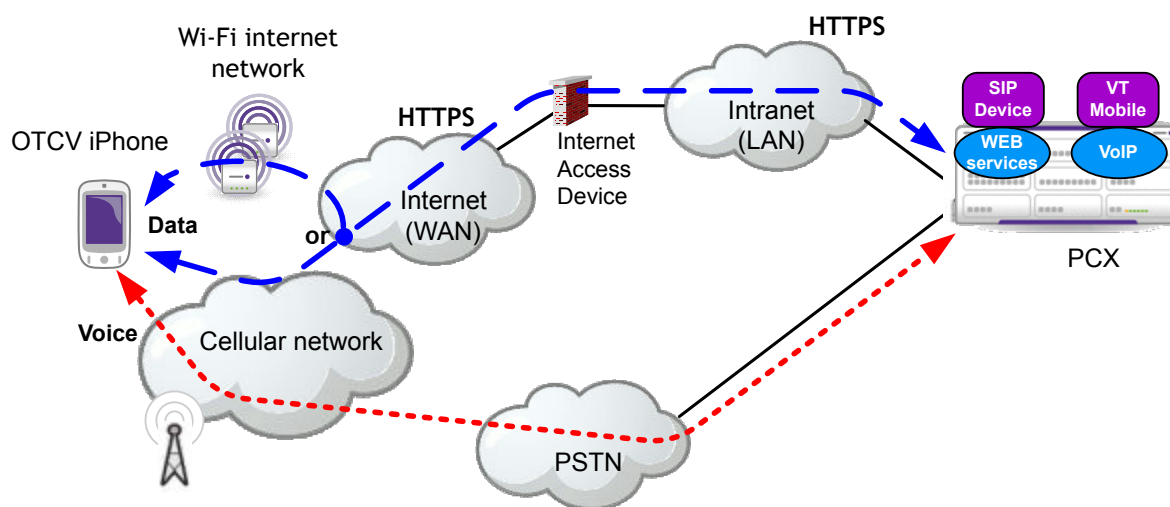


Figure 8.2: Off-site topology (cellular coverage)

The application switches the mobility destination to associated SIP Companion when the **Mobility** profile is selected and the SIP option is set to on.

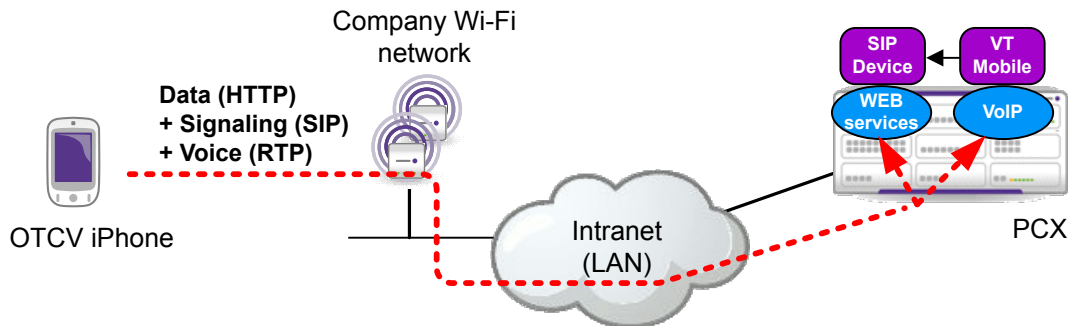


Figure 8.3: On-site topology (Wi-Fi coverage)

Note:

The PBX configuration of an OTCV iPhone in dual-mode requires, in addition to the mobile virtual terminal, the creation of a SIP Companion. The directory number and SIP password are transferred securely over HTTPS to the application, in a configuration file available after user authentication.

8.2.3.1 Wi-Fi Connection

OTCV iPhone supports Wi-Fi connection for web service requests (data channel usage). This uses the Wi-Fi network of the enterprise also called Wireless Local Area Network (WLAN). Engineering rules exist for WLAN infrastructure deployment. For more information, refer to: [WLAN Infrastructure for OpenTouch Conversation applications](#) on page 151).

Wi-Fi connection is used in priority if available (before cellular connection). The use of Wi-Fi network interface for data connection with API is based on iPhone platform connection capabilities. The iPhone OS provides automatic network connection to available interfaces and their monitoring through the Connectivity Manager.

Wi-Fi connection is also used to establish SIP connection with the OXO Connect. This SIP feature is only available when the user is connected to the Enterprise Wi-Fi.

The IP address provided to the OTCV iPhone connected to enterprise Wi-Fi must be routable by the OXO Connect. If this is not the case, problems can be encountered, such as no audio when calling, or no registration.

OTCV iPhone does not support NAT traversal over Wi-Fi.

Firewalls or Access Control Lists (ACL) that may exist between Wi-Fi and the LAN must not filter out SIP, RTP and HTTPS.

Automatic Wi-Fi connection is handled by the iPhone. The OTCV iPhone application does not embed any additional feature relating to connection management.

The OTCV iPhone does not handle the provisioning of Wi-Fi networks configuration: corporate networks are supposed to be configured using the Mobile Device Management solution (including all the necessary certificates), and any other Wi-Fi network must be configured by users themselves.

The user shall configure the wireless interface to ensure authentication and association on Wi-Fi access point (Certificate provisioning in case of 802.1x authentication, WPA-PSK or WEP key, ESSID of Wi-Fi network/access point).

Once connected, the iPhone Wireless Manager provides connection state management and notification functionality. Specifically, it can be used to obtain broadcast information when network connectivity changes and query the state of the available networks.

The iPhone Connectivity Manager automatically manages data routing between cellular and Wi-Fi accesses. It uses in priority the Wi-Fi connection for data routing. If the Wi-Fi connection disappears, it switches automatically to the next data network interface available (cellular); and vice versa when coming back under Wi-Fi coverage.

The user is able to deactivate manually the cellular or Wi-Fi data connection. In this case, he must reactivate the corresponding data channel before the mobile can use it properly.

8.2.3.2 Public and Private Domains

The OTCV iPhone can connect to the PBX through the enterprise Wi-Fi network or through the public network (3G, Home wireless,...). It uses both public and private URLs to target the OXO Connect PBX.

Private and public URLs are configured in the PBX and retrieved by the OTCV iPhone application. When accessing the PBX, the OTCV iPhone behaves as follow:

- The mobile always tries to use private URLs at first.
- If the connection fails using private URLs, the mobile uses public URLs. This happens when the mobile is connected to cellular network or to home/hot spot Wi-Fi networks.

When switching between public and private networks, the OTCV iPhone application handles automatically the switch between public and private URLs usage.

8.2.3.3 Restrictions

In case of network switching from cellular to Wi-Fi, OTCV iPhone is not notified immediately of the network switching, the application should be informed within 10 minutes (see Apple background mode restriction for this delay). During this transition, incoming calls are switched automatically by server to the GSM Number.

There is no call recovery in case of loss of Wi-Fi while in communication.

If the Wi-Fi is lost during call presentation (Ringing state) there is no automatic roaming and the call is redirected to the user voice mail.

8.3 Detailed description

8.3.1 Features Provided

The OTCV iPhone application provides on a mobile device, a subset of the features available from the user's desk phone.

Telephone features are the basic services supported by the OTCV iPhone. They are available only with full data connection. With full data connection (cellular network or WiFi network), services are activated through Web Services handled by the PBX (that is OXO Connect).

When the data channel is available, the services provided to the user by OTCV iPhone are:

- Application management:
 - Starting the application
 - Synchronize configuration
 - Configure the client management server URLs
 - Change password
 - Single ring mode
- Business communications (see: [Business Communications](#) on page 117):
 - Make an outgoing call
 - Dial by Name

- Dial By number
- Answer an incoming call
- Release a simple call
- Make a second call or another call
- Transfer the call
- Release the active call
- Put a call on hold
- Take the call on hold
- Dual-mode feature (using SIP companion)
- Three-party conference
- Call routing profiles (see: [Call Routing Profiles](#) on page 118)
- Directory services (see: [Directory Services](#) on page 119):
 - Search in directory
 - Display contact details
 - Send an e-mail to a contact
- Call log services (see: [Business Call Logs](#) on page 120):
 - Consult the call log
 - Delete the call log
 - Acknowledge a call log item
 - Delete a call log item
- Voice mail services (see: [Business Voice Mail](#) on page 120):
 - Consult voice mails
 - Play a voice mail
 - Remove a voice mail
 - Call back the message sender
- Instant Messaging services:
 - View the conversation list
 - Delete instant messages in a conversation
 - Send and receive instant messages
 - Delete conversations
 - Call the sender of instant messages
 - Decline an incoming call with an instant message

For more information on Instant Messaging services, refer to the **Instant Messaging** section in document [3].

8.3.2 Business Communications

The OTCV iPhone only manages business communications. Only incoming and outgoing call from the PBX are managed by the application. Private communications are out of its scope.

In the business context, communications are handled through the PBX (only when the data channel is available), ensuring rich telephonic features. The iPhone can receive and make business calls; but can also make private calls through the native iPhone application.

To leave the business context, the user must select the **Office** or **No mobility** routing profile (see: [Call Routing Profiles](#) on page 118). This means that no more business calls are received on the mobile.

Remarks:

- *Since the client cannot send DTMF codes, OTCV iPhone application does not support any fallback.*

- It is not possible to make a business outgoing call from the native dialer.
- A Business outgoing call must be set up from the OTCV iPhone application. The call is invoked through the web service with a recall from the Call Server.
- A Private outgoing call must be set up from the native iPhone application. The call does not go through the PBX.

8.3.3 Call Routing Profiles

When the OTCV iPhone application is launched from the iPhone, the user can configure the current routing profile for outgoing and incoming calls.

Two call routing profiles can be configured from the OTCV iPhone application:

- The **Office** profile: this call routing profile is only available when the OTCV iPhone is associated to one or more phone sets in a multi-set configuration. If there is no multi-set configuration, the **Office** profile is replaced by **No Mobility** on screen.

When the **Office** profile is selected, the user cannot handle calls from the OTCV iPhone. Call handling can only be performed from the other phone sets associated to the user.

Note:

In this configuration, the user can also forward incoming calls to voice mail or a preferred number (four numbers can be defined in the routing profile).

- The **Mobility** profile: the user can make calls from the OTCV iPhone and configure the destination to which incoming calls are routed. The destination number can be any of the following:
 - **My Mobile**: incoming calls are presented to the OTCV iPhone. If the user has one or more other phone sets (multi-set configuration), the application only rings for incoming business communications. Other associated phone sets do not ring. If configured in the OMC, their screen only indicate an immediate forward to the application name or directory number.

Note:

*At first OTCV iPhone connection, a pop-up window requests to enter a GSM number. When this is done, this mobile phone number is automatically associated to the **Mobility** profile.*

- **My Mobile and Office**: this option is only available when the OTCV iPhone is associated to one or more other phone sets in a multi-set configuration. Incoming calls are presented to all the devices associated to the user.
- **Forward to voice mail**: Incoming calls are forwarded to the user voice mail.
- **Forward to number**: Incoming calls are forwarded to a phone number, which is either a number previously configured in the OTCV iPhone or a phone number entered manually. Four predefined phone numbers can be entered in the OTCV iPhone.

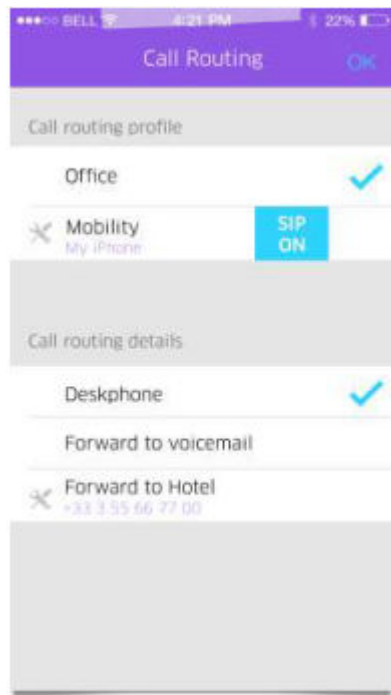
Note:

*When call forwarding information is not available (not retrieved at initialization, or when the data channel is not available), the home page displays **unknown** as phone set state.*

When the **Mobility** profile is selected, the OTCV iPhone can operate in cellular mode or dual-mode (Wi-Fi/cellular) within company premises. This is defined by the SIP option available when the **Mobility** profile is selected:

- SIP on: the OTCV iPhone can operate in dual-mode (Wi-Fi/cellular) within company premises. The OTCV iPhone uses by priority:
 - The Wi-Fi enterprise network (that is the WLAN)
 - The cellular network If the Wi-Fi is unavailable
- SIP off: the OTCV iPhone only uses the cellular network

Office profile screen example



Mobility profile screen example

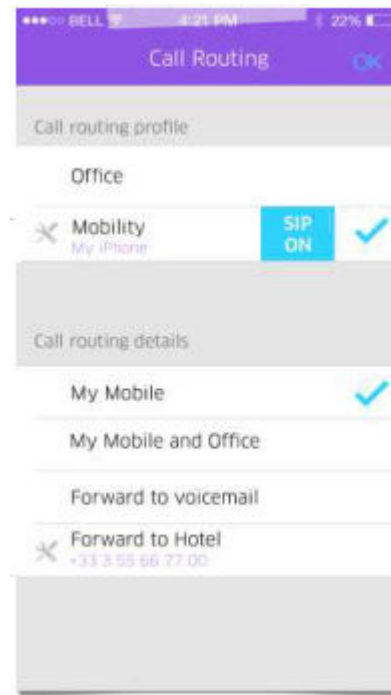


Figure 8.4: Routing profile screen overview

When call forwarding information is not available (not retrieved at initialization, or when the data channel is not available), the home page displays **unknown** as phone set state.

Note:

When OTCV iPhone is included in a multi-set, for external diversion to operate correctly, the External diversion right must be enabled for all phone sets of the multi-set.

8.3.4 Directory Services

OTCV iPhone handles several services related to business and local directories.

The contact detail page includes contact identity and provides detailed information about a contact, and lists the different ways the contact can be reached, depending on presence and media capabilities.

Identity information can include:

- The contact name
- The contact business and mobile phone numbers, home number or other number (if available)
- The contact e-mail address (if available)
- The contact photo (If available)

In some cases, phone numbers for outgoing calls must be preceded by an outgoing prefix. This occurs when the phone number (for an outgoing call) is entered manually or retrieved from business or local directories.

OTCV iPhone can add this prefix to the phone number, so that the PBX can establish the call.

Depending of the origin of the phone number, the following rules are applied:

- If the number comes from the OXO Connect phonebook, the number is used without modification to make the call
- If the number comes from a call log or a voice mail, the number is used without modification to make the call
- If the phone number comes from the LDAP directory, OTCV iPhone automatically adds the prefix and makes the call

Note:

It is recommended to have phone numbers registered in canonical form in the LDAP directory.

- If the user enters a phone number manually, OTCV iPhone automatically adds the prefix and make the call
- If the number comes from the iPhone local contact, OTCV iPhone automatically adds the prefix and makes the call

8.3.5 Business Call Logs

The Business Call Log contains call log items related to the user. It includes:

- Caller details
- Date and time information

It concerns all events related to **One Number Services**.

The user call log is managed by the PBX. It is limited by the PBX call log limit. To optimize response time and data channel consumption, OTCV iPhone limits the download to the fifty most recent call log items.

Call log lists are displayed when an appropriate data channel is available. When there is no data channel, lists are not available.

8.3.6 Business Voice Mail

OTCV iPhone handles several services related to business voice mails. Voice mails are displayed in a specific menu and can be selected individually.

The selected voice mail is downloaded from the OXO Connect on a specific URL and played on the iPhone speaker. Information about each voice mail includes:

- Caller phone number
- Caller name
- Voice mail date

Actions that can be taken for message include:

- Listen to a voice mail
- Delete a voice mail
- Call the person who left the voice mail
- Activate/disable the speaker

Voice mail list consultation and voice mail play are available when data coverage (WiFi or 3G/3G+) is implemented.

Note:

OTCV iPhone does not work without voice mail. By default, a voice mail is created for OTCV iPhone

It is not recommended to delete the voice mail of the OTCV iPhone or the voice mail of its associated set in multi-set configuration.

8.3.7 Collaboration Services

OTCV iPhone application does not support any collaboration services.

8.3.8 Ring tones

OTCV iPhone provides different ring tones for incoming calls. From the application settings, users can perform any of the following:

- Change the default ring tone
- Select different ring tones to identify the type of incoming calls (internal or external)

Users cannot use the ring tones provided by the iPhone, and they cannot add their own ring tones in the OTCV iPhone settings.

Note:

When the OTCV iPhone operates in dual-mode (Wi-Fi/cellular), the SIP companion ringing tone is different from the iPhone selected ringing tone for incoming calls. No option is available to modify the SIP companion ringing tone and make it identical to the iPhone incoming call ringing tone.

8.4 Configuration procedure

8.4.1 Checking the license

In the OMC tool, the creation of an OTCV iPhone application is refused when the number of such applications has reached the maximum value indicated by the present license.

To verify the license:

1. From the OMC tool, navigate to the menu: **Modification Typical > System > Software key**
2. Click **Details**
3. In the **Voice Communication (Continued)** tab, check that the option **My IC Mobile users** is enabled (the maximum value is 50)

8.4.2 Checking the VoIP protocol

To use OTCV iPhone, you must verify that the VoIP protocol is set to SIP in the OXO Connect configuration.

To check, and, if necessary, modify the VoIP protocol:

1. From the OMC tool, navigate to: **Voice over IP > VoIP: Parameters**
2. Click the **General** tab and verify that the **VoIP Protocol** parameter is set to **SIP**

8.4.3 Declaring the OTCV iPhone

The OTCV iPhone application must be declared in the OXO Connect using OMC. The OTCV iPhone applications are created in the OXO Connect regardless of the mobile type on which the applications must run (there is no hardware link between the mobile device and the OXO Connect). This simplifies OTCV iPhone declaration, as the mobile device IMEI or MAC address is not necessary.

To declare an OTCV iPhone:

1. From the OMC tool, navigate to the screen **Subscribers/Basestations List** and click **Add**.

This displays the **Add User** screen.

2. Select the **My IC Mobile** check box
3. Select the number of application to create (default: 1)
4. Keep the proposed directory number for the application or select another free number

5. Click **OK** to validate

The My IC Mobile is displayed in the list of subscribers

6. In the **Details** tab, click **Cent Serv.**
7. Check the **Nomadic Right** box
8. Click **OK** to validate
9. Click **OK** to leave the **Details** tab

This operation automatically creates a configuration file on the OXO Connect required for OTCV iPhone commissioning. The configuration file is identified by the directory number specified at OTCV iPhone declaration. The configuration file is named: `MOBILE_<application directory number>@OXO Connect private FQDN.xml`. At first startup, the application automatically downloads its configuration file using the OXO Connect URLs and the credentials entered by the user.

Notes:

- OTCV iPhone does not work without voice mail. By default, a voice mail is created for OTCV iPhone then it is not recommended to delete the voice mail of the OTCV iPhone or the voice mail of its associated set in multi-set configuration.
- The user is required to allow microphone access for the OTCV iPhone application. For more details, see [Microphone access](#) on page 123.

8.4.4 Configuring the dual-mode (Wi-Fi/Cellular)

To enable the dual-mode (Wi-Fi/Cellular) on OTCV iPhone, the following steps are mandatory:

- Checking the licence, see [Checking the licence](#) on page 122
- Creating a SIP Companion, see [Creating a SIP Companion](#) on page 122
- Associating a SIP companion to an iPhone, see [Associating a SIP Companion to an OTCV iPhone](#) on page 123

8.4.4.1 Checking the licence

The number of OpenTouch Conversation users allowed to use the dual-mode is controlled by a software license. This license controls the number of SIP companions. If the maximum number of SIP companions is reached, the creation of a new one is refused.

To verify the dual-mode license:

1. In OMC, navigate to **Hardware and Limits > System Software key > System Software key**
2. Click **Details**
3. In the **Voice Communication (continued)** tab, check that the option **SIP Companions** is enabled (the maximum value is 50)

8.4.4.2 Creating a SIP Companion

To create a SIP companion:

1. In OMC, navigate to the screen **Subscribers/Basestations List** and click **Add**.

This displays the Add Subscriber screen.

2. Select the **SIP Companion** check box and click **OK** to validate

Note:

*This choice is not proposed if **SIP Companions** license is not present or if the maximum number of SIP companions that can be created has been reached.*

3. Click the **Modify** button.

8.4.4.3 Associating a SIP Companion to an OTCV iPhone

1. In OMC, navigate to the screen **Subscribers/Basestations List** and select in the list the OTCV iPhone on which dual-mode has to be activated.
2. Click the **Details** button
The OTCV iPhone parameters page is displayed
3. Click the **Mobility** button.
The **Mobility** page is displayed
4. In the **SIP Companion** drop list, select the previous created SIP companion.

Note:

*If the dual-mode is already activated, the associated SIP Companion number is shown in the list. If the dual-mode is not activated, the value **None** is displayed and all available SIP Companions are proposed in the list.*

5. Click **OK** to validate

Note:

*In the **Call Routing** page of OTCV iPhone, the SIP ON/OFF button in front of the **Mobility** profile indicates whether the dual-mode feature is enabled or not for this OTCV iPhone. In fact, this box allows to deactivate temporarily the dual-mode feature on the current mobile. This information can be modified only if a SIP companion has been selected in the list. At the first selection of a SIP companion, the dual-mode feature is enabled by default, so this box checked.*

8.4.5 Associating a desk phone to the OTCV iPhone

The OTCV iPhone application can be associated to the user desk phone or can be used as standalone. The association with desk phone is achieved with the multi-set feature available in the OXO Connect (see: [3] Multi-sets).

8.4.6 Microphone access

With iOS 8 and 9, Apple enforced security about access to microphone of the iPhone.

If an application attempts to access the microphone of the iPhone, the user is automatically prompted at first access to allow the application to use the microphone.

OTCV iPhone requests the microphone for VoIP calls. With the first incoming or outgoing VoIP call, a pop-up requests to allow access.

This setting can be modified in the iPhone Settings, in the **Privacy** menu, **Microphone** section.

8.5 Operation

8.5.1 Loading the Application from the iPhone AppStore

Standard installation procedures are applied through iTunes or the AppStore.

To download the application from the iPhone AppStore, use any of the following keywords to find the application:

- OpenTouch
- Conversation
- SMB
- Phone
- Messaging
- Collaboration
- Communication

- Mobility
- Call
- Voice
- Alcatel-Lucent

Note:

The complete name of the application is: Alcatel-Lucent Enterprise OpenTouch Conversation for iPhone.

8.5.2 Configuring Server Settings to Access the OXO Connect

The user must enter the private or public URL to access the OXO Connect. OTCV iPhone automatically downloads configuration files after confirmation.

Note:

If the private URL is entered while connecting to a public network (3G, home/hotspot wireless) and in some cases, if the public URL is entered in the enterprise network, download can fail, and the user must modify the URL by using the URL configuration screen.

8.5.3 Configuration File Deployment

The application automatically downloads the configuration files, whatever the network topology (LAN and WAN). At the first launch of the application, users are prompted to enter their credentials to allow the download of the configuration files. If users do not enter their credentials when requested, the application does not start.

8.5.4 Initialization Process

The application can be started using iPhone platform facilities.

During initialization, the application performs the following operations:

1. Connection procedure. Depending on local settings, connection can start automatically or after user confirmation.
2. If the connection URL is empty or invalid, the user is prompted to enter a valid URL .
3. It synchronizes configuration with the Client Management server.
4. After configuration, the application starts connecting to the Instant Communications infrastructure. It receives Instant Communications connection parameters and downloads the different Web Services URLs.

All available services are started using URL parameters.

5. The device attempts to log the user to the Instant Communications server.

During these operations, the user may be prompted for credentials using the appropriate login.

6. When the iPhone is logged into Instant Communications, the application downloads the necessary initial information using appropriate web services: framework account information and rights, user's profile dialing rules, etc.
7. The application displays the **Home page**.

This can be configured by the user.

8. The application downloads the current phone state/call forwarding settings, number of unanswered calls and voice mails, and updates the home screen.

Remark:

Standard iPhone application update procedures are applied through iTunes or the AppStore.

9.1 Overview

9.1.1 Introduction

OpenTouch Conversation® for Android (also called OTCV Android) is a software client application running on a mobile phone using the Android Operating System. It provides an access to enterprise telephone services over a mobile Internet access or WiFi network, so that the Android phone operates as a business phone.

OTCV Android provides access to business telephone features. In addition to the ordinary business telephony access, OTCV Android provides data connection to:

- Business directory
- Business call logs
- Business voice mail

OTCV Android:

- Interacts with native Android applications to enrich communication services (local contacts)
- Can be used in remote locations, e.g. via Internet, to have access to the same level of services as in the Enterprise premises (See [13] chapter: Network configuration for remote accesses, for detailed information about network configuration from Internet/WAN)
- Can be associated to a deskphone (call routing profile configuration) or can operate as unique user telephone device

For information about the list of compatible devices and OS versions, see the Technical Communication TC1637, available from the Enterprise Business Portal (reference name: MIC_UC_Client_DeviceWhiteList_8AL90822AAAA).

Note:

Data connection is dependent on network availability. OTCV Android cannot handle any fallback mode or business services when the data connection is not available.

9.2 Architecture

9.2.1 Overview

This module presents the network topologies to access the PBX services from an OTCV Android application.

For data communication, the OTCV Android accesses the PBX services using OmniTouch 8400 ICS web services implemented in the PBX (that is OXO Connect). It requires either one of these network connectivities:

- The enterprise Wi-Fi network inside the enterprise

Note:

A Wi-Fi Internet access or hot spot can be used at home for data transmission.

- An Internet/data connection provided by some cellular networks (2.5G, 3G, 3G+, 4G and GPRS) outside the enterprise. See the section **Network configuration for remote accesses** in document [13] for detailed information about network configuration from Internet/WAN

For voice communication:

- If the OTCV Android application is connected to the enterprise Wi-Fi network inside the enterprise, it is possible to use the VoWiFi (Voice over IP over WiFi) mode. In a Wi-Fi connected mode, the OTCV Android application then operates as SIP device (see [SIP Mode](#) on page 127)

Note:

When the OTCV Android operates in dual-mode (Wi-Fi/cellular), the application automatically uses the enterprise Wi-Fi network (also called Wireless Local Area Network (WLAN)) for call handling (VoIP calls). If the Wi-Fi is not available, the cellular network is used for call handling.

- In all other contexts, the regular cellular network (2.5G, 3G, 3G+, 4G and GPRS) and PSTN network are used for voice communications.

The OTCV Android application relies on the following components:

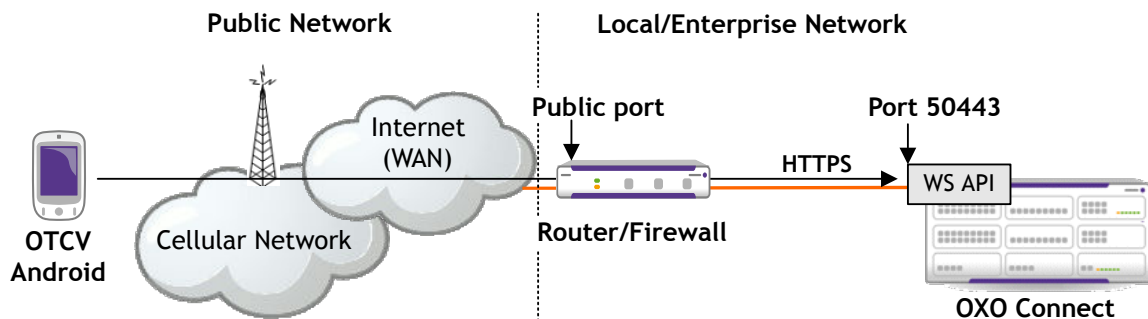
- Instant Communications web services to access the different services; including:
 - Telephony
 - Universal Directory Access (UDA)
 - Business Call Log
 - Voice mails
- The Event Server (EVS), in charge of publishing device related events and notifications, such as alarms and configurations changes in the different user applications or services. OTCV Android application uses the HTTP(s) protocol to connect with the servers within the enterprise. Note that the server digital certificate of the OXO Connect must be installed in the OTCV Android application for server authentication, and enable HTTPS connection (see the **Certificate management** section in document [13]).

9.2.2 Access Provided from the WAN/Internet

In order to set the appropriate security measures and configuration rules for connecting OTCV Android from the WAN/Internet, please follow with care the recommendations in the section **Network configuration for remote accesses** in document [13].

When connected from the WAN/Internet, the OTCV Android is seen as an external device of the enterprise network (distant access). In this configuration, the public URL of OXO Connect is used to connect. The public URL must be configured in the OXO Connect and entered in OTCV Android application at login.

The public URL consists of the public hostname/IP address, optionally the port (separated by colon), for example: `enterprise.loc:443`



For HTTPS connection, OTCV Android application must embed the authority certificate of OXO Connect server certificate. With such configuration, users are not warned that they use an HTTPS certificate issued from an unknown authority. This requires consistent DNS resolution from the outside or inside enterprise network. For more information about certificate management, see the section **Network configuration for remote accesses** in document [13].

9.2.3 SIP Mode

The SIP mode only occurs when the OTCV Android operates in dual-mode (Wi-Fi/cellular) within company premises.

The SIP mode feature adds VoIP capabilities to the OTCV Android application. Its embedded SIP client connects to OXO Connect through the Wi-Fi network of the enterprise. The voice and signaling (RTP and SIP) are carried over Wi-Fi (VoWi-Fi) instead of the cellular network. When the mobile is out of reach of the enterprise Wi-Fi network, it uses the cellular network for voice and data.

Following connectivity modes are supported:

- In the enterprise network coverage, OTCV Android application is connected to the OXO Connect by its private IP address with one of the following configurations:
 - Voice over IP and data over Wi-Fi network
 - Voice over cellular network and data over Wi-Fi network
- Outside of the enterprise network coverage, OTCV Android application is connected to the OXO Connect with one of the following configurations:
 - Voice and data over cellular network
 - Voice over cellular network and data over a Wi-Fi network (public or private) connecting to the Internet Access Device public IP address of OXO Connect

The operating mode VoWi-Fi or cellular is controlled by the OTCV Android application, based on the network connectivity available and the routing profile selected in the application settings (see: [Dual mode Wi-Fi/cellular](#) on page 130).

The application switches the mobility destination to the mobile phone number when the **Mobility** profile is selected and the SIP option is set to off.

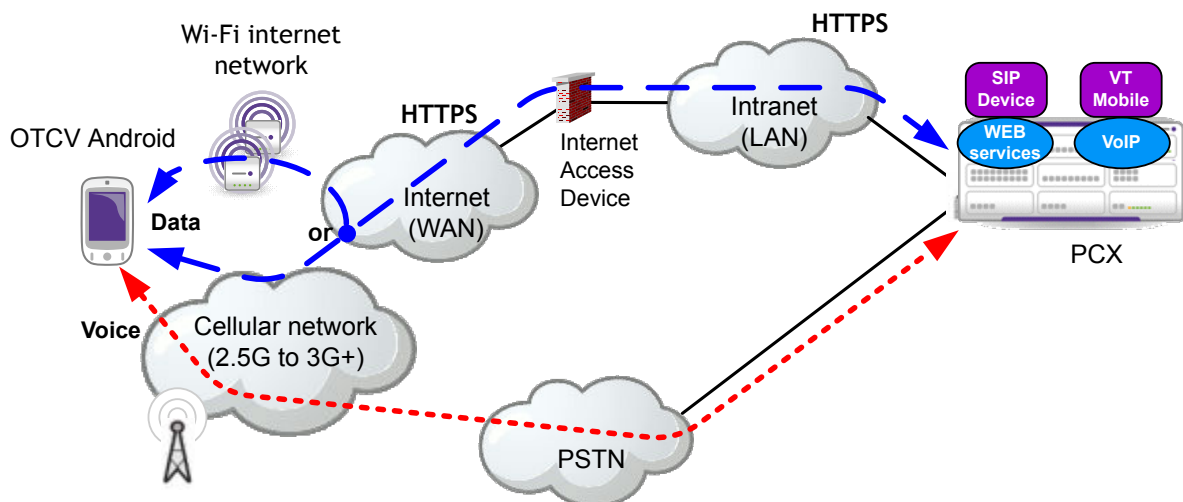


Figure 9.1: Off-site topology (cellular coverage)

The application switches the mobility destination to associated SIP Companion when the Mobility profile is selected and the SIP option is set to on.

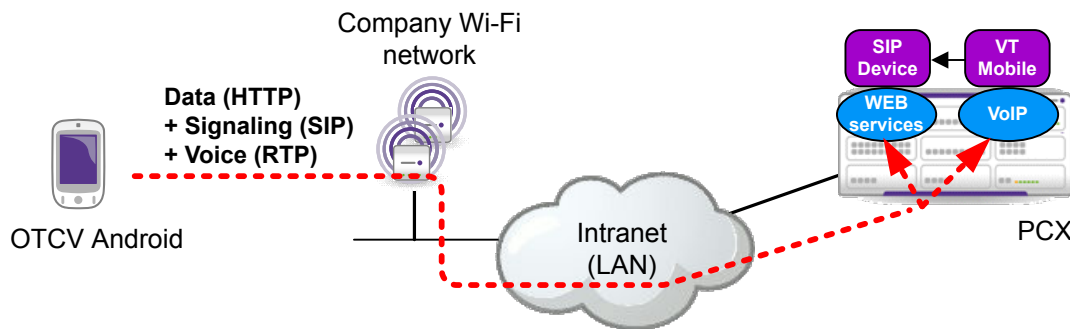


Figure 9.2: On-site topology (Wi-Fi coverage)

Note:

The PBX configuration of an OTCV Android in dual-mode requires, in addition to the mobile virtual terminal, the creation of a SIP Companion. The directory number and SIP password are transferred securely over HTTPS to the application, in a configuration file available after user authentication.

9.2.3.1 Wi-Fi Connection

OTCV Android supports Wi-Fi connection for web service requests (data channel usage). This uses the Wi-Fi network of the enterprise also called Wireless Local Area Network (WLAN). Engineering rules exist for WLAN infrastructure deployment. For more information, see [WLAN Infrastructure for OpenTouch Conversation applications](#) on page 151.

Wi-Fi connection is used in priority if available (before cellular connection). The use of Wi-Fi network interface for data connection with API is based on Android platform connection capabilities. The Android OS provides automatic network connection to available interfaces and their monitoring through the Connectivity Manager.

Wi-Fi connection is also used to establish SIP connection with the OXO Connect. This SIP feature is only available when the user is connected to the Enterprise Wi-Fi.

The IP address provided to the OTCV Android connected to enterprise Wi-Fi must be accessible by the OXO Connect. If this is not the case, problems can be encountered, such as no audio when calling, or no registration.

OTCV Android does not support NAT traversal over Wi-Fi.

Firewalls or Access Control Lists (ACL) that may exist between Wi-Fi and the LAN must not filter out SIP, RTP and HTTPS. Automatic Wi-Fi connection is handled by the Android. The OTCV Android application does not embed any additional feature relating to connection management.

The OTCV Android does not handle the provisioning of Wi-Fi networks configuration: corporate networks are supposed to be configured using the Mobile Device Management solution (including all the necessary certificates), and any other Wi-Fi network must be configured by users themselves.

The user shall configure the wireless interface to ensure authentication and association on Wi-Fi access point (Certificate provisioning in case of 802.1x authentication, WPA-PSK or WEP key, ESSID of Wi-Fi network/access point).

Once connected, the Android Wireless Manager provides connection state management and notification functionality. Specifically, it can be used to obtain broadcast information when network connectivity changes and query the state of the available networks.

The Android Connectivity Manager automatically manages data routing between cellular and Wi-Fi accesses. It uses in priority the Wi-Fi connection for data routing. If the Wi-Fi connection disappears, it switches automatically to the next data network interface available (cellular); and vice versa when coming back under Wi-Fi coverage.

The user is able to deactivate manually the cellular or Wi-Fi data connection. In this case, he/she must reactivate the corresponding data channel before the mobile can use it properly.

9.2.3.2 Public and Private Domains

The OTCV Android can connect to the PBX through the enterprise Wi-Fi network or through the public network (3G, Home wireless,...). It uses both public and private URLs to target the OXO Connect PBX.

Private and public URLs are configured in the PBX and retrieved by the OTCV Android application. When accessing the PBX, the OTCV Android behaves as follow:

- The mobile always tries to use private URLs at first
- If the connection fails using private URLs, the mobile uses public URLs. This happens when the mobile is connected to cellular network or to home/hot spot Wi-Fi networks

When switching between public and private networks, the OTCV Android application handles automatically the switch between public and private URLs usage.

9.3 Detailed description

9.3.1 Main Features

The OTCV Android application provides a subset of the features available from the user's deskphone on a mobile phone.

Telephone features are the basic services supported by OTCV Android. They are available only with full data connection. With full data connection (cellular network or WiFi network), services are activated through Web Services handled by the OXO Connect.

When the data channel is available, the services provided to the user by OTCV Android are:

- Application management:
 - Start the application
 - Synchronize configuration
 - Configure the client management server URLs
 - Restrict ringing to incoming business communications
- Business communications (see: [Business Communications](#) on page 130):
 - Make an outgoing call
 - Dial by Name
 - Dial By number
 - Answer an incoming call
 - Release a simple call
 - Make a second call
 - Transfer the call
 - Release the active call
 - Put a call on hold
 - Take the call on hold
 - Three-party conference
- Dual-mode connectivity: cellular and Wi-Fi (see: [Dual mode Wi-Fi/cellular](#) on page 130)
- Call routing profiles (see: [Call routing Profiles](#) on page 131)
- Directory services (see: [Directory Services](#) on page 133):
 - Search in the directory
 - Display contact details

- Send an e-mail to a contact
- Send an SMS
- Call log services (see: [Business Call Logs](#) on page 134):
 - Consult the call log
 - Delete the call log
 - Acknowledge a call log item
 - Delete a call log item
- Voice mail services (see: [Business Voice Mail](#) on page 134):
 - Consult voice mails
 - Play a voice mail
 - Remove a voice mail
 - Call back the message sender
- Instant Messaging services
 - View the conversation list
 - Delete instant messages in a conversation
 - Send and receive instant messages
 - Delete conversations
 - Call the sender of instant messages
 - Decline an incoming call with an instant message

For more information on Instant Messaging services, refer to the **Instant Messaging** section in document [3].

9.3.2 Business Communications

Private communications are out of the scope of OTCV Android. It only manages business communications, consisting in incoming and outgoing call from the PBX.

In a business context, communications are handled through the PBX (provided the data channel is available), ensuring rich telephone features. The mobile device can receive and make business calls; but can also make private calls through the native mobile device application.

To leave the business context, the user selects the **Office** or **No mobility** routing profile (see: [Call routing Profiles](#) on page 131). This means that no more business calls are received on the mobile.

When the user initiates an outgoing call from a native application while OTCV Android is running, the call is intercepted by OTCV Android and the user is prompted to choose to make a business or a private call. If OTCV Android is not started, the call is made as a private call.

Notes:

Since the client cannot send DTMF codes, OTCV Android does not support any fallback.

9.3.3 Dual mode Wi-Fi/cellular

Within company premises, OTCV Android can operate in cellular mode or dual-mode (Wi-Fi/cellular) provided that:

- The dual-mode has been configured on the OXO Connect. This consists in creating and associating SIP companions to OTCV Android applications (see: [Configuring the dual-mode \(Wi-Fi/Cellular\)](#) on page 136)
- The user has selected the **Mobility** profile (with the SIP option activated) in the OTCV Android settings (see: [Call routing Profiles](#) on page 131)

In dual-mode, the OTCV Android automatically uses the Wi-Fi enterprise network (that is the WLAN) for call handling (VoIP calls). If the Wi-Fi is not available, the cellular network is used for call handling.

The OTCV Android application can also switch manually between Wi-Fi and cellular networks. The OTCV Android relies on the mobile device platform for the data bearer choice.

When the dual-mode is active and the mobile device roams:

- From the cellular network to the Wi-Fi:
 - If the mobile device is idle (no call in progress), the OTCV Android automatically detects that the mobile device is in a Wi-Fi coverage area and performs a SIP registration on the PBX. After registration, the OTCV Android handles incoming and outgoing calls over the Wi-Fi as it would handle VoIP calls
 - If the mobile device is in communication (cellular call), the communication remains on the cellular network (no handover). When the communication is released, the OTCV Android application performs a SIP registration on the PBX. After registration, the OTCV Android application handles incoming and outgoing calls over the Wi-Fi as it would handle VoIP calls

Note:

In the Wi-Fi coverage, users can handle private calls (incoming/outgoing) from their mobile device via the cellular network, even if the mobile device is registered as SIP device in the PBX and uses the Wi-Fi to handle business calls. While in communication, two situations can occur:

- The user is in business communication and receives a private call: he/she takes the private call. The current business call is put on hold. When the private call is released, the business call on hold is resumed

While in business communication, the user cannot make a private call. Dialing the directory number results in an error message.

- The user is in private communication and receives a business call: he/she cannot take the business call. The business call is directly routed to the user voice mail and the call is seen as missed call

While in private communication, the user cannot make a business call. Dialing the directory number results in an error message.

- From the Wi-Fi network to the cellular network:
 - If the mobile device is idle (no call in progress), the OTCV Android relies on the platform features to select the 3G as a data bearer and all subsequent calls are made using the cellular network
 - If the mobile device is in communication (VoIP call), the user can manually switch the communication to the cellular network without interruption of the communication (seamless handover). The communication is then processed by the cellular network. When the communication is released, the OTCV Android handles incoming and outgoing calls over the cellular network

9.3.4 Call routing Profiles

When the OTCV Android application is launched from the mobile device, the user can configure the current routing profile for outgoing and incoming calls.

Three call routing profiles can be configured from the OTCV Android application:

- The **Office** profile: this call routing profile is only available when the OTCV Android is associated to one or more phone sets in a multi-set configuration. If there is no multi-set configuration, the **Office** profile is replaced by **No Mobility** on screen.

When the **Office** profile is selected, the user cannot handle calls from the OTCV Android. Call handling can only be performed from the other phone sets associated to the user.

Note:

In this configuration, the user can also forward incoming calls to voice mail or a preferred number (four numbers can be defined in the routing profile).

- The **Mobility** profile: the OTCV Android only uses the cellular network within company premises. In this configuration, the OTCV Android application sets the Nomadic mode to the cellular phone number (without any fallback number)
- The **Mobility with SIP** profile: the OTCV Android can operate in dual-mode (Wi-Fi/cellular) within company premises. In this configuration, the OTCV Android application sets the Nomadic mode to the OXO Connect SIP username with cellular phone number as fallback number. The OTCV Android uses by priority:
 - The Wi-Fi enterprise network (that is the WLAN)
 - The cellular network if the Wi-Fi is unavailable

When the **Mobility** or **Mobility with SIP** profile is selected, the user can make calls from the OTCV Android and configure the destination to which incoming calls are routed. The destination can be any of the following:

- **Mobility number**: incoming calls are presented to the OTCV Android. If the user has one or more phone sets (multi-set configuration), the application only rings for incoming business communications. Other associated phone sets do not ring. If configured in the OMC, their screen only indicate an immediate forward to the application name or directory number.

Note:

*At first OTCV Android connection, a pop-up window requests to enter a GSM number. When this is done, the mobile phone number is automatically associated to the **Mobility** profile.*

- **Mobility number and Office phone**: this option is only available when the OTCV Android is associated to one or other phone sets in a multi-set configuration. Incoming calls are presented to all devices associated to the user.
- **Forward to number**: Incoming calls are forwarded to a phone number, which is either a number previously configured in the OTCV Android or a phone number entered manually. Four predefined phone numbers can be entered in the OTCV Android.

Note:

*When call forwarding information is not available (not retrieved at initialization, or when the data channel is not available), the home page displays **unknown** as phone set state.*

- **Forward to voicemail**: Incoming calls are forwarded to the user voice mail.

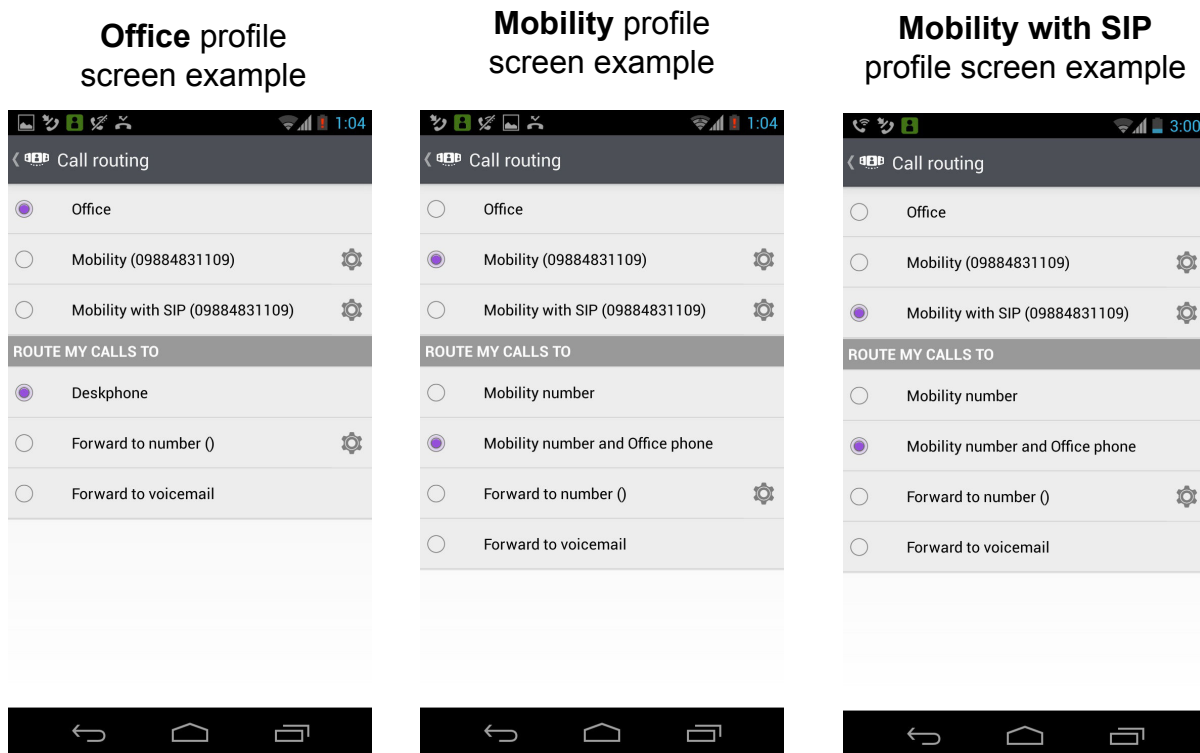


Figure 9.3: Routing profile screen overview

When call forwarding information is not available (not retrieved at initialization, or when the data channel is not available), the home page displays **unknown** as phone set state.

Note:

When OTCV Android is included in a multiset, for external diversion to operate correctly, the **External diversion** right must be enabled for all sets of the multiset.

9.3.5 Directory Services

OTCV Android handles several services related to business and local directories.

OTCV Android automatically launches a search when users enter more than two characters and use the **Search** button.

The contact detail page includes contact identity and provides detailed information about a contact, and lists the different ways the contact can be reached.

Identity information can include:

- Full name (last name and first name)
- Phone numbers
- e-mail address

In some cases, phone numbers for outgoing calls must be preceded by an outgoing prefix. This occurs when the phone number (for an outgoing call) is entered manually or retrieved from business or local directories.

OTCV Android can add this prefix to the phone number, so that the PBX can establish the call.

Depending on the origin of the phone number, the following rules are applied to make the call:

- The number is used without modification:
 - When the number comes from the OTCV Android phonebook

- When the number comes from a call log or a voice mail
- When the phone number comes from the LDAP directory

Note:

It is recommended to have phone numbers registered in canonical form in the LDAP directory.

- OTCV Android automatically adds the prefix before making the call:
 - When the number comes from the mobile device local contact list
 - When the user enters a phone number manually, provided this number does not contain the external outgoing prefix

9.3.6 Business Call Logs

The Business call log contains call log items related to the user. It includes:

- Caller details
- Date and time information

It concerns all events related to **One Number Services**.

The user call log is managed by the PBX. It is limited by the PBX call log limit. To optimize response time and data channel consumption,OTCV Android limits download to the fifty most recent call log items.

Call log lists are updated when an appropriate data channel is available. When there is no data channel, lists are not updated.

9.3.7 Business Voice Mail

OTCV Android handles several services related to business voice mails. Voice mails are displayed in a specific menu and can be selected individually.

The PBX starts a GSM call to OTCV Android to play a voice mail.

Information about each voice mail includes:

- Caller phone number
- Caller name
- Voice mail date/time and duration

Actions that can be taken for messages include:

- Listen to a voice mail
- Go to next/go to previous voice mail
- Pause
- Delete a voice mail
- Call the person who left the voice mail
- Activate/disable the speaker

Voice mail list consultation and voice mail play are available when data coverage (WiFi or 3G/3G+) is implemented.

9.3.8 Collaboration Services

OTCV Android does not support collaboration services.

9.3.9 Limitations

On some devices, the Android mute API does not operate: the API can be called and returns a success code, but the microphone is not muted. For this reason, the mute/unmute actions are not available/ displayed on Samsung and Motorola devices.

[Table 1](#) indicates the devices affected by this limitation.

table 9.1: Mute device examples

Device	Mute	Loudspeaker
HTC Desire	OK	OK
Samsung Galaxy S	disabled	OK
Google Nexus One	OK	OK
Motorola Defy	disabled	OK
Google Nexus S	disabled	OK
Samsung Galaxy S2	disabled	OK
Samsung Galaxy S3/S3 mini/S4	OK	OK
Samsung Galaxy Note 2/3	OK	OK
HTC sensation	OK	OK

9.4 Configuration procedure

9.4.1 Checking the license

In the OMC tool, the creation of an OTCV Android application is refused when the number of such applications has reached the maximum value indicated by the license.

To verify the license

1. From the OMC tool, navigate to: **Modification Typical > System > Software key**
2. Click **Details**
3. In the **Voice Communication** tab, check that the option **My IC Mobile users** is enabled (the maximum value is 50)

9.4.2 Checking the VoIP protocol

To use OTCV Android, you must verify that the VoIP protocol is set to SIP in the OXO Connect configuration.

To check, and, if necessary, modify the VoIP protocol:

1. From the OMC tool, navigate to: **Voice over IP > VoIP: Parameters**
2. Click the **General** tab and verify that the **VoIP Protocol** parameter is set to **SIP**

9.4.3 Declaring the OTCV Android

The OTCV Android application must be declared in the OXO Connect, using OMC. The OTCV Android applications are created in the OXO Connect regardless of the mobile type on which the applications must run (there is no hardware link between the mobile device and the OXO Connect). This simplifies OTCV Android declaration, as the mobile device IMEI or MAC address is not necessary.

To declare an OTCV Android:

1. From the OMC tool, navigate to: **Subscribers/Basestations List** and click **Add**

This displays the **Add User** screen.

2. Select the **My IC Mobile** check box
3. Select the number of application to create (default: 1)
4. Keep the proposed directory number for the application or select another free number
5. Click **OK** to validate

The My IC Mobile is displayed in the list of subscribers

6. In the **Details** tab, click **Cent Serv**.
7. Validate the **Nomadic Right** check box to allow the OTCV Android to operate in dual-mode (Wi-Fi/cellular) within company premises
8. Click **OK** to validate
9. Click **OK** to leave the **Details** tab

This operation automatically creates a configuration file on the OXO Connect required for OTCV Android commissioning. The configuration file is identified by the directory number specified at OTCV Android declaration. The configuration file is named: `MOBILE_<application directory number>@server private FQDN.xml`. At first startup, the application automatically downloads its configuration file using the OXO Connect URLs and the credentials entered by the user.

9.4.4 Configuring the dual-mode (Wi-Fi/Cellular)

To enable the dual-mode (Wi-Fi/Cellular) on OTCV Android, the following steps are mandatory:

- Checking the licence, see [Checking the licence](#) on page 136
- Creating a SIP Companion, see [Creating a SIP Companion](#) on page 136
- Associating a SIP companion to a mobile device, see [Associating a SIP Companion to an OTCV Android](#) on page 137

9.4.4.1 Checking the licence

The number of OpenTouch Conversation users allowed to use the dual-mode is controlled by a software license. This license controls the number of SIP companions. If the maximum number of SIP companions is reached, the creation of a new one is refused.

To verify the dual-mode license:

1. In OMC, navigate to **Hardware and Limits > System Software key > System Software key**
2. Click **Details**
3. In the **Voice Communication (continued)** tab, check that the option **SIP Companions** is enabled (the maximum value is 50)

9.4.4.2 Creating a SIP Companion

To create a SIP companion:

1. In OMC, navigate to the screen **Subscribers/Basestations List** and click **Add**.

This displays the Add Subscriber screen.

2. Select the **IP terminal** check box and click **OK** to validate

The new IP terminal is displayed in the list of subscribers

3. In the list, select the newly created IP terminal and select **SIP Companion** in the **Terminal/Basestat.** combo box

Note:

*This choice is not proposed if **SIP Companions** license is not present or if the maximum number of SIP companions that can be created has been reached.*

4. Click the **Modify** button.

9.4.4.3 Associating a SIP Companion to an OTCV Android

1. In OMC, navigate to the screen **Subscribers/Basestations List** and select in the list the OTCV Android on which dual-mode has to be activated.
2. Click the **Details** button.

The OTCV Android parameters page is displayed

3. Click the **Mobility** button.

The **Mobility** page is displayed

4. In the **SIP Companion** drop list, select the previous created SIP companion.

Note:

*If the dual-mode is already activated, the associated SIP Companion number is shown in the list. If the dual-mode is not activated, the value **None** is displayed and all available SIP Companions are proposed in the list.*

5. Click **OK** to validate

Note:

*In the **Call Routing** page of OTCV Android, the **Mobility** and **Mobility with SIP** profiles indicate whether the dual-mode feature is enabled or not for this OTCV Android. Switch the **Mobility with SIP** profile to **Mobility** allows to deactivate temporarily the dual-mode feature on the current mobile. This information can be modified only if a SIP companion has been selected in the list. At the first selection of a SIP companion, the dual-mode feature is enabled by default, so the **Mobility with SIP** profile selected.*

9.4.5 Associating a desk phone to the OTCV Android

The OTCV Android can be associated to the user desk phone or can be used as standalone device. The association with a desk phone is achieved with the multi-set feature available in the OXO Connect (see: [3] Multi-sets).

9.4.6 Installation

OTCV Android is installed in the following order:

1. OXO Connect is installed with the MyIC application configured for office use and the system is stable
2. The OTCV Android application is downloaded to the client telephone
3. The telephone is declared in the OXO Connect MyIC application

9.4.7 Application installation in the mobile device

An OTCV Android application is bundled into an Android package (APK), an archive file marked by an .apk suffix. This file is the vehicle for distributing the application and installing it on mobile devices; it is the file users download to their devices. All the code of a single .apk file is considered as one application.

The APK may be downloaded over the air through Android Market or any web server, or through a wired connection.

Note:

There is no automatic software update for OTCV Android through the OXO Connect.

When the application is installed on the mobile device, the  icon is visible on the mobile device application desk.

9.4.7.1 Loading the application from the Android Market

9.4.7.1.1 Loading the application from a computer

Use a browser to navigate to <https://market.android.com> and use the search engine to find the OTCV Android application. Any of the following keywords may be used:

- Alcatel, Alcatel-Lucent, Lucent
- OpenTouch
- Conversation

The complete name of the application is: OpenTouch Conversation for Android. The application is intended for the two products OXO Connect and OpenTouch.

Mail the application to your mobile device mailbox.

9.4.7.1.2 Loading the application from the mobile phone set

1. Navigate to the Android market and use the search engine to find the OTCV Android application.

Note:

Any of the keywords listed: [Loading the application from a computer](#) on page 138, may be used

The list of applications is displayed

2. Select the application and touch **Accept & download**

The download status is indicated

3. Install the application.

On completion, the **Start** window is displayed

4. Once connected, the configuration window is displayed.

Enter the public and/or private URL for the OTCV Android to connect to the OXO Connect

Note:

*The **Private URL** field can be empty, as it is optional.*

When a router is used, OTCV Android is seen as an external device of the enterprise network (distant access). In this configuration, the public URL of OXO Connect is used. The public URL must be configured in the OXO Connect and entered in the OTCV Android application at login.

The public URL consists of the public hostname/IP address, optionally the port (separated by colon) and the path to the root URL, when access is performed from the public network (for example: <https://enterprise.loc/DM>).

Note:

The system performs verifications on the URLs:

- *Entered URLs are valid URLs (conform to RFC 2396). An empty URL is considered as invalid.*
- *Both URLs (private URL and public URL) are set*

For more information about ports used by OXO Connect and router configuration, see [13] Access Control.

9.4.7.2 Client management

At startup, the mobile gets a configuration file from Client Management which contains:

- The general infrastructure information such as PBX parameters and Wi-Fi parameters
- Specific ICS user information

The OTCV Android application stores the configuration values downloaded in the device from the previous application session. If the Client Management server remains unreachable at startup, OTCV Android displays a confirmation popup to accept the previous parameters.

9.4.7.3 Configuration file deployment

The application automatically downloads the configuration file, whatever the network topology (LAN and WAN). At the first launch of the application, users are prompted to enter their credentials and the OXO Connect public/private URLs to allow the download of the configuration file. If users do not enter their credentials when requested, the application does not start.

9.4.7.4 Device inventory

After downloading of the configuration file, the inventory file is pushed to the PBX. This upload is performed using a PUT HTTP(s) request on the URL provided in the configuration file (the appropriate one, public or private, depending on the current type of data channel).

9.5 Operation

Under normal conditions the telephone services are those provided by the PBX.

Depending on the phone status, the native phone application can be pushed on top of OTCV Android. This limitation is due to the current Android platform.

When the user makes an outgoing call using web services, the PBX first calls back the mobile and initiates the outgoing call to the called party. This mechanism is also used to consult the business voice mail: the application tries to answer automatically the PBX callback.

For incoming calls under data coverage (WiFi, 3G/3G+), OTCV Android can receive call events from the server. It can display the incoming call screen on top of the native screen (in order to offer "Divert to voice mail/One number services" and the "Answer call" features). To answer the incoming call, the user clicks the "Take call" button.

Security policies may prevent using the incoming call screen in this manner.

For example, the IT manager may activate a security policy that forces the user to enter a complex password to unlock the device. This can occur when using an MS-Exchange account on the mobile.

In this case, when users receive an incoming call while the mobile is locked, they are prompted to enter a password before they can answer the incoming call. The extra time required can cause the call to be missed.

To address such situations, OTCV Android includes a setting parameter: a check box in OTCV Android local settings offers the choice to display incoming call screens.

By default, the "display OTCV Android incoming call screen" check box is not validated (meaning that incoming call screens are not displayed).

9.5.1 WiFi or 3G/3G+ coverage

Under WiFi or 3G/3G+ data coverage, the mobile can reach web services even during communications. Voice call management behavior is as follows:

- The connection with the Event Server is established permanently when the device screen is on. The EVS connection is closed when the device screen is turned off, and re-opened when the device screen goes on again (except during an active call where the connection is never stopped).
- Outgoing calls are initiated using web services.
- When in communication, the application displays the conversation screens. Mid call services are performed using web services.

- When the device screen is turned off, and the EVS connection is closed, events (missed calls, callback requests, voice mails) are polled every 10 minutes.
- Incoming calls are presented using the OTCV Android screen (if authorized in the settings).
- If the mobile loses the data connection while in communication, the current conversation screen is hidden. The display switches to the native dialer (provided that the user has not used some other application in-between). Depending on the current telephone state, the user may experience odd behaviors; for instance:
 - In a one-to-one communication, when the user has put the call on hold, it may prove impossible to retrieve the call put on hold.
 - In a broker call, the user cannot go back and forth between the two communications, nor transfer the call or switch to a three-party conference.
 - In case of a second business incoming call, the user cannot take this second call.

9.5.2 EDGE or GPRS coverage

Under EDGE or GPRS data coverage, the mobile phone cannot access the data channel when a communication is established. Voice call management behavior is as follows:

- The connection with the Event Server is not established, even when the user is not in communication.
- Outgoing calls are initiated using web services on the OXO Connect (no fallback mode).
- Incoming calls are presented only using the native telephonic screen.
- When in communication, OTCV Android conversation screens are not displayed. The user has only access to the native telephone application. There is no access to business mid call services.
- If the mobile recovers an appropriate data connection during communication, OTCV Android displays the conversation screen for the current business telephone state, with all the usual business services activated.

10.1 Overview

OpenTouch Conversation® for Windows Phone (also called OTCV Windows) is a software client application running on a mobile phone using the Windows Phone Operating System. It provides an access to enterprise telephone services over a mobile Internet access or WiFi network, so that the Windows mobile phone operates as a business phone.

OTCV Windows provides access to business telephone features. In addition to the ordinary business telephony access, OTCV Windows provides data connection to:

- Business directory
- Business call logs
- Business voice mail

OTCV Windows:

- Interacts with native Windows Phone applications to enrich communication services (local contacts)
- Can be used in remote locations, e.g. via Internet, to have access to the same level of services as in the Enterprise premises (See [13] chapter: Network configuration for remote accesses, for detailed information about network configuration from Internet/WAN)
- Can be associated to a deskphone (call routing profile configuration) or can operate as unique user telephone device

For information about the list of compatible devices and OS versions, see the Technical Communication TC1637, available from the Enterprise Business Portal (reference name: MIC_UC_Client_DeviceWhiteList_8AL90822AAAA).

Note:

Data connection is dependent on network availability. OTCV Windows cannot handle any fallback mode or business services when the data connection is not available.

10.2 Architecture

10.2.1 Overview

This module presents the network topologies to access the PBX services from an OTCV Windows application.

For data communications, the OTCV Windows accesses the PBX services using OmniTouch 8400 ICS web services implemented in the PBX (that is OXO Connect). It requires either one of these network connectivities:

- The enterprise Wi-Fi network inside the enterprise

Note:

A Wi-Fi Internet access or hot spot can be used at home for data transmission.

- An Internet/data connection provided by some cellular networks (2.5G, 3G, 3G+, 4G and GPRS) outside the enterprise. See [13] Network configuration for remote accesses for detailed information about network configuration from Internet/WAN)

For voice communications, the regular cellular network (2.5G, 3G, 3G+, 4G and GPRS) and PSTN network are used

When the connection to OXO Connect is via an EDGE network, services are limited on OTCV Windows. Behavior is as follows:

- When the application is in idle state (no calls):
 - The network banner is green
 - The available features are:
 - Outgoing/Incoming calls (cannot control call capabilities)
 - Dial by name

For all the other services, the behavior is the same as when no network is available. When a user performs an unsupported action, the error message: **"Please check your network connectivity."** is displayed.

- When the application is in conversation:
 - The network banner is red
 - All services, such as incoming/outgoing calls, dial by name, missed calls, VM, IM, are unavailable

The OTCV Windows application relies on the following components:

- Instant Communications web services to access the different services; including:
 - Telephony
 - Universal Directory Access (UDA)
 - Business Call Log
 - Voice mails
- The Event Server (EVS), in charge of publishing device related events and notifications, such as alarms and configurations changes in the different user applications or services. OTCV Windows application uses the HTTP(s) protocol to connect with the servers within the enterprise. Note that the server digital certificate of the OXO Connect must be installed in the OTCV Windows application for server authentication, and enable HTTPS connection (see [13] Certificate management).
- The Microsoft Windows Push Notification Services (WNS), used to send notifications from the OXO Connect to the OTCV Windows applications. When the OXO Connect sends an event, it generates a push notification and sends a request to the WNS. The WNS receives the request and routes the notification to the appropriate OTCV Windows application. The notification is then displayed in a toast window, live tile, or lock screen.

A web proxy can be configured for the network. In this case, the web proxy details must be configured in OMC. For more information, see [Engineering rules](#) on page 143.

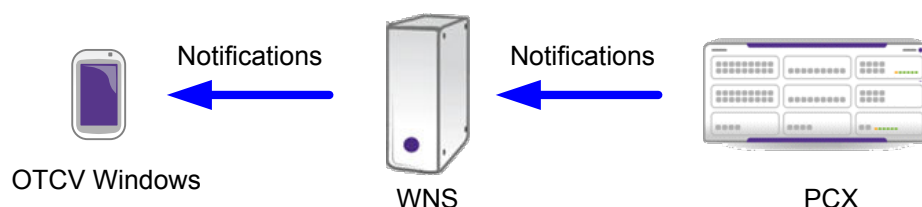


Figure 10.1: Windows Push Notification Services (WNS)

10.2.2 Access Provided from the WAN/Internet

In order to set the appropriate security measures and configuration rules for connecting OTCV Windows from the WAN/Internet, please follow with care the recommendations in [13] Network configuration for remote accesses.

When connected from the WAN/Internet, the OTCV Windows is seen as an external device of the enterprise network (distant access). In this configuration, the public URL of OXO Connect is used to

connect. The public URL must be configured in the OXO Connect and entered in OTCV Windows application at login.

The public URL consists of the public hostname/IP address, optionally the port (separated by colon), for example: `enterprise.loc:443`

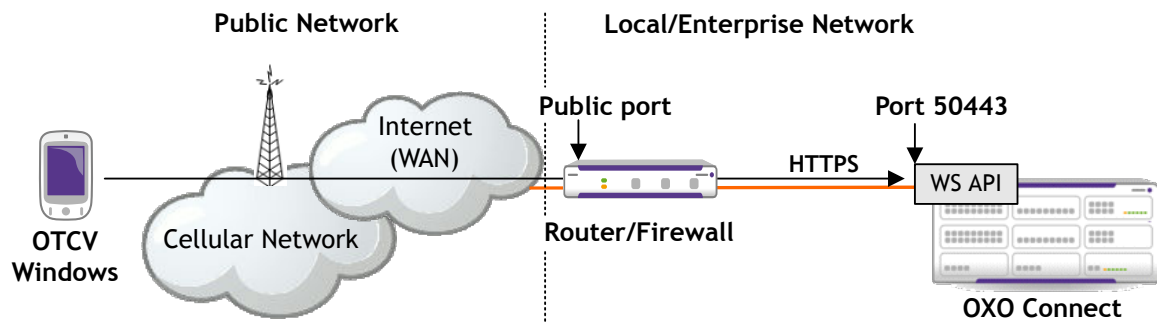


Figure 10.2: Data Transmission via a Router/Firewall

For HTTPS connection, OTCV Windows application must embed the authority certificate of OXO Connect server certificate. With such configuration, users are not warned that they use an HTTPS certificate issued from an unknown authority. This requires consistent DNS resolution from the outside or inside enterprise network. For more information about certificate management, see [13] Certificate management.

10.2.3 Public and Private Domains

The OTCV Windows can connect to the PBX through the enterprise Wi-Fi network or through the public network (3G, Home wireless,...). It uses both public and private URLs to target the OXO Connect PBX.

Private and public URLs are configured in the PBX and retrieved by the OTCV Windows application. When accessing the PBX, the OTCV Windows behaves as follow:

- The mobile always tries to use private URLs at first
- If the connection fails using private URLs, the mobile uses public URLs. This happens when the mobile is connected to cellular network or to home/hot spot Wi-Fi networks

When switching between public and private networks, the OTCV Windows application handles automatically the switch between public and private URLs usage.

10.2.4 Engineering rules

Connection between OXO Connect and the WNS:

- A connection to Internet must be available.
- The DNS server IP addresses must be configured in OMC in **Hardware and Limits > LAN / IP Configuration > DNS/DHCP** tab. This is necessary to resolve the WNS name coded in the OXO Connect, so that the OXO Connect can reach the Windows Notification server directly.

Connection between the applications and OXO Connect:

- To receive the WNS notifications, OXO Connect and the devices (PIMphony Touch / OTCV Windows) must have an internet connection.
- The port used by the applications to reach OXO Connect must be open on the access router and redirected to the WAN port of OXO (default: 50443).
- The URL services must be authorized: <https://host/services/lcs/7.0/>
- The URL for event must be authorized.

Configuration with web proxy:

- The web proxy details must be configured in OMC in **Hardware and Limits > LAN / IP Configuration > Web proxy** tab.

10.3 Detailed description

10.3.1 Main Features

The OTCV Windows application provides a subset of the features available from the user's deskphone on a mobile phone.

Telephone features are the basic services supported by OTCV Windows. They are available only with full data connection. With full data connection (cellular network or WiFi network), services are activated through Web Services handled by the OXO Connect.

When the data channel is available, the services provided to the user by OTCV Windows are:

- Application management:
 - Start the application
 - Synchronize configuration
 - Configure the client management server URLs
 - Restrict ringing to incoming business communications
- Business communications (see: [Business Communications](#) on page 145):
 - Make an outgoing call
 - Dial by Name
 - Dial By number
 - Answer an incoming call
 - Release a simple call
 - Make a second call
 - Transfer the call
 - Release the active call
 - Put a call on hold
 - Take the call on hold
 - Three-party conference
- Call history management
- Favorites
- Programmable keys
- Call routing profiles (see: [Call routing Profiles](#) on page 145)
- Directory services (see: [Directory Services](#) on page 146):
 - Search in the directory
 - Display contact details
- Call log services (see: [Business Call Logs](#) on page 146):
 - Consult the call log
 - Delete the call log
 - Acknowledge a call log item
 - Delete a call log item
- Voice mail services (see: [Business Voice Mail](#) on page 147):
 - Consult voice mails

- Play a voice mail
- Remove a voice mail
- Call back the message sender
- Instant Messaging services
 - View the conversation list
 - Delete instant messages in a conversation
 - Send and receive instant messages
 - Delete conversations
 - Call the sender of instant messages
 - Decline an incoming call with an instant message

For more information on Instant Messaging services, refer to: [3] Instant Messaging.

10.3.2 Business Communications

Private communications are out of the scope of OTCV Windows. It only manages business communications, consisting in incoming and outgoing call from the PBX.

In a business context, communications are handled through the PBX (provided the data channel is available), ensuring rich telephone features. The mobile device can receive and make business calls; but can also make private calls through the native mobile device application.

To leave the business context, the user selects the **Office** routing profile (see: [Call routing Profiles](#) on page 145). This means that no more business calls are received on the mobile.

Notes:

Since the client cannot send DTMF codes, OTCV Windows does not support any fallback.

10.3.3 Call routing Profiles

When the OTCV Windows application is launched from the mobile device, the user can configure the current routing profile for outgoing and incoming calls. From the application home page, the access path is: **Settings > Routing**.

Two call routing profiles can be configured from the OTCV Windows application:

- The **Office** profile: this call routing profile is only available when the OTCV Windows is associated to one or more phone sets in a multi-set configuration. If there is no multi-set configuration, **No Mobility** is displayed on screen.

When the **Office** profile is selected, the user cannot handle calls from the OTCV Windows. Call handling can only be performed from the other phone sets associated to the user.

Note:

In this configuration, the user can also forward incoming calls to voice mail or a preferred number (four numbers can be defined in the routing profile).

- The **Mobility** profile: the user can configure the Nomadic destination to which incoming calls are routed. The destination number can be any of the following:
 - **Mobility number**: incoming calls are presented to the mobile phone number associated to the OTCV Windows. Four predefined phone numbers can be entered in the OTCV Windows. If the user has one or more phone sets (multi-set configuration), the application only rings for incoming business communications. Other associated phone sets do not ring. If configured in the OMC, their screen only indicate an immediate forward to the application name or directory number.
 - **Mobility number and Office phone**: this option is only available when the OTCV Windows is associated to one or other phone sets in a multi-set configuration. Incoming calls are presented to all devices associated to the user.

- **Forward to number:** Incoming calls are forwarded to a phone number, which is either a number previously configured in the OTCV Windows or a phone number entered manually. Four predefined phone numbers can be entered in the OTCV Windows.

Note:

*When call forwarding information is not available (not retrieved at initialization, or when the data channel is not available), the home page displays **unknown** as phone set status.*

- **Forward to voicemail:** Incoming calls are forwarded to the user voice mail.

Note:

*When call forwarding information is not available (not retrieved at initialization, or when the data channel is not available), the home page displays **unknown** as phone set status.*

When other types of call forwarding, such as Do Not Disturb (DND) or call forwarding on busy are defined, the Other type of forward is activated message is displayed on the screen.

Note:

*When OTCV Windows is included in a multi-set, for external diversion to operate correctly, the **External diversion** right must be enabled for primary set of the multi-set.*

10.3.4 Directory Services

OTCV Windows handles several services related to business and local directories.

OTCV Windows automatically launches a search when users enter more than two characters and use the **Search** button.

The contact detail page includes contact identity and provides detailed information about a contact, and lists the different ways the contact can be reached.

Identity information can include:

- Full name (last name and first name)
- Phone numbers
- e-mail address

In some cases, phone numbers for outgoing calls must be preceded by an outgoing prefix. This occurs when the phone number (for an outgoing call) is entered manually or retrieved from business or local directories.

OTCV Windows can add this prefix to the phone number, so that the PBX can establish the call.

Depending on the origin of the phone number, the following rules are applied to make the call:

- The number is used without modification:
 - When the number comes from the OTCV Windows phonebook
 - When the number comes from a call log or a voice mail
 - When the phone number comes from the LDAP directory
- Note:*
It is recommended to have phone numbers registered in canonical form in the LDAP directory.
- OTCV Windows automatically adds the prefix before making the call:
 - When the number comes from the mobile device local contact list
 - When the user enters a phone number manually, provided this number does not contain the external outgoing prefix

10.3.5 Business Call Logs

The Business call log contains call log items related to the user. It includes:

- Caller details

- Date and time information

It concerns all events related to **One Number Services**.

The user call log is managed by the PBX. It is limited by the PBX call log limit. To optimize response time and data channel consumption,OTCV Windows limits download to the fifty most recent call log items.

Call log lists are updated when an appropriate data channel is available. When there is no data channel, lists are not updated.

10.3.6 Business Voice Mail

OTCV Windows handles several services related to business voice mails. Voice mails are displayed in a specific menu and can be selected individually.

The PBX starts a GSM call to OTCV Windows to play a voice mail.

Information about each voice mail includes:

- Caller phone number
- Caller name
- Voice mail date/time and duration

Actions that can be taken for messages include:

- Listen to a voice mail
- Go to next/go to previous voice mail
- Pause
- Delete a voice mail
- Call the person who left the voice mail
- Activate/disable the speaker

Voice mail list consultation and voice mail play are available when data coverage (WiFi or 3G/3G+) is implemented.

10.4 Configuration procedure

10.4.1 Checking the license

In the OMC tool, the creation of an OTCV Windows application is refused when the number of such applications has reached the maximum value indicated by the license.

To verify the license

1. From the OMC tool, navigate to: **Modification Typical > System > Software key**
2. Click **Details**
3. In the **Voice Communication** tab, check that the option **My IC Mobile users** is enabled (the maximum value is 50)

10.4.2 Checking the VoIP protocol

To use OTCV Windows, you must verify that the VoIP protocol is set to SIP in the OXO Connect configuration.

To check, and, if necessary, modify the VoIP protocol:

1. From the OMC tool, navigate to: **Voice over IP > VoIP: Parameters**
2. Click the **General** tab and verify that the **VoIP Protocol** parameter is set to **SIP**

10.4.3 Declaring the OTCV Windows

The OTCV Windows application must be declared in the OXO Connect, using OMC. The OTCV Windows applications are created in the OXO Connect regardless of the mobile type on which the applications must run (there is no hardware link between the mobile device and the OXO Connect). This simplifies OTCV Windows declaration, as the mobile device IMEI or MAC address is not necessary.

To declare an OTCV Windows:

1. From the OMC tool, navigate to: **Subscribers/Basestations List** and click **Add**

This displays the **Add User** screen.

2. Select the **My IC Mobile** check box
3. Select the number of application to create (default: 1)
4. Keep the proposed directory number for the application or select another free number
5. Click **OK** to validate

The My IC Mobile is displayed in the list of subscribers

6. In the **Details** tab, click **Cent Serv.**
7. Validate the **Nomadic Right** check box
8. Click **OK** to validate
9. Click **OK** to leave the **Details** tab

This operation automatically creates a configuration file on the OXO Connect required for OTCV Windows commissioning. The configuration file is identified by the directory number specified at OTCV Windows declaration. The configuration file is named: `MOBILE_<application directory number>@server private FQDN.xml`. At first startup, the application automatically downloads its configuration file using the OXO Connect URLs and the credentials entered by the user. This occurs whatever the network used: intranet (LAN) or internet (WAN).

Caution:

If the configuration changes on the OXO Connect and the OTCV Windows is opened, it is required to log out and log in again to force the download of the new configuration file.

10.4.4 Associating a desk phone to the OTCV Windows

The OTCV Windows can be associated to the user desk phone or can be used as standalone device. The association with a desk phone is achieved with the multi-set feature available in the OXO Connect (see: [3] Multi-sets).

10.5 Operation

10.5.1 Overview

The OTCV Windows must be downloaded and installed on the mobile device using the Windows Phone Store.

10.5.2 Prerequisites

The OTCV Windows must be present in the Windows Phone Store for Windows products.

The OTCV Windows must work normally and be connected to the internet via the cellular network.

You need a Microsoft account to download the OTCV Windows application from the Windows Phone Store. If this is not the case, go to: <http://www.outlook.com> and follow the instructions on screen to create a Microsoft account.

10.5.3 Installing directly the application from the mobile device

1. From the mobile device home page (), select the  icon to access the Windows Phone Store
2. Enter the credentials of your Microsoft account
3. From the Windows Phone Store, search for the OTCV Windows with keywords, for example: Alcatel-Lucent or conversation

The complete name of the application is: `OpenTouch Conversation for Windows`.

4. Follow the instructions on screen to download the OTCV Windows

When download is finished, the mobile device automatically installs the application. After installation, a tile dedicated to OTCV Windows is displayed in the list of applications present on the mobile device

10.5.4 Launching the OTCV Windows

Once the OTCV Windows is installed on the mobile device, proceed as follows:

1. From the mobile device home page, press the OTCV Windows tile

A login page opens

2. You are prompted to enter:

- The public and private addresses to connect to the OXO Connect. The available formats are:
 - `https://<IP address>`
 - `IP address`
 - `<IP address: port>`
 - `DNS name`
- The user credentials to access the OTCV Windows (directory number and password). At first startup, the user is prompted to change the initial password by a new password (trivial password is forbidden)

3. Click the **login** icon () to open OTCV Windows

At first connection, a certificate installation screen is displayed.

4. Click **Install**

This operation installs the OXO Connect certificate in the mobile device trusted certificate store. When the certificate is successfully installed, a confirmation screen is displayed.

5. Click **OK**

At first installation, you are prompted to change the default password

6. Change the initial password by a new password

7. Click the **done** icon () to save your modification

Note:

At startup, the OTCV Windows first tries to reach the private FQDN of the OXO Connect. If the private FQDN of the OXO Connect cannot be reached, the OTCV Windows tries to reach the OXO Connect through its public FQDN.

10.5.5 Modifying the connection parameters to the OXO Connect

After startup, connection parameters to the OXO Connect can be modified from the OTCV Windows settings as follows:

1. From the OTCV Windows home page, click the ... button in the application bar present at the bottom of the screen and select the **settings** option

The settings page opens

2. Select the **Configuration** option

The **Configuration** page opens

3. In the **Server Details** area, modify the public and/or private addresses of the OXO Connect according to your needs
4. Click the **done** button () to save your modifications

10.5.6 Accessing logs

The OTCV Windows provides applicative logs. These log files can be sent by e-mail or uploaded to the OneDrive space (formerly SkyDrive). The second solution requires to install the OneDrive application on the mobile device. This application is available on the Windows Phone Store.

To retrieve log files:

1. From the OTCV Windows home page, click the ... button in the application bar present at the bottom of the screen and select the **settings** option

The settings page opens

2. Select the **TraceSettings** option

The **Configure Logs** page opens

Note:

*Touch the screen and move the finger to the left (or right) displays the **Delete Logs** page*

3. Select the type of messages to send (**Error** option is selected by default)
4. To retrieve the corresponding log messages, use any of the following:

- Click the **email** icon () to send the log messages by e-mail.
- Click the **upload to skydrive** icon () to upload the log messages to the OneDrive space.

This opens the live connect login page

1. Enter the credentials of your Microsoft account and click **Sign in**

An access page opens

2. Click **Yes** to enable access to the OneDrive space

The trace setting page displays the progression of the log file upload. A confirmation message opens when the log file is successfully uploaded.

3. Click **Ok** to return to the **Configure Logs** page

WLAN Infrastructure for OpenTouch Conversation applications

11.1 Introduction

Voice applications are sensitive to network characteristics (such as delay, jitter, bandwidth), which are very variable among the WLAN deployments. This chapter describes engineering rules (for network design) and troubleshooting tools (for field support).

Deployment size must be taken into account. Knowing that dual mode customers can be configured on small sites with just a few OpenTouch Conversation applications to larger sites where up to the maximum of up to 50 OpenTouch Conversations clients are in service. The constraints of both deployments are of course not the same.

In the first case, the WLAN infrastructure is created with basic equipment, in the latter case a more sophisticated network is required.

Troubleshooting tools can help to identify network related issues, in case of malfunctioning application or voice quality problems on a small WLAN network which was not originally designed to comply with VoWLAN requirements.

Conversely for larger scale deployments, a WLAN analysis and design is required, unless the customer infrastructure already meets the requirements of VoWLAN.

Note:

WLAN design can be used to avoid some problems in smaller deployments.

A site survey is mandatory to ensure a correct coverage for voice.

11.2 Network architectures

OXO Connect can be deployed in overly simple network architectures, where the WAN router connects to OXO Connect and also acts as a WiFi access point. Generally, no network engineering has been carried out for designing the network, and no WLAN coverage analysis has been performed. Entry level access points have limited troubleshooting capabilities. That's why the troubleshooting tools provided by OXO Connect and OpenTouch Conversation are of higher importance.

Generally, without prior WLAN analysis and a proper WLAN design, it is not possible to guarantee the correct operation of OpenTouch Conversation in VoWLAN mode. Networks that are not designed for VoWLAN are not supported.

In larger capacity networks, or if a large number of OpenTouch Conversation need to be deployed, network engineering is required. Controller based architecture, like Alcatel-Lucent OmniAccess Wireless LAN switch (also called OAW controller), provides the tools for analyzing and troubleshooting the WLAN network.

11.2.1 Standalone Access Point

The WLAN consists of a single standalone Access Point (AP) without a controller and generally deployed without prior network engineering. This means that the network may contain radio coverage white spots, be subject to interference and exhibit common WLAN problems.

The features provided by the APs vary from a minimal feature set to advanced features such as troubleshooting tools, QoS support for VLANs and multiple SSIDs (Service Set Identifiers).

Several independent APs or repeaters can be used to extend the capacity or the range of the WLAN network, but cannot provide seamless roaming between the AP's.

The Access Point may be embedded in the ADSL access router, or provided by a separate device.

A DHCP server is necessary. It can be provided by the AP, OXO Connect, or by another element in the network.

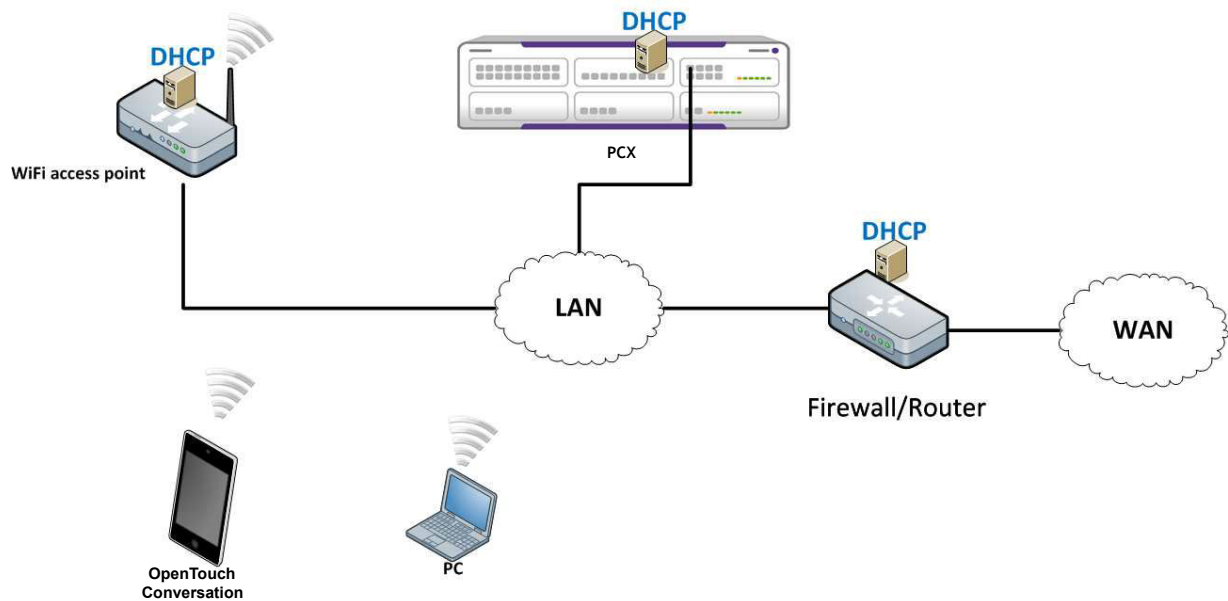


Figure 11.1: Standalone AP

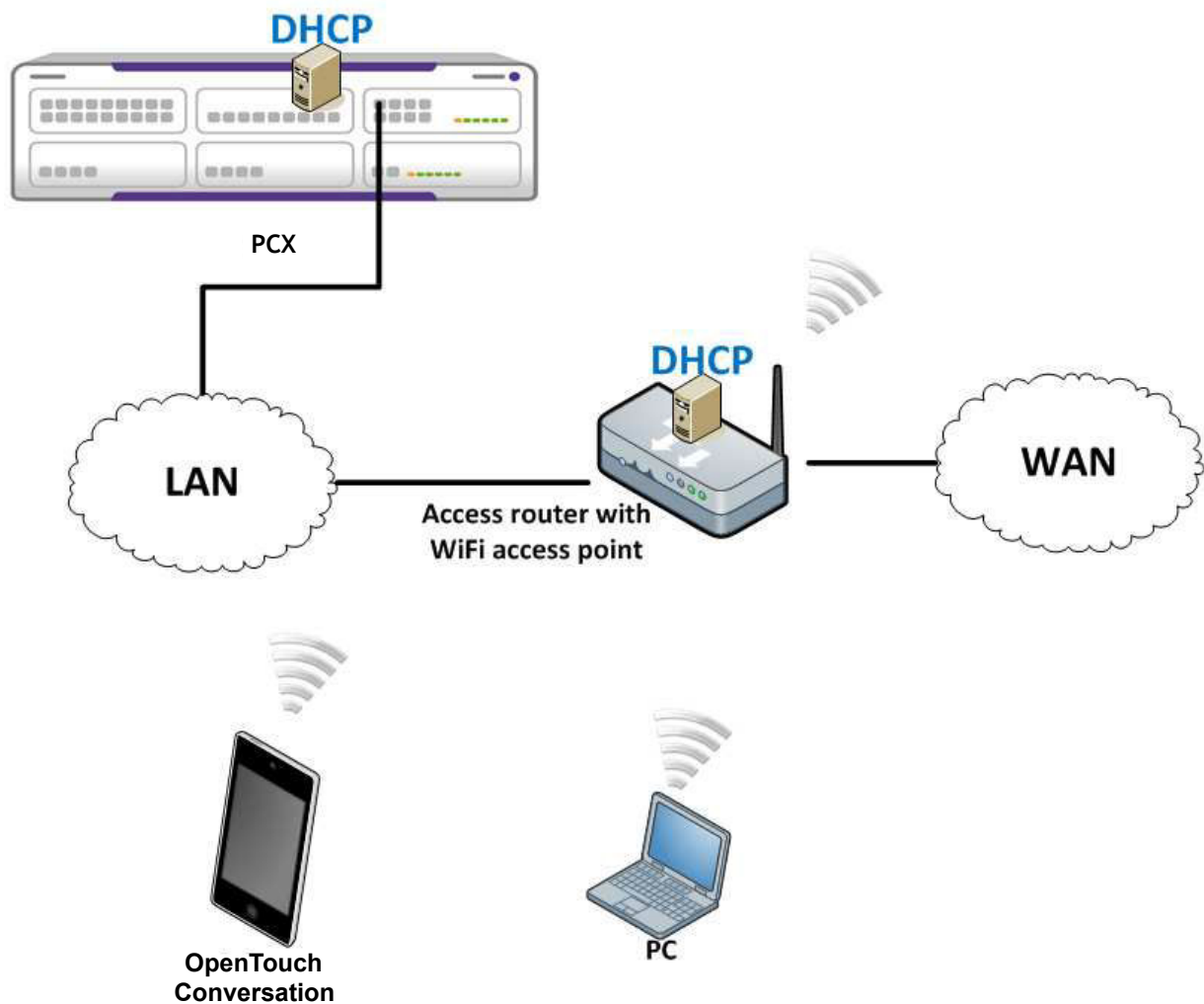


Figure 11.2: AP embedded in access router

Often the WiFi coverage is increased by adding an AP to the network. This solution however does not provide seamless roaming during established calls. Normally, standalone APs do not provide roaming support. Roaming is achieved by a disassociation from one AP and association to another AP. The handover decision is handled by the mobile device's WiFi drivers based on the RSSI of the cells.

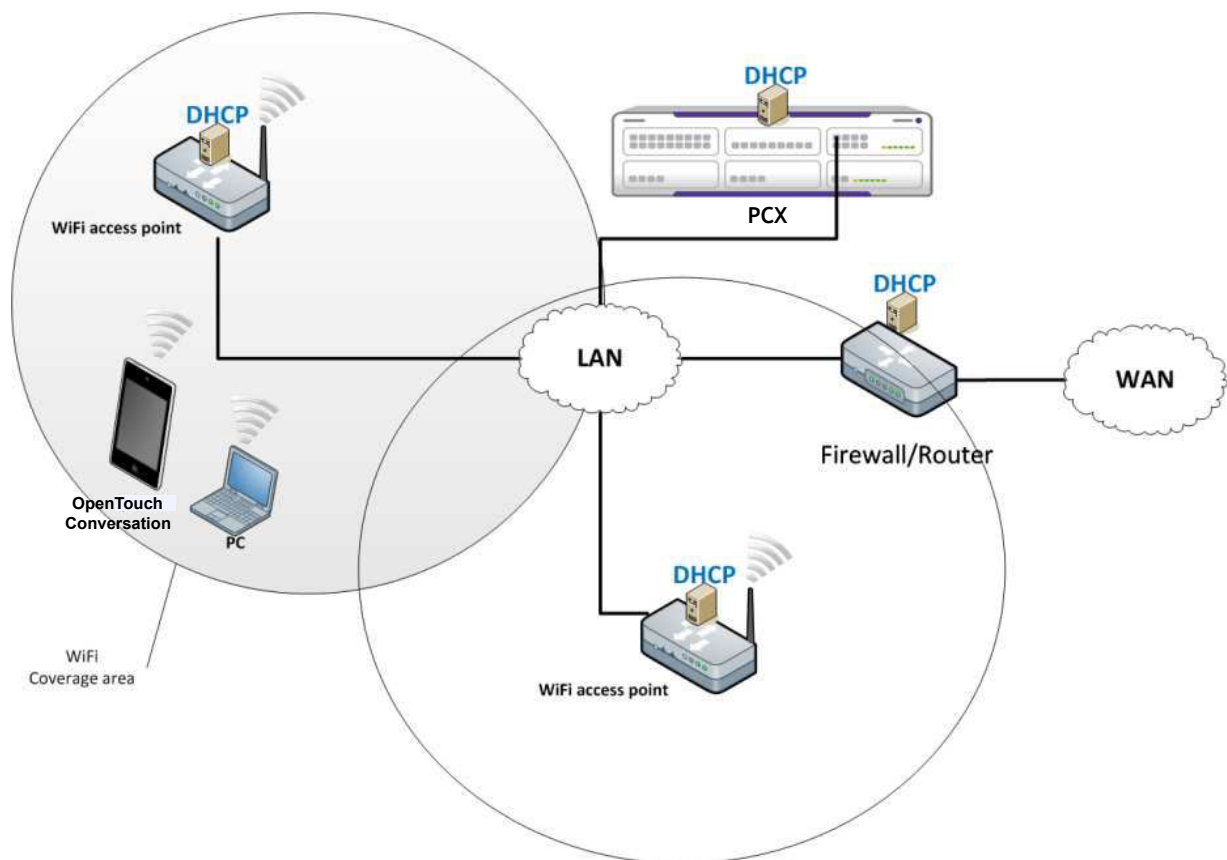


Figure 11.3: Multiple standalone APs

Seamless roaming is not supported in this topology.

11.2.2 OAW controller based architecture

OAW controller based architectures are deployed when the WLAN network:

- Is centrally managed
- Contains many APs
- Needs to be seamless
- Is used for many users

Note:

This type of deployment is nearly impossible to build with standalone APs

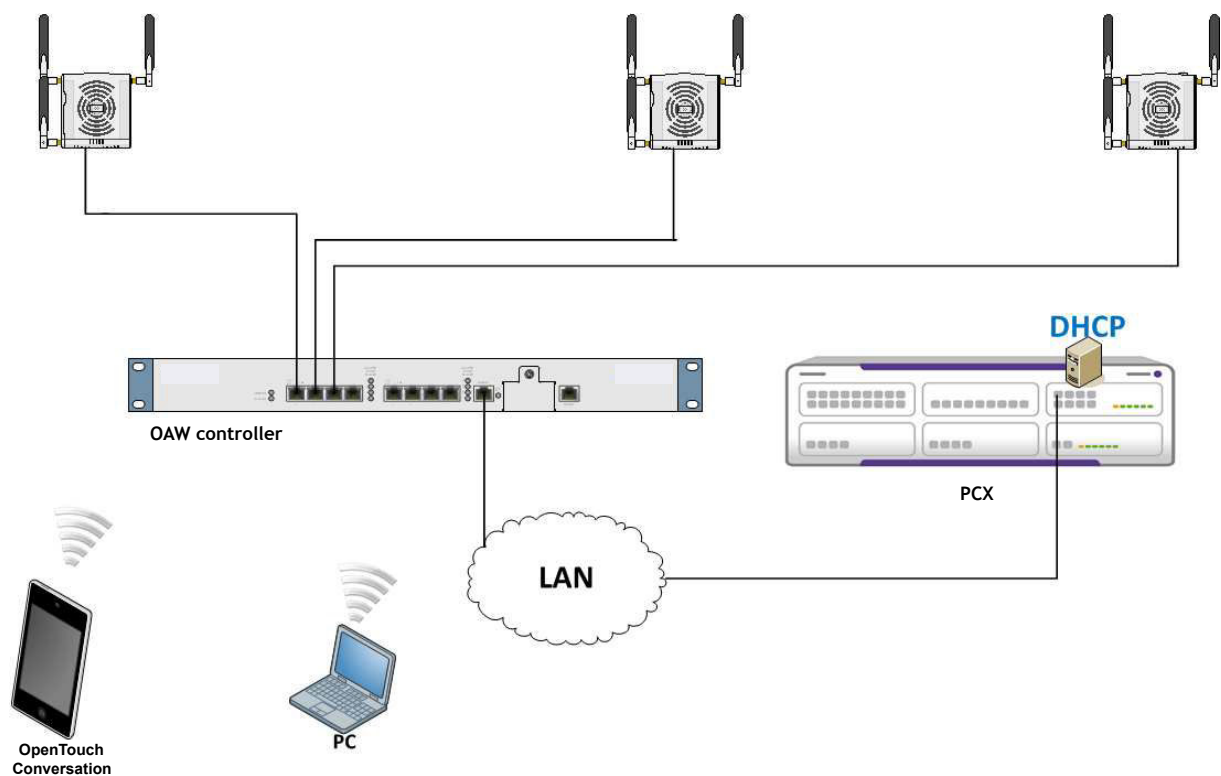


Figure 11.4: OAW controller based architecture

11.2.3 VPN topologies

The usability of this VoWLAN topologies depends on:

- WLAN factors as described in [VoWLAN design recommendations](#) on page 157
- Permitted delay and packet loss inherent to the WAN connection
- Acceptable delay added by the tunnel encapsulation

11.2.3.1 RAP topology

The RAP is a Wi-Fi access point that creates a secure tunnel to an OAW VPN server. The OpenTouch Conversation can connect to the OXO Connect via the tunnel and uses the VoIP mode.

The RAP establishes a tunnel with the OAW and directs the WLAN traffic to the LAN. The RAP can also work in a split tunnel mode, where only the traffic to the OXO Connect is sent via the tunnel (the Policy Enforcement Firewall license is then required).

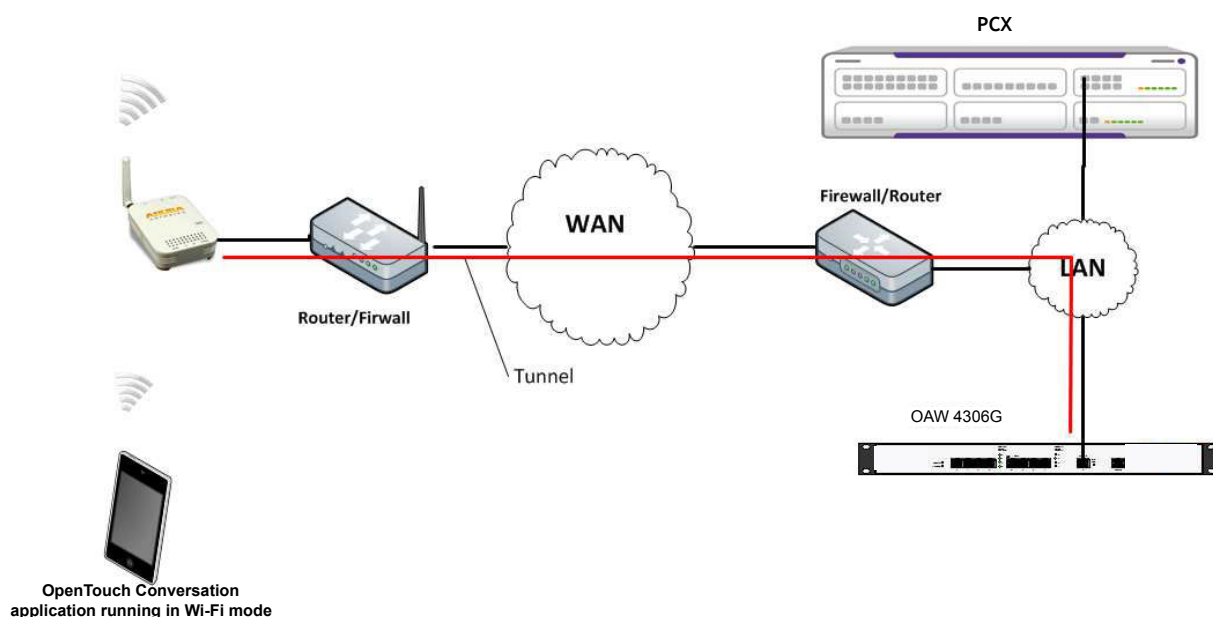


Figure 11.5: RAP topology example

11.2.3.2 Easy VPN topology

The VIA (Virtual Intranet Access) application from Aruba provides secure VPN connectivity to an OAW Networks Mobility Controller. This application must be installed in the mobile devices (iPhone and Android) on which OpenTouch Conversation is running in Dual Mode.

In the same way as for RAP, the OAW VIA application establishes a tunnel between the OpenTouch Conversation and the OAW controller and secures the business calls to or from the OpenTouch Conversation via SIP/TLS and SRTP. This can be used over a Wi-Fi or cellular network (2G, 3G or 4G). In all cases, the Policy Enforcement Firewall Next Generation (VIA/VPN Users) license must be installed in the OAW controller.

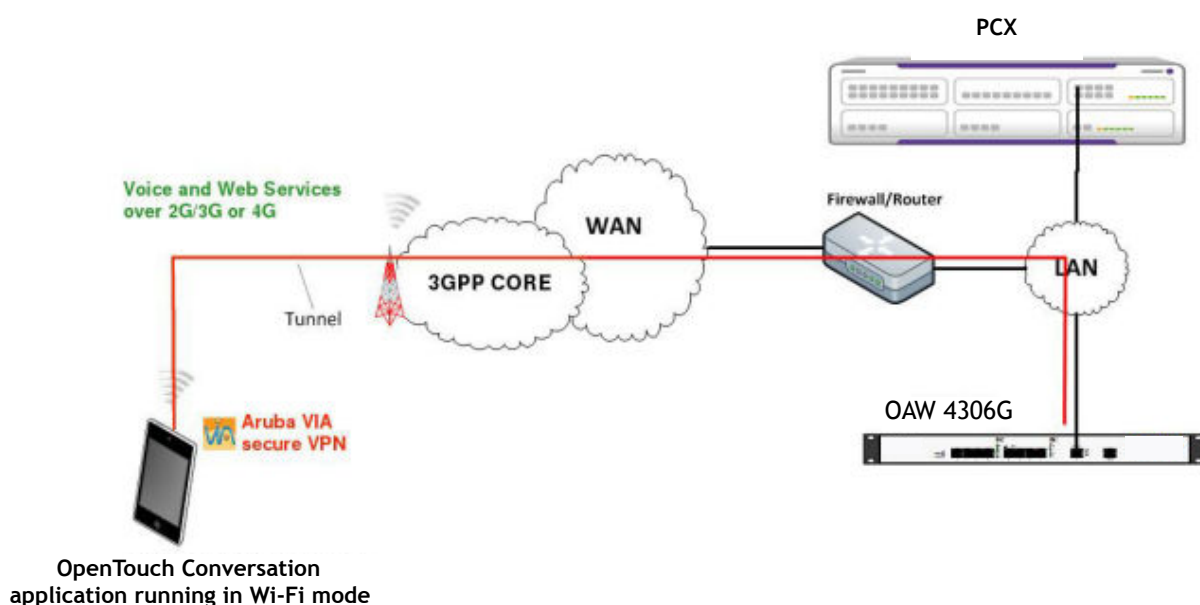


Figure 11.6: Easy VPN over cellular network

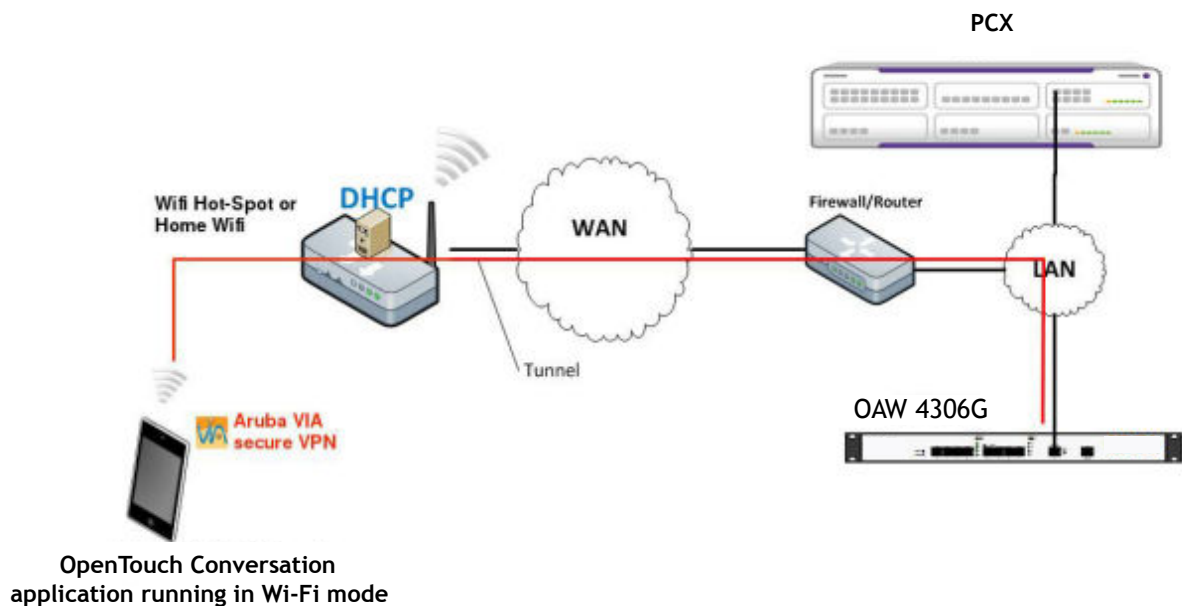


Figure 11.7: Easy VPN over Wi-Fi network

11.3 VoWLAN design recommendations

11.3.1 MAC layer retransmissions

The effects of MAC retransmissions can result in diminished voice quality due to:

- Increased latency and jitter in the packet delivery
- Decreased throughput

MAC retransmissions have multiple causes:

- Degraded signal quality due to interferences and/or poor coverage
- Environment and RF interferences: reflections and/or multi path occurrences
- Hidden node (AP placement)
- Power settings mismatch

If the AP transmits at a higher power than the mobile, the mobile device configures a higher data rate than it can sustain. For OpenTouch Conversation running on iPhone devices, the AP should be configured at the same power level as the iPhone: 13 dBm.

For VoWLAN, the level of MAC retransmission should be less than 3%.

The number of retransmissions can be measured with a protocol analyzer or statistics on the WLAN controller.

Jitter and latency can be analyzed by the OXO Connect QoS tickets provided in Webdiag.

To avoid these effects, it is mandatory to do a site survey and design the network appropriately for:

- AP Positioning
- Power settings (< 13 dBm)

A site survey dedicated to voice is mandatory to insure a good voice coverage.

The mobile device must "see" the AP at -67 dBm or more in all the area covered.

The AP should "see" the mobile device at -67 dBm or more whatever its position in the covered area.

11.3.2 Coverage and capacity tradeoff

Coverage and capacity are competing characteristics of WLAN networks. For an access point, either the coverage or the capacity can be maximized: the larger the cell, the lower the capacity.

As the mobile device gets further away from the AP, the bandwidth is reduced due to 802.11 dynamic rate switching. This impacts the bandwidth of all other mobile devices in the cell. The mobile devices transmitting at lower data rates require more airtime than mobile device transmitting at higher data rates; consequently the low data rate mobile devices affect the whole WLAN network.

Increasing the power of the AP is not a solution as it creates other problems:

- Interference on adjacent channels
- Dissymmetry in station AP for mobile devices near the edge of the cell: they hear the AP but the AP does not hear them.

The size of the cell can be reduced by:

- Reducing the power of the transmitter
- Disabling the lower bit rates

For the VoWLAN, it is recommended to disable (in the AP) the lowest rates: 1, 2, 5.5, and 11 Mbps.

Some basic APs do not provide this capability, it is therefore not possible to restrict the size of the cell. If this is the case, an additional AP can be considered.

The following table shows the relation between data rate, cell size and required sensitivity to 802.11g for a 30 mW transmitter with a 2 dBi gain antenna.

Rate (Mbps)	RX threshold VoIP (dBm)	RX threshold DATA (dBm)	Approximate cell size
54	-56	-61	27 m
36	-58	-63	30 m
24	-62	-67	42 m
12	-67	-72	64 m
1	Not recommended	-84	124 m

To prevent dead calls when the mobile device leaves the WiFi coverage zone, SIP session timers are implemented in OXO Connect. The session timer kills the call if it is not refreshed after 90 s. The timer is specified by a noteworthy address 'Session Timer for SipPhone Dual Mode'

11.3.3 Roaming

In the example considered here, roaming is the case of a mobile moving from one WiFi cell to another cell (on the same LAN).

To be seamless, roaming needs to be completed in less than 150ms with uninterrupted communications.

Seamless roaming is available on ESS architectures, when the cells are overlapping cells and have the support from the WLAN controller. OAW controller based architecture is able to provide seamless roaming.

The decisions about roaming are taken by the mobile device's WLAN driver. The algorithm is chip or vendor specific. Typical conditions for roaming are:

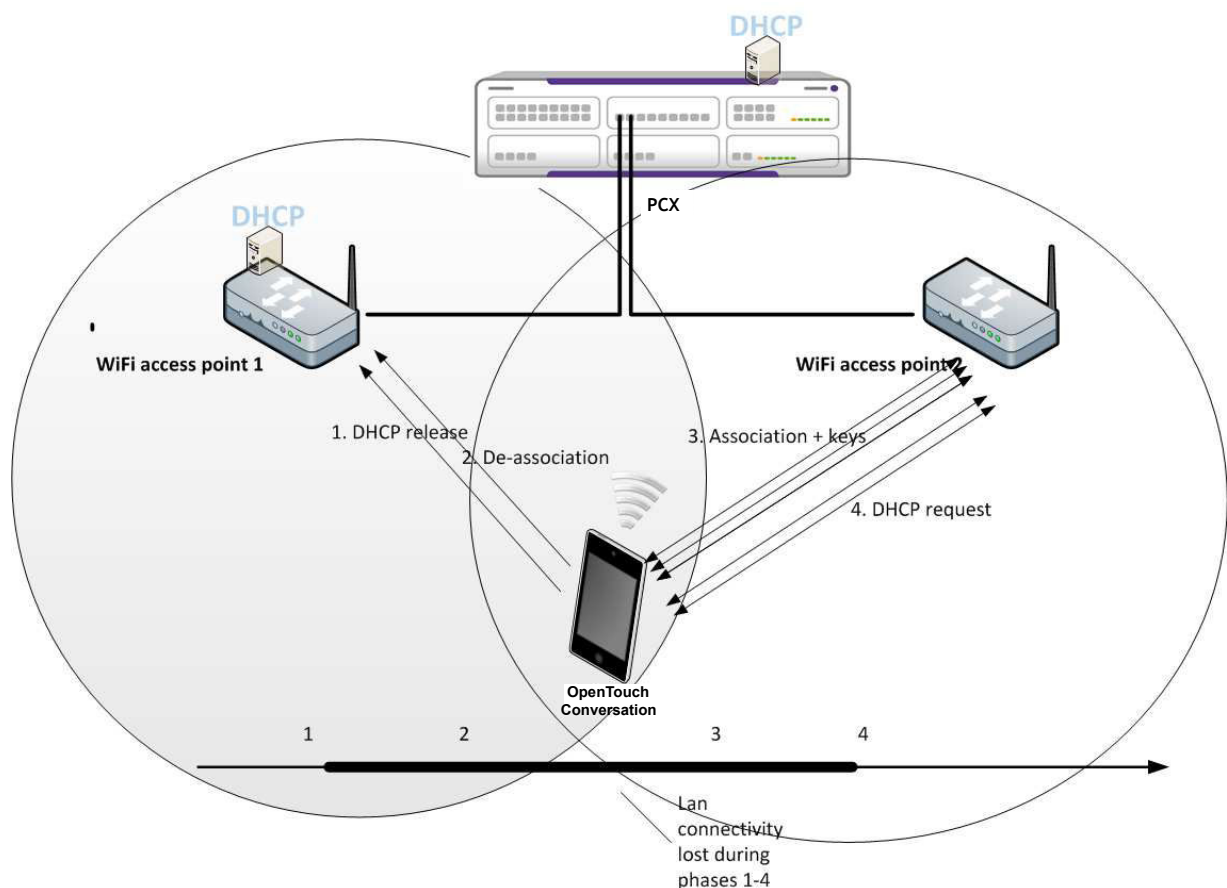
- If the RSSI descends below a specific level (not known), the WLAN interface disassociates and re-associates to the AP with a better RSSI.
- Excessive number of data retries provokes a search
- Low SNR provokes a search

IEEE802.11r-2008 amendment specifies fast secure roaming. This protocol is supported by the following OS:

- iOS 6 on iPhone 4S and 5
- Android

11.3.3.1 Case of standalone AP's

Standalone APs connected to the LAN do not provide support for seamless roaming. When the mobile device moves from one cell to another, the network connectivity is lost and connections may be interrupted, depending on the time required for the re-association.



In order to reduce the roaming delay, the following configurations can be applied:

- Access points on same subnet
- Same SSID and same WPA key can simplify the deployment
- Fixed IP addresses for the OpenTouch Conversation implemented in the DHCP server

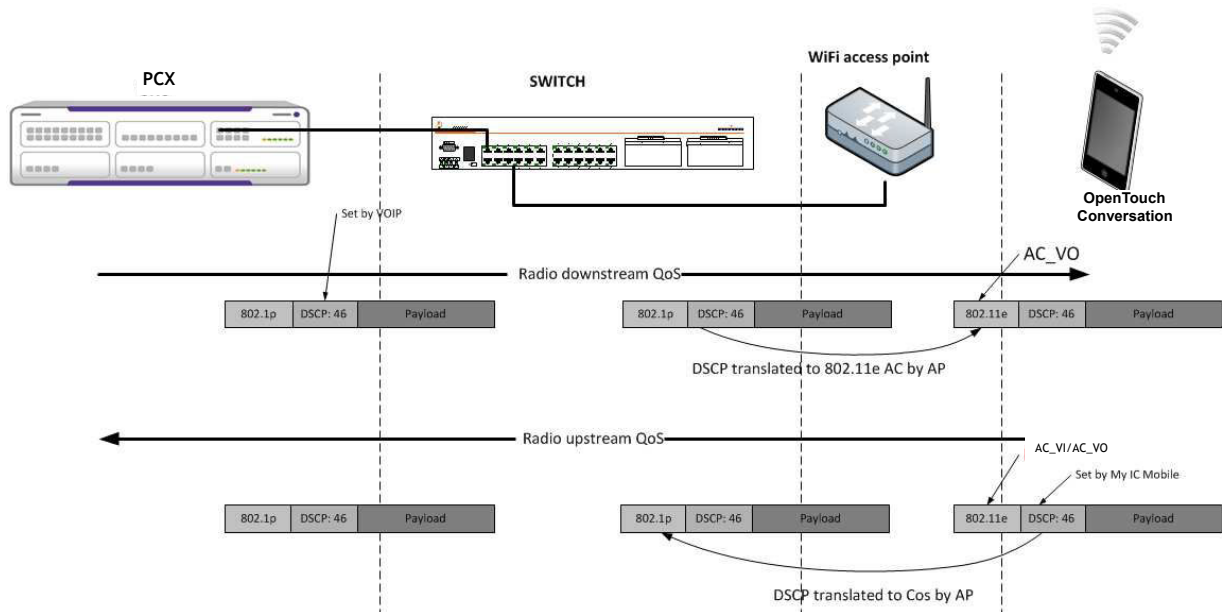
Seamless roaming is not supported on this topology.

11.3.4 QoS

Latency and jitter is induced by applications contending for the network. media, for example video streaming on the WLAN, can be reduced by appropriate QoS settings.

WMM and IEEE802.11-2007 classify traffic into 4 access categories (AC): voice, video, best effort and background. Each category has its own output queue. The voice class has the highest priority.

The AP and OpenTouch Conversation use frame marking for classification and queuing into the appropriate priority queue.



QoS must be implemented in both upstream and downstream paths:

1. Downstream from OXO Connect to OpenTouch Conversation

- By default, the OXO Connect sets the DSCP to 46 for RTP and SIP. The OXO Connect does not set the 802.1p CoS.
- The switch or router does QoS scheduling based on DSCP or CoS
- The AP prioritizes the frame based on DSCP or CoS (depending on its configuration or features)

2. Upstream from OpenTouch Conversation to OXO Connect:

- The SIP stack of OpenTouch Conversation sets the DSCP in the SIP and RTP frames based on the DSCP value found in the XML configuration file downloaded from OXO Connect (default DSCP 46).
- The WLAN driver of the OpenTouch Conversation prioritizes the frames for QoS (see [QoS on the iPhone platform](#) on page 160 and [Priority mappings](#) on page 161).
- The AP adds an 802.1p marking if configured to do so, and schedules the frame into the appropriate output queue

11.3.4.1 QoS on the iPhone platform

The iPhone classifies the frames based on the DSCP value set by the application into one of the 4 WMM classes.

The DSCP value used by the application is the same as the one used by OXO Connect, which is configured in the VoIP parameters, by default set to 46, and transmitted to the application in the configuration file.

The iPhone applies the following classification:

DSCP	VMM Access class
46	Video (5)
48	Voice (6)

11.3.4.2 Priority mappings

- Frames from wired LAN to WLAN: the AP classifies the frames based on either, the 802.1p COS, or on the DSCP.

DSCP Value	Code point designation	802.1p priority	802.11 access category
48	CS6	6	6, Voice
46	EF	5	6, Voice

The default DSCP value for OXO Connect is 46.

- Frames from WLAN to LAN (frames send from OpenTouch Conversation). The WLAN controller or AP must be configured to implement a priority mapping.
 - If the frame contains a WMM marking, the AP maps the WMM priority to 802.1p as in the table below.
 - If the frame does not contain a WMM marking, the AP examines the DSCP value for mapping to 802.1p.

802.11e priority	Access Category	802.1p priority
1,2	Background	1,2 (lowest)
0,3	Best effort	0,3
4,5	Video	4,5
6,7	Voice	6,7 (highest)

11.3.5 VoIP VLAN

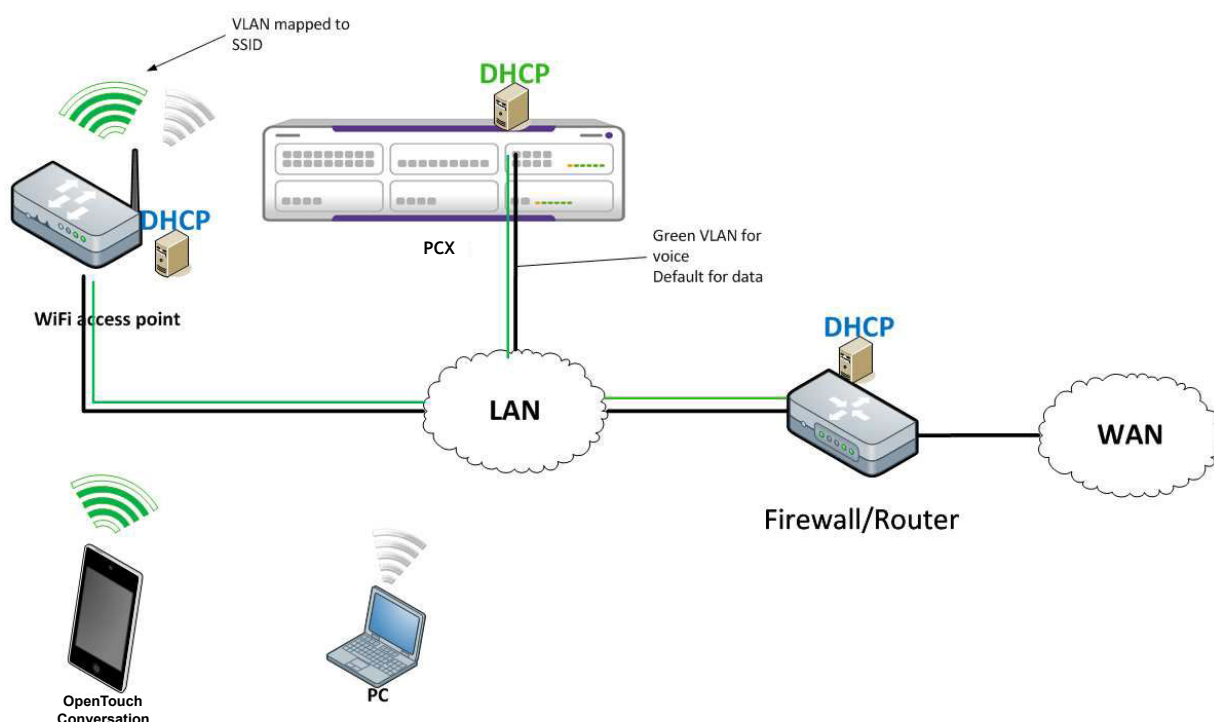
It is possible to segregate the VoIP traffic in a separate VLAN and to map the VLAN to an SSID dedicated to VoIP.

The benefits include:

- Security. Non ciphered voice is isolated in a network; access to the voice network can be managed by access lists and port security.
- Specific QoS rules can be applied for the specific VLAN

Requirements include:

- The AP must be able to support 802.1q and provide the mapping of a VLAN ID to SSID.
- VLAN tagging for VoIP must be enabled on OXO Connect.
- A DHCP server must exist in the VLAN. It can be provided either by the AP or OXO Connect.
- If WAN access is required on the OpenTouch Conversation, a default gateway address should be provided by the DHCP server.



11.4 General recommendations

11.4.1 Network engineering

- In SIP mode in the enterprise premises there must be no NAT/PAT device between the mobile and OXO Connect
 - A DHCP server is required. The OXO Connect's embedded DHCP server can be used for serving mobiles. However the OXO Connect's DHCP server has a limit of 20 entries, which can be reached when fixed IP mappings are used.
 - The DHCP server must be configured to send default gateway and DNS servers if the OpenTouch Conversation requires WAN access.
 - Voice traffic can be segregated into a separate VLAN. In this case, a mapping between the VLAN and SSID must be implemented at the access point. Consequently, the Mobile with the dual mode application must have a specific SSID.
 - A QoS policy is recommended for VoIP with packet taggings: DSCP of 46 and 802.1p priority of 6.
- This policy must be enforced on all network devices on the path between the mobile and OXO Connect.
- If a firewall is implemented between the WLAN and the LAN, the rules must allow the flows, see table below.

It is also helpful for debugging to allow the ping – protocol ICMP ECHO.

Protocol	Description	Source (OpenTouch Conversation)	Destination (OXO Connect)
https (tcp)	Web services, configuration, inventory, QoS tickets	Any	443

sip (tcp)	SIP	Any	5059
rtp (udp)	RTP media	32000-32256	32000-32256

11.4.2 VoWLAN engineering

VoWLAN engineering requirements include:

- AP and OpenTouch Conversation "see" each other a -67 dBm or more in all cell areas to be covered
- IEEE802.11 MAC level packet loss must be below 3%
- Signal Noise Ratio should be at least 25 dB
- QoS is recommended when there is non-VoIP traffic on the network that impacts voice quality. AP must be configured to support WMM.
- Roaming between standalone AP's is not seamless. On controller based architectures fast roaming is recommended. In all cases, the roaming delay must be below 100ms .
- The RTT delay must be below 300 ms for VoIP.
- The capacity of the VoWLAN network must be designed to support the planned number of OpenTouch Conversations. Non VoIP traffic must also be considered.

Note:

The iPhone WLAN stack does not support the TSPEC call admission control protocol. It is therefore mandatory to design the bandwidth of network for the required number of devices.

- It is recommended to disable the 802.11b protocol, and in 802.11g to disable the 1,6,9 Mbps speeds.
- The WLAN network must provide a protocol supported by the mobile device. Otherwise there is no connection.
- For OpenTouch Conversation® for iPhone: The 802.11 protocols (b/g, a/n) and frequency (2.4 GHz or 5 GHz) band must be compatible with the iPhone fleet (see table below).

iPhone model	2.4 GHz Band	5 GHz band
3, 3G, 3GS	802.11 b/g	-
4, 4S	802.11 b/g/n	-
5	802.11 b/g/n	802.11 a/n

- For OpenTouch Conversation® for Android: A lot of mobile models can run under android. As a result, verify the WLAN infrastructure and the WLAN capabilities of the corresponding mobile device
- A 100% radio coverage cannot be guaranteed
- The WLAN must comply to VoWLAN requirements

11.5 Troubleshooting tools

The SIP mode serviceability tools include:

- Syslog client embedded in OpenTouch Conversation, see [OpenTouch Conversation for iPhone syslog client](#) on page 164
- OpenTouch Conversation RTP statistics pushed on OXO Connect, see [OpenTouch Conversation RTP statistics pushed on OXO Connect](#) on page 164

- OXO Connect Webdiag VoIP channels statistics, see [OXO Connect WebDiag VoIP channels statistics](#) on page 165
- OXO Connect Webdiag QoS tickets, see [OpenTouch Conversation QoS tickets](#) on page 165
- OXO Connect Webdiag tcpdump, see [OXO Connect webdiag's tcpdump](#) on page 166
- Third party investigation, troubleshooting and analysis tools, see [WLAN analysis tools](#) on page 166
- Tools provided by third party WLAN routers and controllers, see [WLAN analysis tools](#) on page 166
- OXO Connect historic events, see [OXO Connect historic event](#) on page 167
- Logs on OpenTouch Conversation, see [Logs on OpenTouch Conversation](#) on page 167

11.5.1 OpenTouch Conversation® for iPhone syslog client

The OpenTouch Conversation® for iPhone embedded syslog client allows logging on a syslog server available on the local network.

As syslog consumes some WLAN bandwidth, applications internal logs are not only pushed to the server, but are also stored locally in a file on the iPhone.

The user interface for setting the logs parameter (server IP address) are in the advanced debug menu for the application.

Note:

The syslog server is not running on OXO Connect, as its resources are limited (file system size, log file rotation, induced CPU overhead when many clients are logging). So a specific syslog server must be provided by the installer.

11.5.2 OpenTouch Conversation RTP statistics pushed on OXO Connect

The application logs the RTP statistics available in the SIP stack at the end of the call. The statistics are related to incoming RTP flow on the iPhone side.

The statistics include for the two OpenTouch Conversation applications (iPhone and Android):

- Jitter values
- Round trip
- Packets counts, packet losses, duplicated, discarded
- IP address of the peer

The statistics also include for OpenTouch Conversation® for Android:

- WI-FI signal strength (RSSI) min, max and average values
- WI-FI speed
- Number of WI-FI roaming (no cellular)

When the QoS ticket generation is enabled in VoIP menu of OMC, the SIP stack statistics described in [OpenTouch Conversation for iPhone syslog client](#) on page 164 are pushed to OXO Connect and can be displayed in WebDiag in the QoS ticket menu (refer to [OpenTouch Conversation QoS tickets](#) on page 165) or with the NMC (ie 4760).

The statistics are formatted as an OXO Connect QoS ticket and pushed to OXO Connect on a URL similar to the inventory with same security checks: the files are size limited and the push is restricted to a mobile residing on the LAN.

Note:

When the feature is activated in OMC, it is necessary to logout and login again, so that the configuration file is read from the system. The same applies when the feature is disabled in the OMC.

11.5.3 OXO Connect WebDiag VoIP channels statistics

The VoIP channel stat tool in Webdiag provides statistics about RTP for a call in progress or the last call. No history is maintained. When the media is RTP direct, no VoIP channels statistics are available on OXO Connect.

This feature is useful for analyzing voice quality problems.

The available statistics are available in the following directory: Voip Information/Voip Debug/Amcv Debug/DSP stats. It contains:

- Source IP
- Jitter statistics (late, corrupt, lost, out of order packets)
- Echo strength, delay, noise

Last switchings details										
Id	Noise	ERL	Delay	Source IP	Corrupted	Late	Out of Order	Not Received	Not Send	Lost
32	-62.0	30.0	--	172.25.50.10	0	0	0	0	0	7
33	0.0	0.0	0.0	0.0.0.0	0	0	0	0	0	0
34	0.0	0.0	0.0	0.0.0.0	0	0	0	0	0	0
35	0.0	0.0	0.0	0.0.0.0	0	0	0	0	0	0
36	0.0	0.0	0.0	0.0.0.0	0	0	0	0	0	0
37	0.0	0.0	0.0	0.0.0.0	0	0	0	0	0	0
38	0.0	0.0	0.0	0.0.0.0	0	0	0	0	0	0
39	0.0	0.0	0.0	0.0.0.0	0	0	0	0	0	0
40	0.0	0.0	0.0	0.0.0.0	0	0	0	0	0	0
41	0.0	0.0	0.0	0.0.0.0	0	0	0	0	0	0
42	0.0	0.0	0.0	0.0.0.0	0	0	0	0	0	0
43	0.0	0.0	0.0	0.0.0.0	0	0	0	0	0	0
44	0.0	0.0	0.0	0.0.0.0	0	0	0	0	0	0
45	0.0	0.0	0.0	0.0.0.0	0	0	0	0	0	0
46	0.0	0.0	0.0	0.0.0.0	0	0	0	0	0	0
47	0.0	0.0	0.0	0.0.0.0	0	0	0	0	0	0

Legend:

- The value "--" for the Delay means that there is no echo or the delay is constantly varying.
- The value "--" for the Noise means that this parameter is unavailable.
- A number of packet in red means that this number represents more than 1% of all packets received.

Clear

Figure 11.8: RTP tickets in Webdiag

11.5.4 OpenTouch Conversation QoS tickets

OXO Connect provides a QoS tickets logging feature for VoIP including the SIP companion used for dual mode. The tickets are stored locally on OXO Connect and can be viewed in WebDiag tickets provide a history of the VoIP calls.

This feature is useful for analyzing voice quality problems.

The QoS ticket logging must be enabled in OMC : **VoIP->Parameters->Gateway -> RTP Ticket activation**

The new tickets are stored until the logging is disabled in the OMC.

The tickets are available on the following directory: Voip RTP tickets/display (after a freeze command). It contains:

- Local and remote IP

- Packets sent, received, lost packets
- Jitter and latency statistics

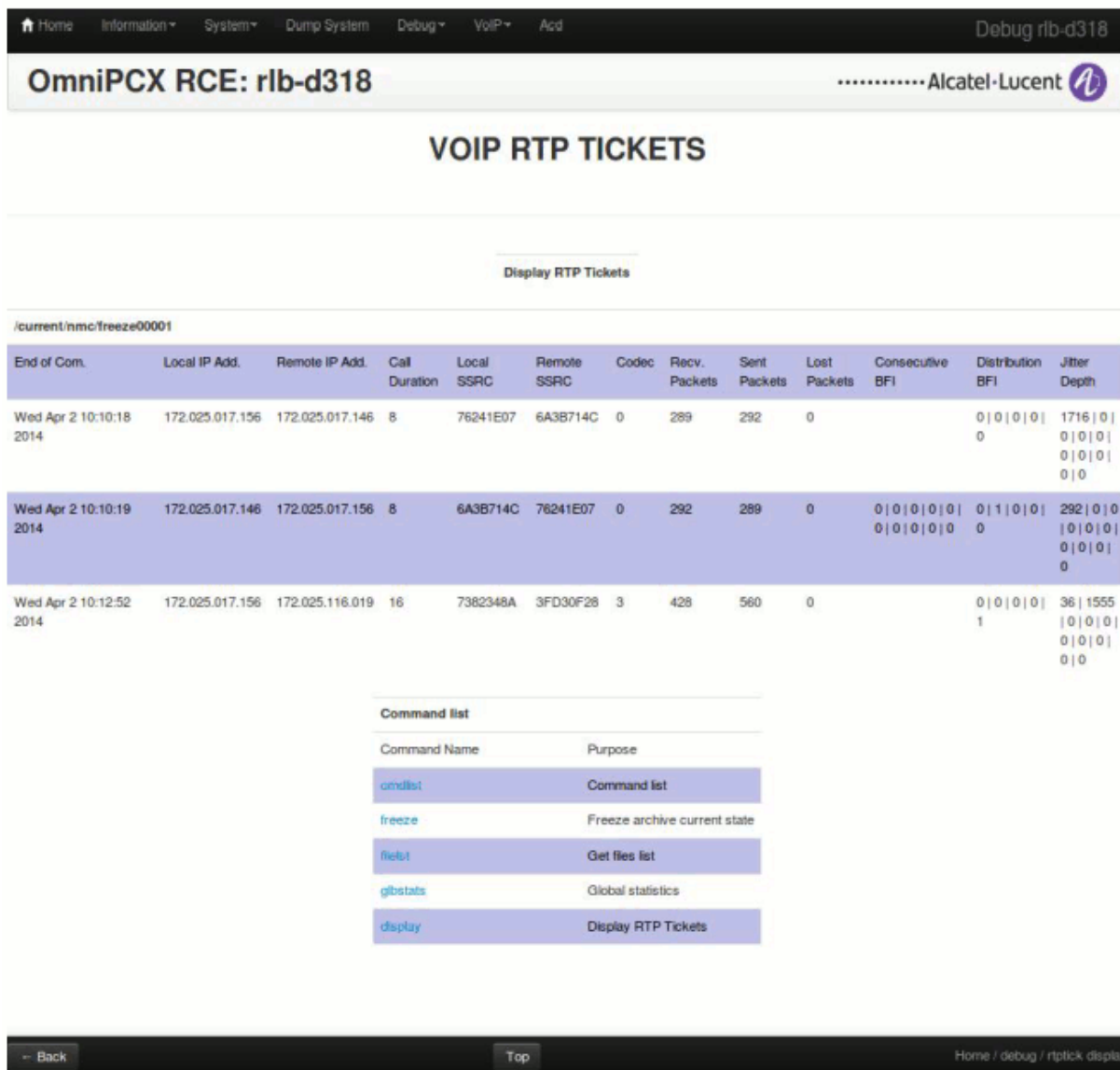


Figure 11.9: RTP tickets in Webdiag

A QoS ticket is created only when a VoIP channel is required by the call. Note that no tickets are produced in case of RTP direct.

11.5.5 OXO Connect webdiag's tcpdump

OXO Connect Webdiag based tcpdump tool can be used to dump IP packets from an OpenTouch Conversation client.

This feature is useful for analyzing early connectivity problems occurring when the mobile connects to OXO Connect, typically to test whether IP packets from the mobile arrive at the OXO Connect.

11.5.6 WLAN analysis tools

WLAN analysis tools consist in:

- Network sniffers: for debugging at protocol level
- Coverage analysis tools, measure RSSI, site survey.
- Protocol analyzers: retransmissions statistics, QoS control

11.5.6.1 Analysis tools

These tools are used for packet and network analysis, they sniff the wireless network on several channels. It is a Windows application running on a laptop with additional USB Wireless keys.

- Wireshark
- Riverbed Airpcap

11.5.6.2 Signal strength measurement

The WIFI signal strength (RSSI) provided on the iPhone is limited to 4 levels, which is not sufficient for assessing the strength of a WiFi signal.

The RSSI is available using the Android APIs. It is not currently managed by the application to update its mobility when the voice quality becomes bad or just before losing the WI-FI signal.

The following tools provide more accurate RSSI measurement:

- Netstumbler: laptop with windows
- Wi-spy <http://www.metageek.net/products/wi-spy/> (spectrum analyzer)
- Android based applications that can be used for getting RSSI: wifianalyzer, network signal info, or OAW utilities available from the Android play store

11.5.7 OXO Connect historic event

Device error events 112 are produced when the dual mode SIP device registration expires. Typically this happens when the OpenTouch Conversation leaves the coverage of the WLAN network. Conversely an event 110 is produced when the SIP device registers.

The SIP devices embedded in OpenTouch Conversation produce an event each time they dissociate from the AP and again when they associate with the AP. As the number of events grows, the historic event table is OXO Connect tend to overflow. In order to avoid this, and also to ease the analysis, the events related to dual mode SIP companion are filtered out, in a separate file that can be viewed in WebDiag (system files -> log files -> historicevt.log).

11.5.8 Logs on OpenTouch Conversation

OpenTouch Conversation provides applicative logs. These log messages are stored locally and can be sent by e-mail, provided that an e-mail access has been configured on the mobile device.

12.1 Presentation

OpenTouch Conversation® for iPhone (also called OTCV iPhone), OpenTouch Conversation® for Android (also called OTCV Android) and OpenTouch Conversation® for Windows Phone (also called OTCV Windows) are communication applications running respectively on iPhone, Android, and Windows Phone platforms and interacting with the OXO Connect; either on the intranet through the wifi interface or remotely (WAN) via a 3G/2.5G/GPRS operator. These applications require a data connection to the OXO Connect and a switched circuit for voice transport. They use a web services session.

My IC Web is a web based application running in a browser. It uses a data connection (http/https) to the OXO Connect. This application can be used on the intranet or remotely (WAN), provided the network has been set up. My IC Web is associated to a set and uses a web services session.

The most common use cases are:

- Terminal in the enterprise and the specific application for mobile phones remotely
- Terminal in the enterprise and My IC Web to change the nomadic behavior of the terminal in a remote location (in a hotel room, at home etc.)
- Augmenting the capability of an Analog phone with services provided by My IC Web.
- Use the specific application for mobile phones as main phone.

Restrictions

The smartphone and nomadic applications are not fully compatible.

Restriction rules are:

- SIP phones and 8082 My IC Phone sets do not support the nomadic feature
- The My IC Web application cannot be associated to the following phone sets:
 - 8082 My IC Phone
 - OTCV iPhone
 - OTCV Android
 - OTCV Windows
 - PIMphony (all versions)

12.2 Available configurations

For details about network configuration of remote accesses, see the section **Network configuration for remote accesses** in document [13].

12.2.1 Single set configuration

12.2.1.1 Handsets compatible with My IC Web

The following sets are compatible with My IC Web:

- IP DeskPhones
- Digital Premium DeskPhones
- Analog sets
- DECT and WLAN sets



Figure 12.1: Handset with My IC Web configuration example

On My IC Web application, nomadic settings are displayed only when the set has the nomadic rights.

12.2.1.2 Mobile smartphone

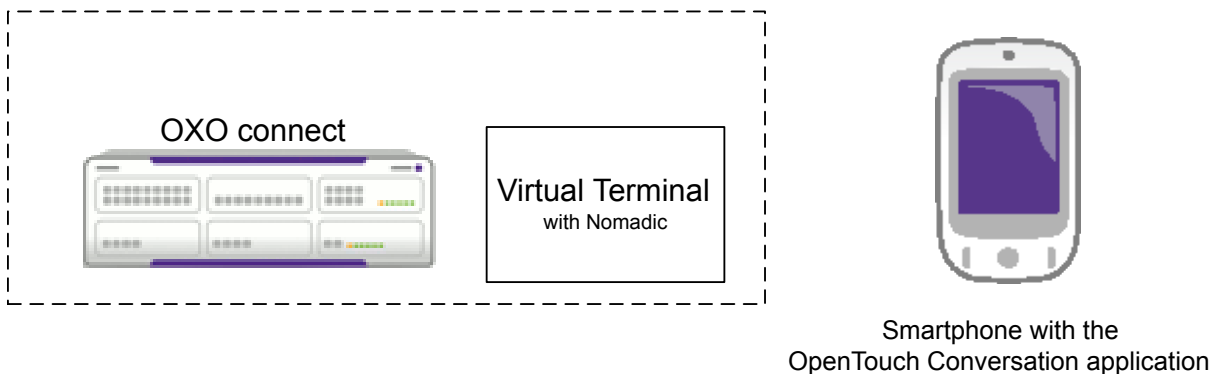


Figure 12.2: Mobile smartphone configuration example

A virtual terminal is associated to the phone on which an OpenTouch Conversation application (OTCV iPhone, OTCV Android or OTCV Windows) is running.

A virtual terminal with the nomadic feature must be declared. The smartphone on which the application is running is associated to the virtual terminal.

Note:

My IC Web cannot be associated to a virtual terminal.

12.2.1.3 8082 My IC Phone

8082 My IC Phone cannot be associated to a My IC Web with the nomadic feature. A work around is possible see: [8082 My IC Phone with nomadic destination](#) on page 171.

12.2.1.4 Handsets compatible with the Nomadic feature

The following sets are compatible with the Nomadic feature:

- IP DeskPhones
- Digital Premium DeskPhones
- Analog sets
- DECT and WLAN sets

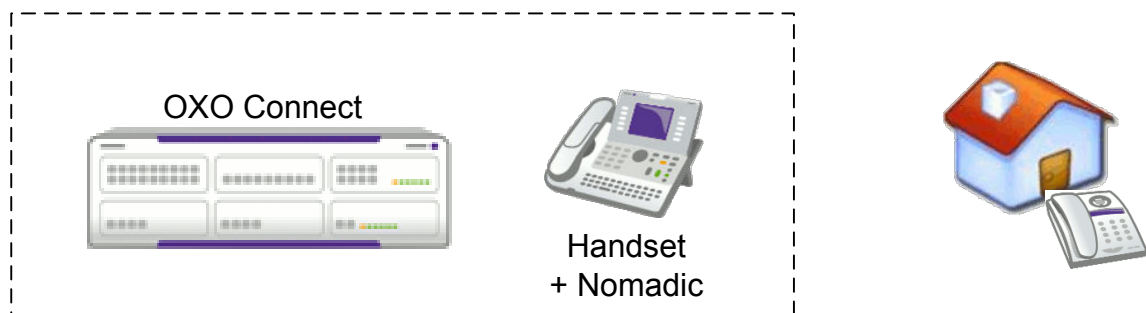


Figure 12.3: Handset with the Nomadic feature configuration example

The external set is associated to a handset with the nomadic feature. The nomadic feature is activated via VMU or PIMphony.

12.2.1.5 Handsets with nomadic and My IC Web

The following sets are compatible with nomadic and My IC Web:

- IP DeskPhones
- Digital Premium DeskPhones
- Analog sets
- DECT and WLAN sets

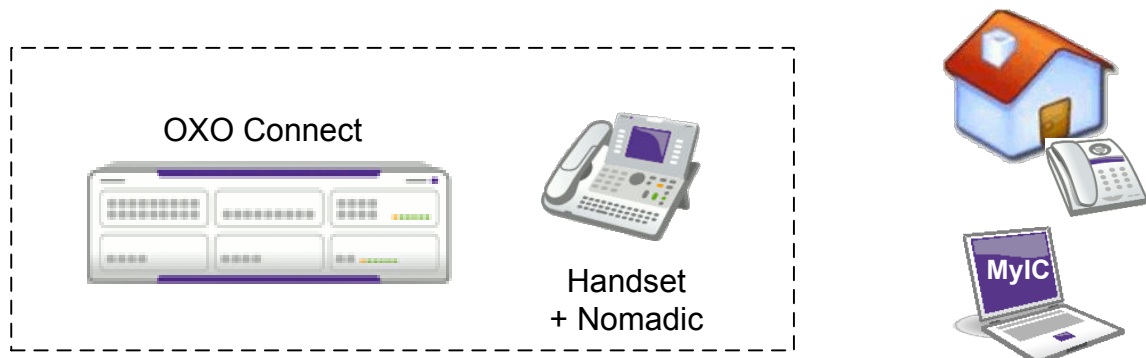


Figure 12.4: Handset with nomadic and My IC Web configuration example

The external set is associated to a handset with the nomadic feature. The nomadic feature is activated via the My IC Web application.

12.2.2 Multi-set configuration

The multi-set feature is used to work around some restrictions.

12.2.2.1 Handset and smartphone

The mobile virtual terminal is the secondary set in a multi-set configuration.

The primary set is one of the following:

- IP DeskPhones
- Digital Premium DeskPhones
- Analog set
- DECT and WLAN set
- SIP set

The secondary set supports the nomadic feature. This nomadic feature is activated by the application running on the smartphone.

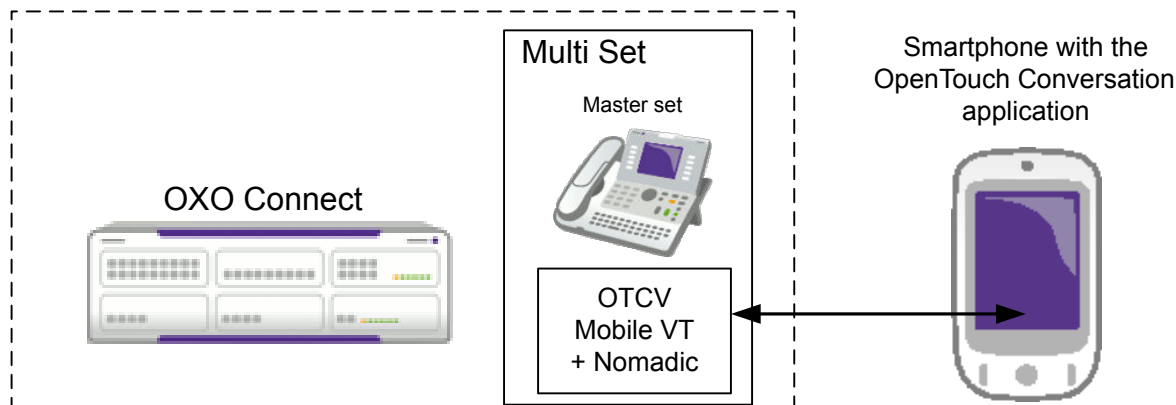


Figure 12.5: Handset and smartphone configuration example

12.2.2.2 8082 My IC Phone and smartphone

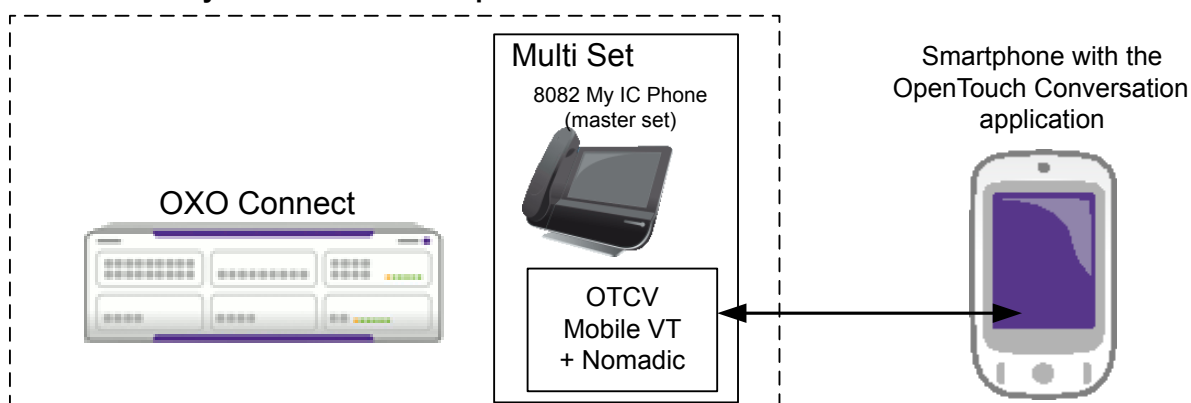


Figure 12.6: 8082 My IC Phone and smartphone configuration example

The 8082 My IC Phone and the virtual terminal are included in a multi-set configuration.

The virtual terminal, which is the secondary set, supports the nomadic feature. This nomadic feature is activated by the application running on the smartphone.

12.2.2.3 8082 My IC Phone with nomadic destination

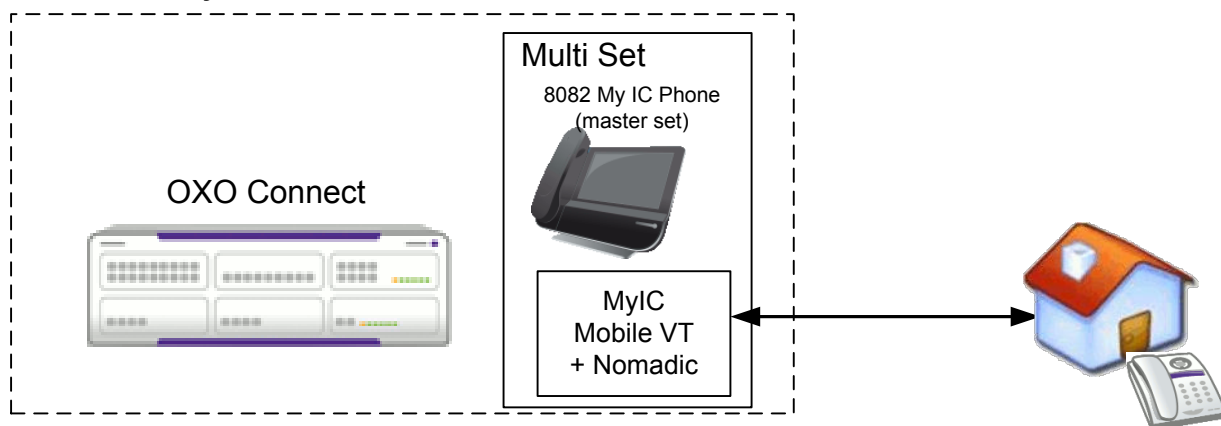


Figure 12.7: 8082 My IC Phone with nomadic destination configuration example

The 8082 My IC Phone and the virtual terminal are included in a multi-set configuration.

The virtual terminal which is the secondary set supports the nomadic feature. This nomadic feature is activated by the VMU or PIMphony.

12.2.2.4 8082 My IC Phone with My IC Web and nomadic destination

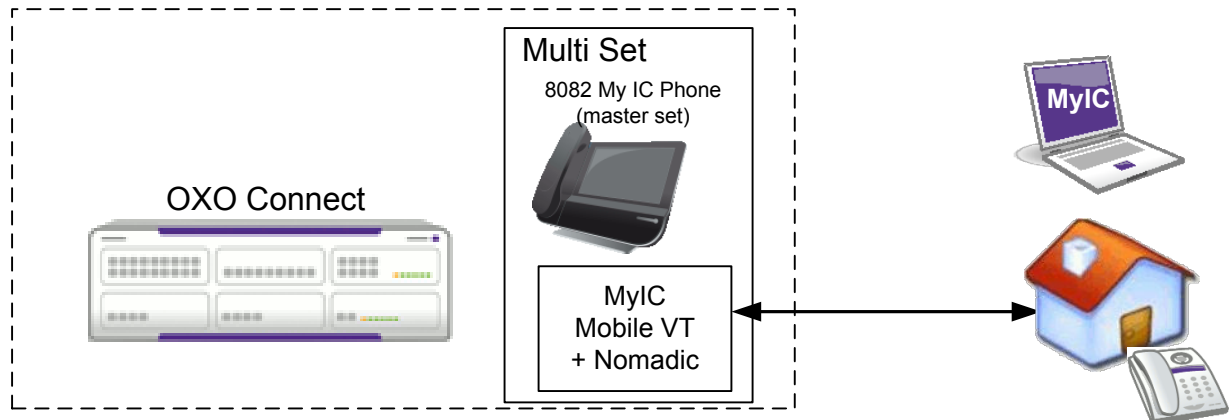


Figure 12.8: 8082 My IC Phone with My IC Web and nomadic destination configuration example

The 8082 My IC Phone and the virtual terminal are included in a multi-set configuration.

The virtual terminal, which is the secondary set, supports the nomadic feature. This nomadic feature is activated by the My IC Web application.