IP-DECT Lite
For OXO / SMB market

Customer Engineer Manual for SIP Connectivity

4080 IP-DECT

8340 Smart IP-DECT

8AL90870USBA ed01 – 10/2013

Contents

Preface

This manual is valid for IP-DECT Lite system.

IMPORTANT:

This manual gives information for setting up an IP-DECT Lite system. However, the IP-DECT Lite is normally part of an IP network. The success of the installation depends on the structure and components in the IP network. Make sure that you have sufficient knowledge of the customers IP network.

The IP-DECT Lite is also a wireless data communication system. This requires knowledge of radio signal propagation. The radio signal propagation in IP-DECT Lite requires a different approach than for the traditional DECT systems. The success of the installation also depends on the radio signal propagation. Make sure that you have sufficient knowledge about this subject as well.

It is strongly advised to follow the IP-DECT Lite training. Please contact your IP DECT supplier.

No legal rights can be obtained from information in this manual.

PRODUCT DISPOSAL INFORMATION (EN)

For countries in the European Union

The symbol depicted here has been affixed to your product in order to inform you that electrical and electronic products should not be disposed of as municipal waste.

Electrical and electronic products including the cables, plugs and accessories should be disposed of separately in order to allow proper treatment, recovery and recycling. These products should be brought to a designated facility where the best available treatment, recovery and recycling techniques is available. Separate disposal has significant advantages: valuable materials can be re-used and it prevents the dispersion of unwanted substances into the municipal waste stream. This contributes to the protection of human health and the environment.

Please be informed that a fine may be imposed for illegal disposal of electrical and electronic products via the general municipal waste stream.

In order to facilitate separate disposal and environmentally sound recycling arrangements have been made for local collection and recycling. In case your electrical and electronic products need to be disposed of please refer to your supplier or the contractual agreements that your company has made upon acquisition of these products.

For countries outside the European Union

Disposal of electrical and electronic products in countries outside the European Union should be done in line with the local regulations. If no arrangement has been made with your supplier, please contact the local authorities for further information.

THIRD PARTY SOFTWARE

Within the SRTP and TLS, open libraries are applied. The following text is applicable for these open libraries:

SRTP

For SRTP version 1.4.4 is applied. The following license text is applicable to the SRTP library:

Copyright (c) 2001-2005 Cisco Systems, Inc. - All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Cisco Systems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

TLS

For TLS version openssl-0.9.8e of the OpenSSL library is incorporated. The following license text is applicable to the OpenSSL Library:

OpenSSL License:

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

> Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
>
> Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
>
> All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
>
> If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence].

1 DECT System Characteristics

1.1 General Description

The **DECT** System allows mobile users to use the switched telecommunication facilities provided by a SIP Proxy system. Such a mobile user can make or receive calls by using a cordless handset. Many call handling facilities of the SIP Proxy are available on the cordless handset. As the cordless connection is a digital connection, other services will also be possible in the future.

The Digital Enhanced Cordless Telecommunication (**DECT**) interface has been developed by the European Telecommunication Standards Institute (**ETSI**).

Mobile users carry a portable handset which uses a radio transceiver to communicate with the DECT System. In this manual the DECT system is the IP-DECT Lite system connected to the SIP Proxy via an IP Ethernet connection. The radio transceivers are placed within the working area so that a portable handset/telephone is always within radio coverage area of at least one such transceiver.

The portable telephone is called a Portable Part (**PP**) according to the DECT standard. However, in this manual the portable telephone is also referred to as handset. It also contains a transceiver.

A radio transceiver in the DECT System is called the Radio Fixed Part (**RFP**) according to the DECT Standard. The RFP is also referred to as a base station. However, in the IP-DECT Lite configuration, the RFP is comprises more than just a transceiver, and is therefore called: **DAP** (DECT Access Point).

Figure 1-1 “DECT System Parts (General)” shows a general DECT system setup.

Figure 1-2 “DECT System Parts in an IP Solution as Add-on to a PBX” shows a general IP DECT Solution. It shows the basic system setup for the IP-DECT Lite system.

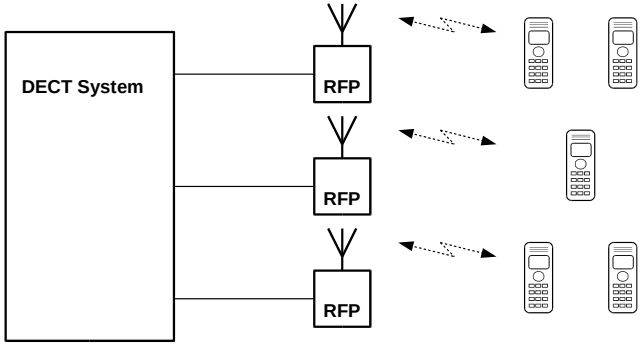
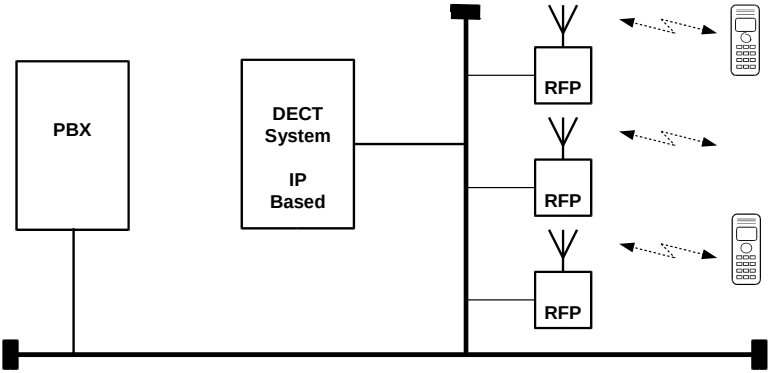


Figure 1-1 “DECT System Parts (General)”



Note: This figure shows a general system setup.
If applied to NEC IP DECT configuration, the:

DECT System IP Based = DAP Controller
PBX= OXO
RFP = DAP (DECT Access Point)

Figure 1-2 “DECT System Parts in an IP Solution as Add-on to a PBX”

Note : The figure 1-2 shows a general system setup. If applied to IP-DECT Lite solution, RFP is DAP (4080 IP-DECT AP or 8340 Smart IPD-DECT) and DECT System IP Bases is the DAP Controller that is integrated in the DAP.

The radio area covered by a single RFP (DAP) is called a **cell**. The RFPs (DAPs) are located so that the cells overlap slightly and the PP can remain in contact with the DECT system when moving from one cell to another. A group of cells belonging to one DECT system is called a cluster. According to the DECT standard, the maximum number of simultaneous calls per RFP can be 12. (The DAP in the IP-DECT Lite supports up to 12 simultaneous calls, depending on the licenses.)

The number of RFPs (DAPs) needed to cover a certain area (within which the mobile telephone users might roam) depends on many factors such as:

- The size of the area.
- The nature of the area:
  - The number and the size of buildings in the area.
  - The radio propagation characteristics of the building(s).
  - Materials used for walls, floors, elevator shafts, reinforced glass, doors etc.
  - Strong magnetic fields in the area (e.g. as result of welding equipment, radar, etc.).
- The amount of telephone users in an area, and how often they make or receive calls.

The speech signal through the air will be encrypted, if the portable handset allows it, to ensure the privacy of the conversation. This encryption is done fully automatically, without the intervention of a technician.

1.2 RFP-PP Communication

The radio link between the RFP and a PP can carry information on any one of ten carrier frequencies and in one out of twelve pairs of time slots (12 in each direction). The ten carrier frequencies are separated by 1728 kHz. The frequency range depends on the region where DECT is used:

- 1880 MHz - 1900 MHz for European countries
- 1910 MHz - 1930 MHz for Latin America region
- 1900 MHz - 1920 MHz for China
- 1920 MHz – 1930 MHz North America (lower transmission power, –3 dB)

The modulated date rate is 1152 kb/s. DECT uses in the OSI physical layer the following multiplexing techniques:

- FDMA (Frequency Division Multiple Access);
- TDMA (Time Division Multiple Access);
- TDD (Time Division Duplex).

The RFP-PP communication radio signal carries time division multiplexed frames; each frame is 10ms long. Each frame contains 12 time slots which carry data from RFP to the PPs, and 12 time slots which carry data from PPs to the RFP. This means that two time

slots in every frame are needed for a full duplex connection to a PP. See Figure 1-3 “Carriers and Timeslots in the DECT Air Interface”.

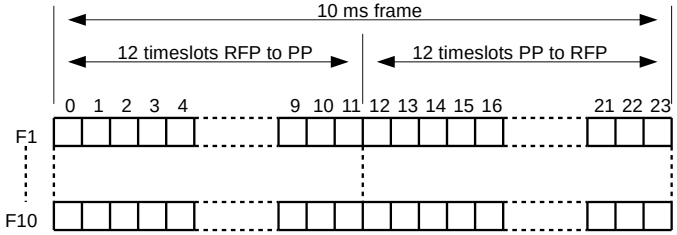


Figure 1-3 “Carriers and Timeslots in the DECT Air Interface”

Each time slot may carry 32 kbs Adaptive Differential Pulse Code Modulated (ADPCM) speech/user data. Each time slot pair can contain ADPCM speech/user data on any one of the ten carrier frequencies so that the RFPs carrier frequency often needs to be changed between time slots: Refer to Figure 1-4 "Each time slot can use any of the 10 Carrier Frequencies". The information within the time slot does not completely fill the time slot; time is allowed for propagation delays, ramp up and ramp down of the transmitter and for switching of the carrier synthesizer between slots.

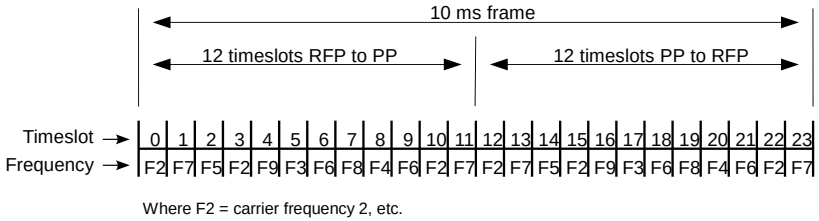


Figure 1-4 "Each time slot can use any of the 10 Carrier Frequencies"

A PP can use any of the 12 time slots (in each direction) on any of the 10 frequencies for a full duplex connection. So a maximum of 120 full duplex channels are available for connections to the PPs, within a cluster of a micro-cellular DECT system. In fact, this is only possible under ideal conditions; no disturbance, no interference, no other channels used,

etc. Normally the conditions are not ideal in office or factory buildings, but the number of channels available will still be more than sufficient.

Note that there is always a fixed relation between the downstream timeslot number (from RFP to PP) and the upstream timeslot number (from PP to RFP) in one connection:

- Upstream timeslot number = downstream timeslot number +12.
- Upstream and downstream timeslot in one connection use always the same carrier frequency.

1.3 Beacon Signal

1.3.1 General

The beacon signal is a signal which is transmitted by an RFP in case the RFP is idle (no active calls).

This beacon signal contains the System Identifier of the DECT System, the so called PARI (Primary Access Rights Identifier) and the number of the RFP, the RPN (Radio Part Number). By means of this information the PP recognizes to which system a signal belongs, and whether it is subscribed to that system or not. When there is a call for a PP, it also contains paging information.

When the RFP is not idle (there is an active call via the RFP), the beacon signal information is also transmitted in the call connection. Therefore, the beacon signal is not necessary at an RFP which has one or more calls active. In the IP-DECT Lite, solution, there are two beacon signals transmitted per RFP (DAP) when the RFP (DAP) is in idle condition. If there is a call only one beacon signal remains active. When there are a number of calls via the RFP (DAP), no beacon signal is transmitted anymore.

1.3.2 Beacon Signal and PP

When the PP is in idle condition (not involved in a conversation) it scans the environment for the signals of a nearby RFP (DAP). It locks onto the best signal that can be found. This signal can be a beacon or a channel which is used for a call, because such a channel contains the beacon signal information.

The PP uses the signal to synchronize its timing with the central system, and then it monitors the information transmitted via that RFP for calls to itself.

If the PP detects too many errors in the received signal (due to interference or weak signal) the PP tries to find another better signal and locks onto another RFP.

In this way, the PP user can move around the area from cell to cell and remain in contact with the DECT system via a radio link with a very good quality.

1.4 Call Handling Procedures between PP and RFP

1.4.1 Setting up a Call

In case the PP user wants to make a call, he/she goes off hook. The PP selects an unused channel at the RFP to which it is locked. This channel is in one of the timeslots (0 ... 11) from RFP to PP; for the communication from the PP to the RFP, the corresponding timeslot is selected in the timeslot range 12 ... 23. This results in a full duplex connection via the air. The connection setup goes through this RFP (via the IP-DECT system integrated in the RFP) to the SIP Proxy (OXO). (The voice connection is setup between the RFP/DAP and the SIP User Agent.)

1.4.2 Paging and Answering a Call

If a PP is locked to a system, it continuously scans the beacon signal for paging information. (This beacon signal can be part of an existing call or as standalone beacon.) If the PP recognizes its own address in the paging data, it selects an unused channel at that RFP to answer the call. This channel is in one of the timeslots (12 ... 23) from PP to RFP; the RFP uses the corresponding timeslot (0 ... 11) from RFP to PP to communicate with this PP. After the setup of the channel/bearer has been successful, the handset starts alerting the mobile user. The user presses the "off-hook" key to answer the call. Then the speech path is opened via the bearer that has already been setup.

1.4.3 Encryption

Most portable sets are capable of encryption and so the user data is encrypted over the air interface. This ensures the privacy of the conversation. Encryption is a process by which the digitised speech is "scrambled" making it impossible for anyone monitoring the frequency to listen to the conversation. For this scrambling, a DCK (DECT Ciphering Key) is used. This is a key which is agreed at the first time data has been transferred between the PP and the RFP (the moment that the PP "locks" to the DECT system).

1.5 Cluster Arrangement

1.5.1 General

A cluster is defined as a logical group of radio cells belonging to one DECT system. Within this arrangement bearer handover is possible. Figure 1-5 "Cluster Arrangement" shows an ideal cluster arrangement of radio cells in which each cell has a boundary with a number of other cells. An omnidirectional radio signal is transmitted equally in all directions so that the actual radio signal from the RFP in cell 1 overlaps slightly into cell 2, cell 3, cell 4, and so on. Similarly, the radio signal from the adjacent cells overlap into cell 1. So, cell 1 can be seen as the centre of a cluster of cells. If a certain frequency is used in a certain timeslot in cell 1, it cannot be used in any of the adjacent cells in the same timeslot because of interference at the cell boundary. But that same frequency can be used in cell 8.

Thus, within a cluster a certain channel/frequency combination can be used again, simultaneously, only if the cell which uses such a combination does not interfere with another cell which uses the same combination.

1.5.2 RFP Behaviour in a Cluster

Each RFP constantly scans the area for signals in each channel. These signals can be generated by other RFPs or other equipment. The RFP selects one or two free channels to transmit the beacon signal. (The number of beacon signals depends on the number of active calls via the RFP.)

1.5.3 PP Behaviour in a Cluster

The PP also picks up all sorts of signals which may come from the closest RFP, the next cell or from outside equipment. It locks onto a good RFP signal, and when it must make or receive a call it chooses a channel with the least interference to do this.

When a call is made to a portable telephone then that telephone must be paged. This means that all RFPs transmit a paging message. The information in each active timeslot transmitted by the RFP contains paging data, whether it is in use for a connection or being used only as a beacon. If an idle PP is locked onto a beacon it examines the signalling data in that signal for paging data. Thus, it always receives all paging requests, so any calls to that PP will be received and recognized. When a paging request is detected for this PP, it starts setting up a connection with the RFP. The PP scans the channels regularly so that it knows which channels are available at the nearby RFP. The PP selects a channel which is not being used. It uses this channel to set up the call.

The PP alerts the PP user, who can then answer the call.

In case the PP user wants to make a call (own initiative), he/she presses the off-hook button. It starts setting up a connection with the RFP. (The PP scans the channels regularly so that it knows which channels are available at the nearby RFP.) The PP selects a channel which is not being used and uses this channel to set up the call.

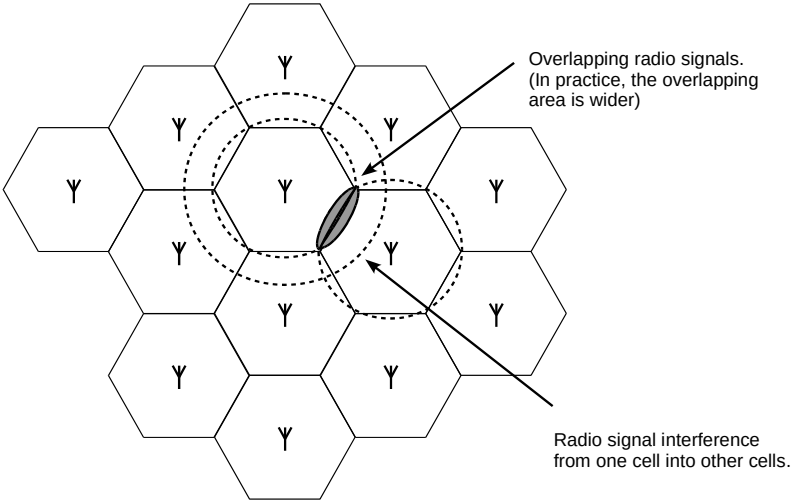


Figure 1-5 "Cluster Arrangement"

1.6 Handover

Both the RFP and PP monitor the quality of the radio link. If the interference on a certain carrier frequency and timeslot combination causes problems, it might be necessary to switch to another frequency and/or timeslot at that same base station. This is called intra-cell handover. This handover procedure requires that the connection can be supported on 2 channels simultaneously, for a while, to allow a "seamless handover" (no breaks and hiccups during the handover). First, the new channel is chosen and the connection is set up via this channel, while the old channel is still in use. Then the old channel is disconnected.

If the mobile user roams from one cell to another, during the conversation, he goes probably out of range of the first RFP and into the range of the second. In that case, when the quality of the transmission requires it, the radio link switches over to the new RFP. This is called inter-cell handover. Once again it is a seamless handover.

Note: *A handover is always initiated by the PP!*

1.7 Call Quality Control

Both the RFP and the PP monitor the quality of the call.

If the PP decides that the quality is not acceptable, it can do one of three things:

Request that the RFP uses its other antenna to communicate with the PP. The signal in the cell may suffer from fading, so that at one place the signal might be poor while very close to it the signal may be acceptable. To counteract this, each RFP has two antennas mounted close together. The system tries to select the best antenna for each channel separately. This method of using two antennas is referred to as **antenna diversity.**

If the quality of the connection warrants it, the PP can request a handover to another channel. That channel may be on the same RFP (intra-cell handover) or on another RFP (inter-cell handover).

During handover, the communication to the PP is built up over the new channel so that for a short time the communication is available over both the old and the new channel. Then the old channel is disconnected. The user does not notice any break in the communication due to handover.

Mute the output (voice connections). It blocks the stream of information from radio signal to user (ear piece, in a telephone). This stops noisy signals being passed on to the user. It is done as a temporary measure, only. Note that muting is done on both ends of the connection independently.

If the RFP decides that the quality of the connection to a certain PP is not acceptable it can do one of three things:

Use the other antenna (antenna diversity). The PP does not notice the change.

Tell the PP that a handover is necessary. The PP always initiates the handover after selecting the best channel as seen from the PP.

It can temporarily block the data stream from PP to the SIP Proxy. (Note that muting is done on both ends of the connection independently.)

1.8 Subscription and De-Subscription

Before a PP can be used, it must be subscribed (registered) to the system. That means that a relation must be defined between the DECT System and the PP. There are three identifiers used to define the relation between the system and the PP:

- **IPUI (International Portable User Identity)**
  This is the identity number of a PP. It is issued from the system to the PP during subscription. From that time onwards, the PP is recognized by the system at its IPUI. This number is a unique number in the system, there is no other PP with the same IPUI.

- **PARK (Primary Access Rights Key), PARI (Primary Access Rights Identity)**
  The PARI is a worldwide unique identifier for an individual DECT system. When stored in the handset, it is called the PARK. The unique DECT system identifier (PARI) is delivered on a certificate, together with the system. It must be entered in the system manually.
- **UAK (User Authentication Key)**
  This is a secret key which uniquely defines the relation between the PP and the DECT system (PARI or SARI)

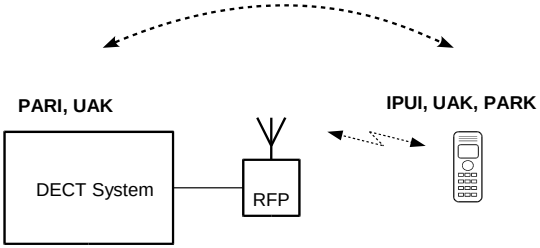


Figure 1-6 "UAK Relation between the IPUI and the PARI"

Note: This is a logical representation (DAP = DECT system + RFP).

When a PP is subscribed (made known) to a DECT system, the relation between the PARI of the DECT System and the IPUI of the PP is defined, see Figure 1-6 "UAK Relation between the IPUI and the PARI". The PARI is stored in the PP as PARK, the PP gets a unique identifier (IPUI) and a secret key (UAK) is assigned to the relation between the PP and the DECT System. From now on the PP knows to which system (PARI) it is subscribed. (In this section only the PARI is mentioned.)

For the subscription procedure the OMC must be used. OMC provides access to the configuration settings in the DAP, which controls the DECT System. Via the OMC subscriber list, one or more IP-DECT accesses can be created and then selected to start the subscription procedure of the (these) extensions (PP). Then the DAP generates a code ("PIN code" or also called "Authentication Code") which is visible via the OMC GAP Registration window. This code must be entered in the PP within a certain time period. If the operation has been completed successfully, the PP is subscribed to the system and is allowed to make and receive calls as soon as the SIP registration sent by the DAP to the OXO has been accepted.

A portable can be subscribed to more than one DECT system. Therefore, it can be used in areas covered by different DECT systems or in different areas with their own DECT system. This allows you for example, to use the same PP for the DECT system which is operational in your company and also for your home DECT. Also if the company is located at different

sites, it is possible to use the same PP at the different sites, if DECT systems are present on these sites. It has a different extension number for each DECT system. It cannot roam from one of these areas to the other, while busy with a conversation. The user of the portable must ensure that his set is communicating with the required DECT system, when making calls in a certain area. This may be done manually by a selection key, depending on the type of the portable. There are also PPs which selects DECT systems automatically.

The OMC can be used to unregister the PP.

When a portable is unregistered via OMC and is within reach of the radio signals, the DAP and the PP exchange information which results in the de-subscription of that PP. It is no longer recognized by the DECT system and it is free to be subscribed again. This is the normal way to de-subscribe a portable set.

If a portable has been disabled, but the DECT System couldn't reach the PP and complete the de-subscription (portable has been lost or damaged), the OXO forces the removal of the portable from the DAP. In that case, the subscription data in the portable has to be removed manually via local MMI.

As long as a DAP is not reachable, handset registration/deregistration is not possible.

2 DECT IN IP NETWORK

2.1 System Architecture

In

Figure 2-1 "IP-DECT Lite - System Configuration" you see the general configuration of the IP-DECT Lite system in an SIP Proxy configuration.

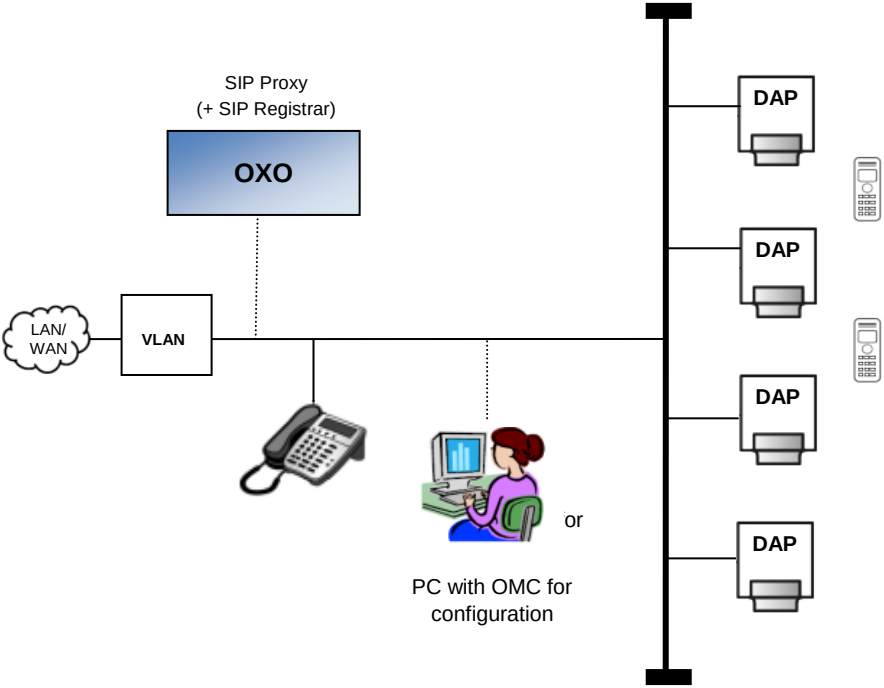


Figure 2-1 "IP-DECT Lite - System Configuration"

- **There are two generations of DAP types: 4080 IP-DECT AP and the 8340 smart IP-DECT AP. The 8340 series is the latest model.**
- **IP-DECT APs (DAP) : DECT Access Point is the actual DECT transmitter/receiver.**
- **IP-DECT APs supports up to 12 simultaneous calls and they operate license free.**
- **IP-DECT APs are powered via the Ethernet interface (PoE).**
- **Besides radio traffic, the IP-DECT APs take care of subscription control and call control data handling to/from the SIP Proxy.**
- **IP-DECT APs are available with either internal antennas or external antennas.**
- **OXO has a SIP Proxy and Registrar embedded:**

  SIP Proxy
  The SIP Proxy Server accepts session requests made by a SIP UA (User Agent). The UA in this configuration, is the user that is subscribed to the IP DECT system, or any other SIP phone. When the SIP Proxy receives a call requests it will normally consult the SIP Registrar server to obtain the recipient UA's addressing information. The SIP Proxy can be combined with the SIP Registrar.

  SIP Registrar
  The SIP Registrar server contains a database with the address information of all User Agents in the SIP domain. The Registrar server receives and sends UA IP addresses and other pertinent information to the SIP Proxy server.

- **VLAN Router**
  The VLAN Router is a "switch" that separates the IP traffic between the WAN and the VLAN. It is strongly recommended to setup a dedicated Ethernet network for the IP-DECT Lite configuration because of the high Quality of Service (QoS) requirements. The load on the network can be high due to rerouting of calls via the LAN.
- **PC with OMC**
  Via the OMC, you can subscribe handsets and change limited number of configuration settings.

When there is a call for a DECT handset, SIP Proxy sends a call setup message (Invite) to a DAP. The DAP forwards this message to the handset. When the handset goes off hook, the speech path is established between the handset, the DAP (as SIP UA) and the other party (other UA).

In the following sections, processes in the system are described in more details.

2.2 Handset Subscription/Registration

Before you can use a handset, the handset must be subscribed to the IP-DECT Lite system. Besides that the handset must be registered as UA in the OXO (SIP Registrar server). Subscription of the handset requires manual intervention, registration is done automatically.

Figure 2-2 “Phases in the Subscription Process” shows the phases in the subscription process.

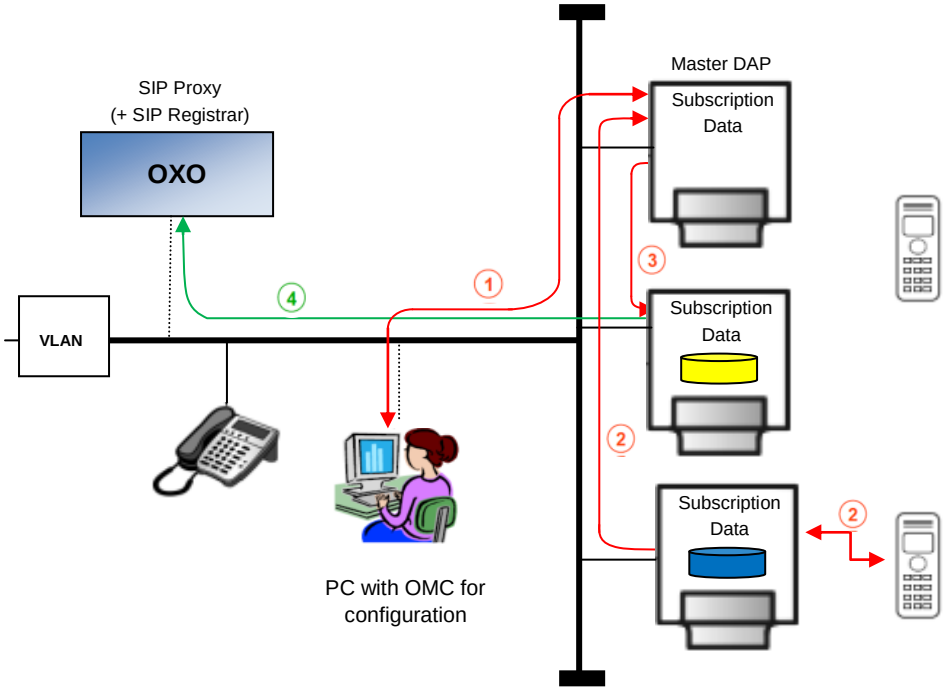


Figure 2-2 “Phases in the Subscription Process”

The following phases are distinguished in the subscription process.

The administrator starts a subscription process via the GAP Registration window of OMC. This window is accessible from Subscriber/Basestations List once an IP-DECT access has been created.

The administrator “starts” a registration, which means that the subscription process is started on the DAP. The IP-DECT Lite is now waiting for action from a handset.

Now the subscription must be executed from the handset. The handset user must enter the PIN code that is displayed on the GAP Registration window of OMC. When the PIN code is entered on the handset, the subscription record is created in the Master DAP Database.

The Master DAP will distribute the subscription data to one of the DAPs. Distribution has the following characteristics:

- The Master DAP tries to distribute the subscription records equally over the DAPs.
- The maximum number of subscription records per DAP is 25.
- Once a subscription record is stored into a DAP, it will normally not be moved to another DAP anymore. There are two exceptions on this: If you “Delete” a DAP manually from the DAPs list in the OMC Subscriber/Basestation List or when a DAP goes down, the subscription records of that DAP will be distributed over the remaining DAPs

The DAP sends a SIP Register to the OXO’s SIP Proxy/Registrar to register itself as a SIP extension (UA). This is done on behalf of the handsets subscribed on it and per handset.

After the subscriptions are executed, each DAP contains a number of subscription records. All the DAPs contain subscription data of all handsets in the system. If the Master DAP is disconnected, the system remains operational, as another DAP will take over the Master DAP role.

The subscription records in the DAPs are stored in Flash Memory.

2.3 Automatic Distribution When DAP Down

When a DAP goes down, the subscription records in that DAP are not accessible anymore, and therefore, the associated handsets cannot be used anymore. However, the subscription records of a broken DAP are automatically distributed over other DAPs after 10 minutes down time. This automatic distribution is not done if more than one DAP are not reachable at the same time. If a DAP becomes reachable again after the automatic distribution of its handsets, this DAP does not retrieve its handsets.

If the master DAP is no more reachable, the DAP with the lowest RPN will become the new master DAP.

This automatic distribution is managed by the Master DAP

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

If you replace a faulty DAP before the 10 minutes down time, the new DAP will retrieve the subscriptions of the faulty one.

2.4 Handset Registration in SIP Registrar

DECT Handset registration means that a DECT Handset makes itself know to the SIP Registrar. This information is needed to store relation between the extension (UA) number and its IP address and/or the full computer/device plus domain name. The Registrar holds a database containing the data of all UAs that are registered in the (local) domain.

Registration data can be stored for a limited time period only, which is by default 3600 seconds. This time period is issued to the Registrar server. The Registrar server normally accepts this time period, but may also change the time period. The Registrar tells the IP-DECT Lite system the stored time period (in the “ACK” message). When the time expires, the registration is removed from the Registrar. However, the IP-DECT Lite system knows when the timer expires and will execute a register again.

An IP DECT handset registers its number:

- at subscription
- when the DAP holding the subscription record of an extension (UA) starts up

***Note**: The registration takes place between the DAP where the subscription record of the handset resides and the SIP Registrar. So, the handset does not have an IP address and the handset does not contact the SIP Registrar directly.*

2.5 Handover Mechanism

The handover mechanism ensures seamless handover from one DAP to the other DAP in a multi DAP (radio) environment. So in other words, when a handset is in an existing voice call, it can move between the DAPs without losing the connection or hearing a click.

In **Erreur ! Source du renvoi introuvable.** a call is depicted between a SIP IP telephone and a DECT handset with extension number 200. The speech path is a peer-to-peer VoIP connection between the SIP IP extension and a DAP.

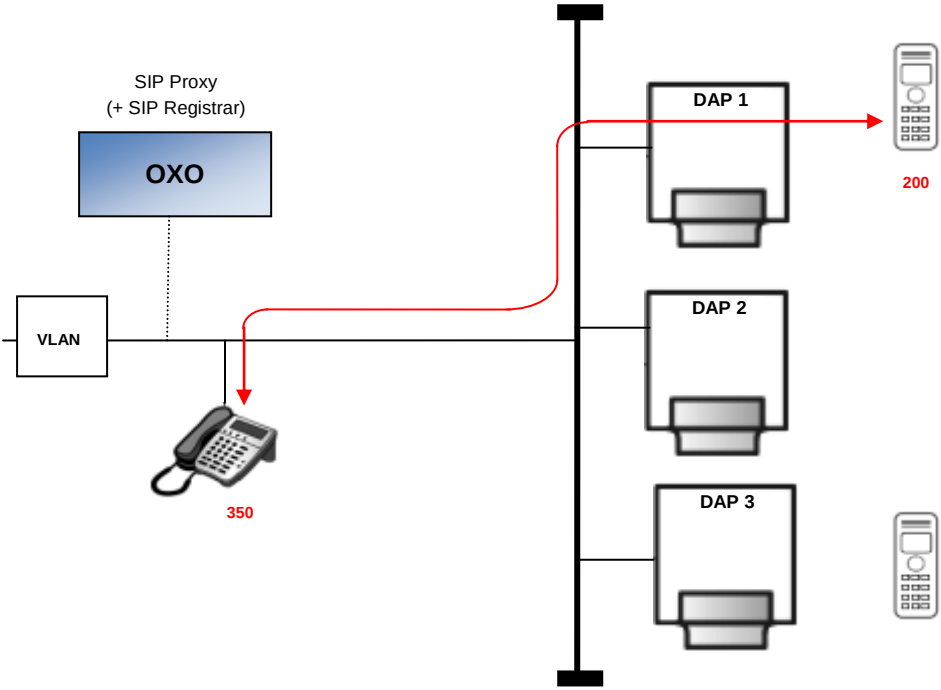


Figure 2-3 “Call connection before handover”

However, handset 200 moves from one DAP to another DAP. See **Erreur ! Source du renvoi introuvable.**. The handset searches for a better radio signal, and detects that the second DAP has a better signal. The handset issues a request for handover to the new DAP. However, the new DAP does not know where the existing voice connection to handset 200 resides so it issues a multicast request for searching previous connection to handset 200 over the network with DAPs. The original/first DAP responds to this request because the call was initially be set up via this DAP.

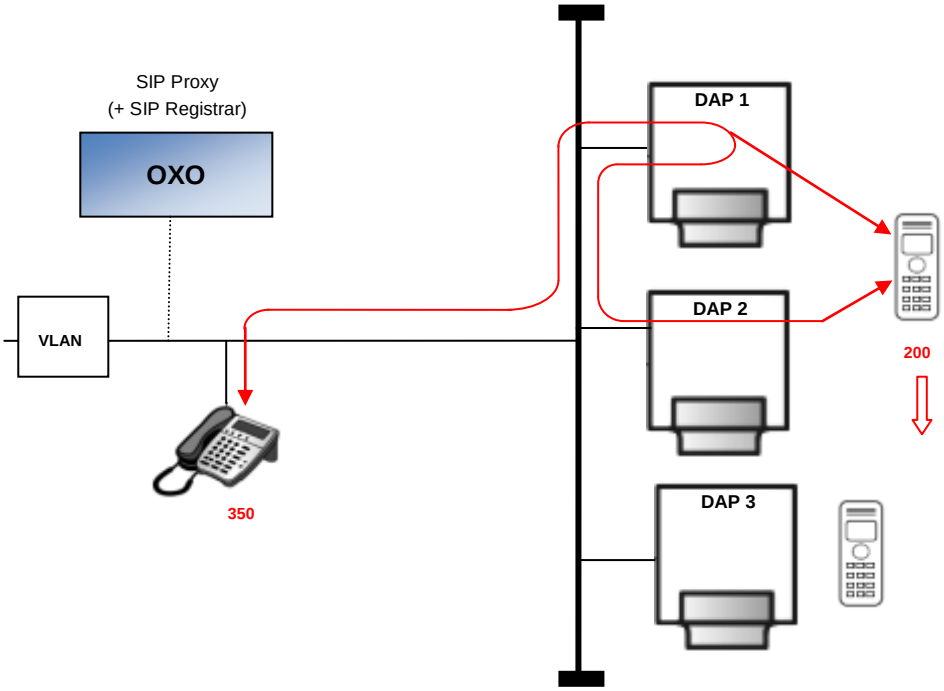


Figure 2-4 "Handover action started"

Now the connection is *copied* from the original/first DAP to the second/new DAP. See **Erreur ! Source du renvoi introuvable.**. The original/first DAP DAP will release the *radio connection* to the handset and the new connection remains in place. Note that the original connection is not removed from the original DAP, but this DAP "relays" the connection to the second DAP. The original DAP cannot release the IP voice connection, because the IP voice connection between the SIP IP extension and the DAP 1 is established, based on a combination of sockets. This combination is fixed during the connection.

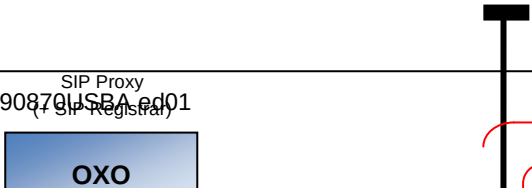


Figure 2-5 "Handover taken place, new connection active"

Note: *When a second handover takes place from DAP 2 to DAP 3, DAP 1 will setup a second relay to DAP 3 and* ***REMOVES*** *the relay to DAP 2. So the maximum number of relayed RTP streams per call in the network is 1.*

2.6 Radio Synchronization

2.6.1 How it Works

The radio network structure supports seamless handover of existing calls. This means that when there is a call, and the handset moves from one radio to another, that other radio should take over the call. The call may not be interrupted and the user may not hear any click or what so ever. If the handset needs to re-synchronize to the other radio, then the user will hear at least a click. So, supporting handover requires an accurate synchronization of the radio signals in the air. How is this achieved?

Synchronization cannot take place via the cabling structure, because Ethernet does not allow transport of synchronous data, or in other words, the timing of data sent via Ethernet is not accurate enough. Therefore synchronization must go via the air.

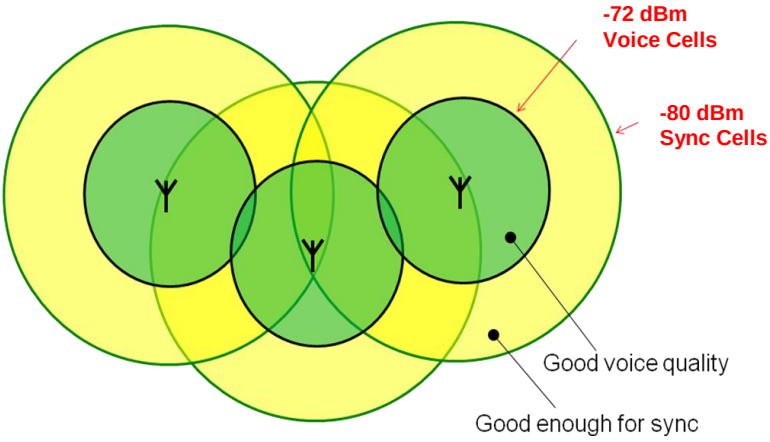


Figure 2-6 "Radio Synchronization"

A DAP (Radio) cell can be seen theoretically as a circle around the DAP. In **Erreur ! Source du renvoi introuvable.** you see two circles around the DAP: one in which you have sufficient radio signal strength for a good voice quality, and another (wider) circle with sufficient signal strength for synchronization. Due to the cellular structure of a DECT Radio Network, there must always be overlap in the cells with sufficient voice quality. The wider cell limit around the DAP will therefore have quite some overlap with the other cell, and will reach to the radio of the other cell. This means that the DAPs of the overlapping cells receive (weak) radio signals of each other. However these radio signals are still strong enough for synchronization purposes.

The receiving DAP checks the radio signals on PARI, to make sure that it belongs to the same DECT system. If they belong to the same DECT system, the DAPs will synchronize with each other according to predefined rules.

The DAPs are always transmitting via a minimum of two bearers. If there are no voice calls via a DAP, the DAP will transmit two dummy bearers. If there is one or more voice calls via the DAP, there will be one dummy bearer plus the voice call(s).

2.6.2 Synchronization Hierarchy

When DAPs try to synchronize to each other, there must be a hierarchy structure. One or more DAPs must be assigned as synchronization source. The system arranges this itself, and under normal conditions you don't need to do anything. However, if you have a complex DAP cell structure, manual intervention might be needed.

When a DAP is started up, it will try to synchronize to a DAP in the environment. Each DAP has its own unique identifier, the RPN (Radio Part Number). The RPN is a hexadecimal two digit number. A DAP will always try to synchronize to a DAP that has a **lower** RPN.

The Master DAP has always the lowest RPN.

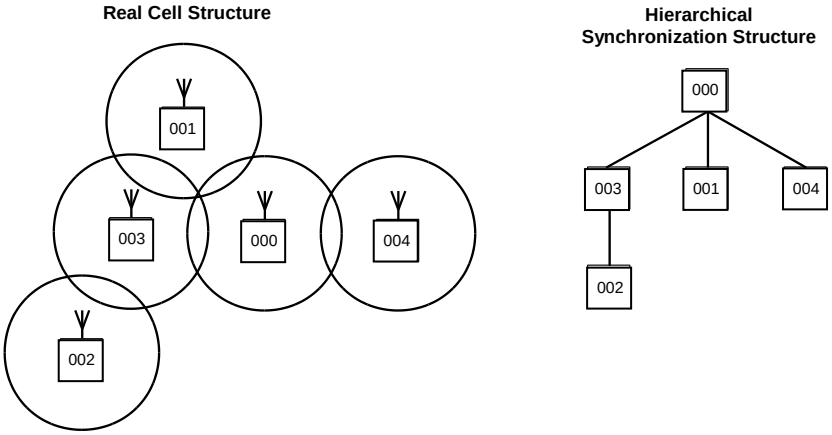


Figure 2-7 "Synchronization Structure"

In Figure 2-7 "Synchronization Structure" you see an example of a simple DAP structure. When the system starts up, the DAPs try to synchronize to the DAP with the lowest RPN. For DAP 000 it means that it will become the synchronization source and the Master DAP! The DAPs with RPNs 001, 003 and 004 will synchronize to RPN 000.

However, RPN 002 will synchronize to RPN 003 although RPN 003 is a higher number. Finding a synchronization source is not limited to one level deep only. DAP 002 knows that DAP 003 is synchronized to a DAP (000) that has a lower number than itself. Therefore DAP 002 will synchronize to DAP 003, because it is aware that DAP 003 gets its source from a DAP with a lower number.

If a DAP "sees" more than one other DAPs, the DAP will synchronize to the DAP that has the shortest path to the synchronization master. If the path to the master is the same number of hops for more DAPs, the DAP will synchronize to the DAP with the lowest RPN.

It is possible that there are more than one "synchronization islands" in the system. In that case, each synchronization island has its own synchronization master. The synchronization algorithm is applicable for each individual island.

Note that the RPN number that the DAPs have, are assigned once, when they start up after installation. The DAP that reports itself at first will get the lowest number, which means that it will become the source for providing the synchronization to the DAP network structure.

If you want to make a DAP a synchronization master, or give a DAP a higher position in the synchronization structure, you can assign a lower RPN number to a DAP manually. RPNs can be assigned manually via the DAP Configurator in the OMC.

The automatically assigned RPNs start at:

- **000**
  The automatic assignment of RPNs starts at 000.
  Manually assigned numbers can be in the range 000 . . . 00F.

After the numbers are assigned at the first time start up, these numbers are stored in a configuration file in OXO and will not change anymore, even after system start-up.

2.6.3 Coverage and Signal Strength Calculation

Synchronization between DAPs requires sufficient radio signal strength between DAPs. The following items are relevant for the signal strength for synchronization.

- To achieve a good voice quality, the minimum signal strength at the receiver in the handset and DAP, must be -72 dBm. (This includes a margin of -10 dBm for fast fading -dips.)
- Synchronization is possible if the strength of the received signal from another DAP is -80 dBm ... -85 dBm (this is adjustable).
- In open area, the distance is doubled if the received signal strength is 6 dB lower. This means that at a minimum signal strength for good voice quality of -72 dBm and a distance “X”, the signal strength at the double distance (2X) is -78 dBm. See Figure 2-8 "Signal Strength Considerations".

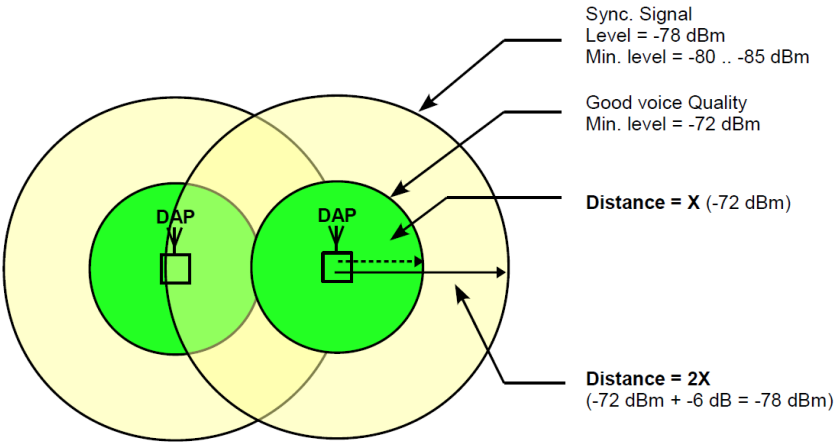


Figure 2-8 "Signal Strength Considerations"

- In open area there is more than sufficient signal strength for synchronization. The expected level at the double distance is -78 dBm. The required level is -80 dBm ... -85 dBm. This leaves a safely margin of 2 ... 7 dB.
- In practice there can be and will be objects in between the DAPs which may introduce some loss. However, there are also (many) objects that causes reflections, which means that the signal will reach the DAP via other paths as well with sufficient signal strength. Real life installations have proven this theory.
- The error rate in the received frames can be much higher than for speech. (50% frame loss is still acceptable).

Practice has indicated that coverage measurements for traditional DECT can also be applied for IP-DECT Lite .

2.7 IP Port Number Assignments

IP Port Numbers are assigned for a speech connection. They are assigned per session, and then released again.

There is a predefined "pool" of IP port numbers. This is specified in file `dapcfg.txt`.

2.8 DAP Characteristics

2.8.1 General

The following DAP types exist:

- 4080 IP-DECT AP Integrated Antennas
- 4080 IP-DECT AP External Antennas
- 8340 Smart IP-DECT AP Integrated Antennas
- 8340 Smart IP-DECT AP External Antennas

All of these DAPs share common characteristics. These characteristics are described in section 2.8.2“Common Characteristics”.

Type dependant characteristics are given in the following subsections.

2.8.2 Common Characteristics

- **Features**

  Note: *The following list contains features that are only supported if the PBX supports it at well.*

  - DECT GAP and CAP compatible.
  - DECT Seamless handover.
  - CLIP and Name Display.
  - Enquiry
  - Call Progress tones.
  - DTMF tones.
  - Message Waiting indication.
  - DAP Software downloadable.

- **Capacity**
  - Max. number of simultaneous calls: 12
    Please note that this maximum number of calls is only applicable when the DAP is synchronization source/master. If the DAP is not the synchronization master, the maximum number of simultaneous calls is 11. Also note that the maximum number of simultaneous calls per DAP is also limited by licenses in a licensed version of IP DECT.
  - Max. number of simultaneous relay calls: 12
  - Max. number of DAPs per network: 16
  - Max. number of simultaneous calls per network with 16 DAPs: 11 x 15 +12 =177. This depends on the network configuration and available DAP channels.

- **IP Interface Characteristics**
  - 10 Base-T and 100 Base-T,
    full duplex (supports auto-negotiation in Ethernet Switch)

Maximum cable length according to the IEE802.3 specification (100 meters).
- Audio Coding: G711 & G729A/G729AB
- DTMF generation: H.245
- Call control protocol: Proprietary.
- IP protocols: DHCP and TFTP

- **Environmental Conditions**
  - Storage temperature range: -25º to +55º Celsius
  - Operational temperature: 0º to +40º Celsius

Note: *The operational temperature range is 0° to 40° Celsius. When you use a DAP outdoor, there is an outdoor box available that will enlarge the temperature range. Please contact your supplier for more information.*

2.8.3 IP-DECT AP Integrated Antennas

Please consult the IP-DECT AP Installation Manual for more information:

2.8.4 IP-DECT AP External Antennas

The 4080 IP-DECT AP External Antennas is the same as the 4080 IP-DECT AP Integrated Antennas but allows you to connect external antenna's.

The 8340 Smart IP-DECT AP External Antennas is the same as the 8340 Smart IP-DECT AP Integrated Antennas but allows you to connect external antenna's.

2.9 4080 IP-DECT AP Power Provision

The IP-DECT APs are powered via PoE. It supports Class detection. The IP-DECT AP is a Class 2 device when used on PoE Switches. For more information consult the IP-DECT AP Installation Manual.

2.10 Licenses

IP-DECT Lite system with IP-DECT AP is license free, full functionality is available without licenses.

3 NETWORK CONFIGURATION

3.1 Typical Configuration

The IP DECT system must be implemented in a company infrastructure For the IP DECT Lite solution used with OXO, only one configuration is supported.

Note: *All IP switches that are involved must support IP multicast, with "IGMP snooping" disabled.*
Furthermore, disable "Spanning Tree Protocol" on ports that are used for DAPs and set the switch ports to "fast forwarding".

3.2 Simple Configuration

Figure 3-1 "Example of Simple IP DECT network configuration" shows an example of a simple configuration. All IP DECT devices are put in one subnet. This subnet is based on one or more IP switches. If the switches serve more than one VLAN, all IP DECT devices are put in one VLAN (therefore behaving as one subnet).

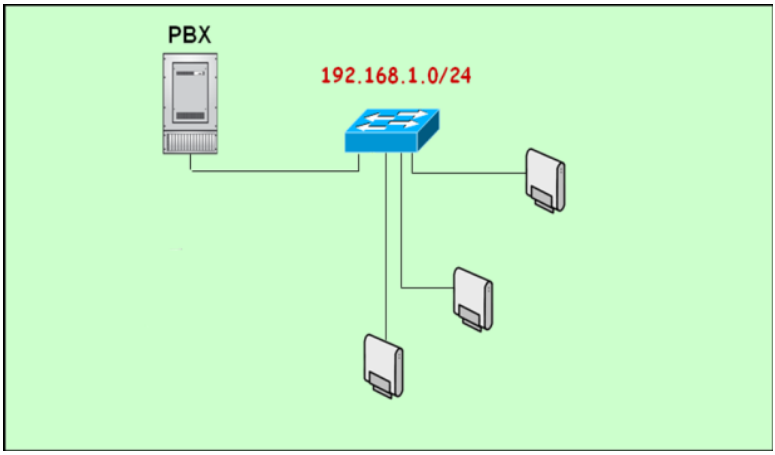


Figure 3-1 "Example of Simple IP DECT network configuration"

In a simple configuration, seamless handover is supported between all DAPs.

4 DAP INSTALLATION ITEMs

4.1 General

The DAPs should be installed on the positions which were determined in the Site Survey (also called Deployment). Besides that, the following should be respected:

- DAPs must be installed with the antennas in vertical position, because that is how the Site Survey is done (normally). (Radiation pattern differs between horizontal and vertical position.)
- Do not mount a DAP to a metal surface.
- Do not roll up remaining cabling behind a DAP.

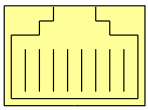
4.2 DAP Power Provision

The DAPs support Power over Ethernet, the so called PoE (laid down in IEEE802.3af specification). The DAPs support both types of PoE: phantom power as well as power over spare wires.

The following overview gives the specifications of the PoE.

- Voltage at the DAP: minimum 36 Volts, maximum 57 Volts.
- Connector: Standard RJ45 connector, using the spare wires pins (wires). See Figure 4-1 "Pin Layout Ethernet Connector RJ45 on the DAP".

- **Maximum cable length: 100 meters.**



DAP “RJ45” Socket

Legend:
1 = 100 Base-T TX+
2 = 100 Base-T TX-
3 = 100 Base-T RX+
4 = + 48 Volt power
5 = + 48 Volt power
6 = 100 Base-T RX-
7 = RTN (0 Volt) power
8 = RTN (0 Volt) power

Figure 4-1 "Pin Layout Ethernet Connector RJ45 on the DAP"

5 CONFIGURATION - DAP CONFIGURATOR TOOL

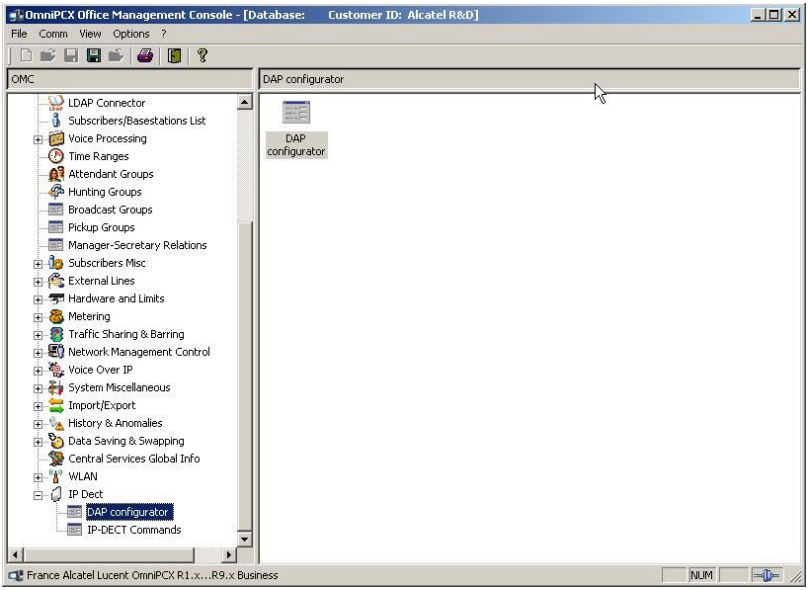
5.1 General

The DAP Configurator is a tool for creating the configuration files for the DAPs. It is embedded in the OMC and is started by double-click in the IP DECT menu.

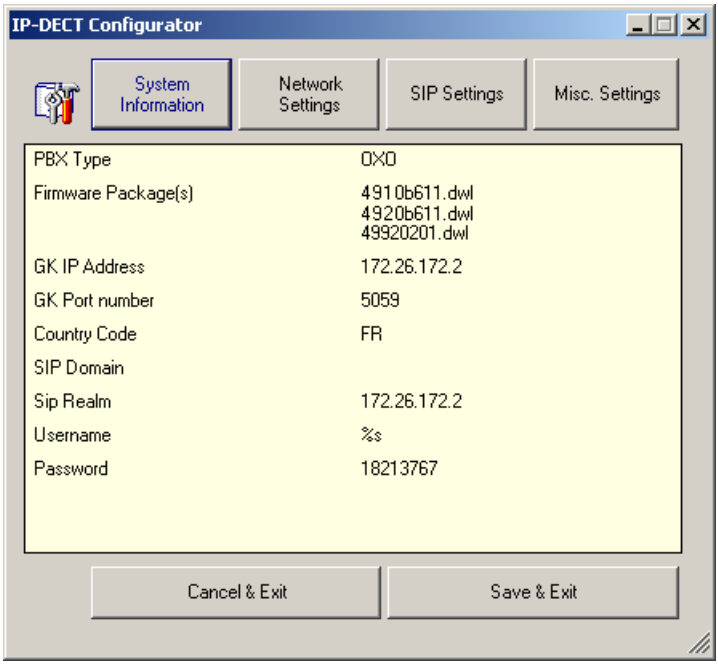
After having entered the required data, a configuration file is created.

5.2 Starting the DAP Configurator

Start the DAP Configurator tool, via OMC, IP Dect menu, DAP Configurator.



This will open the DAP Configurator tool



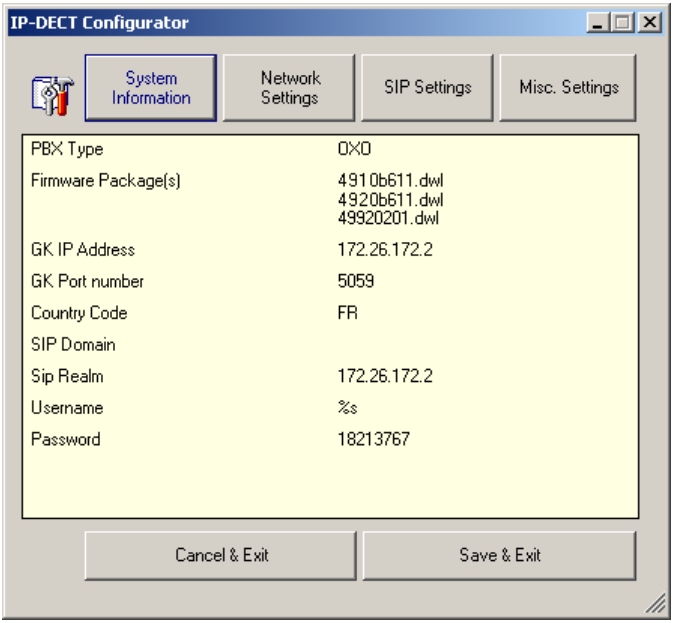
5.3 DAP CONFIGURATOR SETTINGS

5.3.1 Settings Buttons

In the top part of the IP DECT Configurator window, you see a number of buttons that allows you to change settings in the system. In the following subsections these settings are explained.

5.3.2 System Information

When you click the “System Information” the following window is displayed:



The following information are displayed:

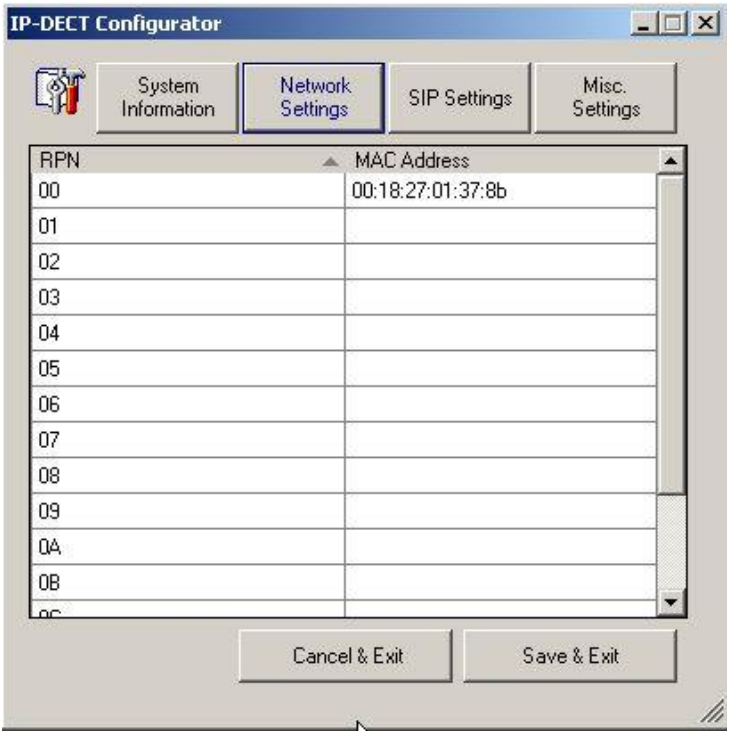
- **PBX Type**
  The PBX Type is always OXO (OmniPCX Office).
- **Firmware Package(s)**
  The firmware package for the 4080 IP-DECT AP available in the PBX is displayed., The file name should look like this: `4910bxyz.dwl` (e.g. `4910b531.dwl`).
  The firmware package for the 8340 Smart IP-DECT AP available in the PBX is displayed., The file name should look like this: `4920bxyz.dwl` (e.g. `4920b531.dwl`).
  The bootloader package for the 8340 Smart IP-DECT AP available in the PBX is displayed., The file name should look like this 49920201.dwl

- **GK IP Address**
  Gatekeeper IP address: this is the PBX IP address
- **GK Port number**
  Gatekeeper port number for SIP protocol
- **Country Code**
  OXO installation target ISO country code.
  The Country code specifies the tone plan for IP DECT and also selects the correct frequency range and transmitter output power.

- **SIP Domain**
  OXO SIP domain name if defined in the OXO configuration
- **SIP Realm**
  OXO SIP Realm (set by default to the OXO IP address)
- **Username**
  User name used to login on the Registrar server (OXO).
  %s means that the user name used to login is the handset's extension number.
- **Password**
  Password for authentication in the Registrar. All the handsets use the same password.

5.3.3 Network Settings

When you click the “Network Settings” button, the following window is displayed:



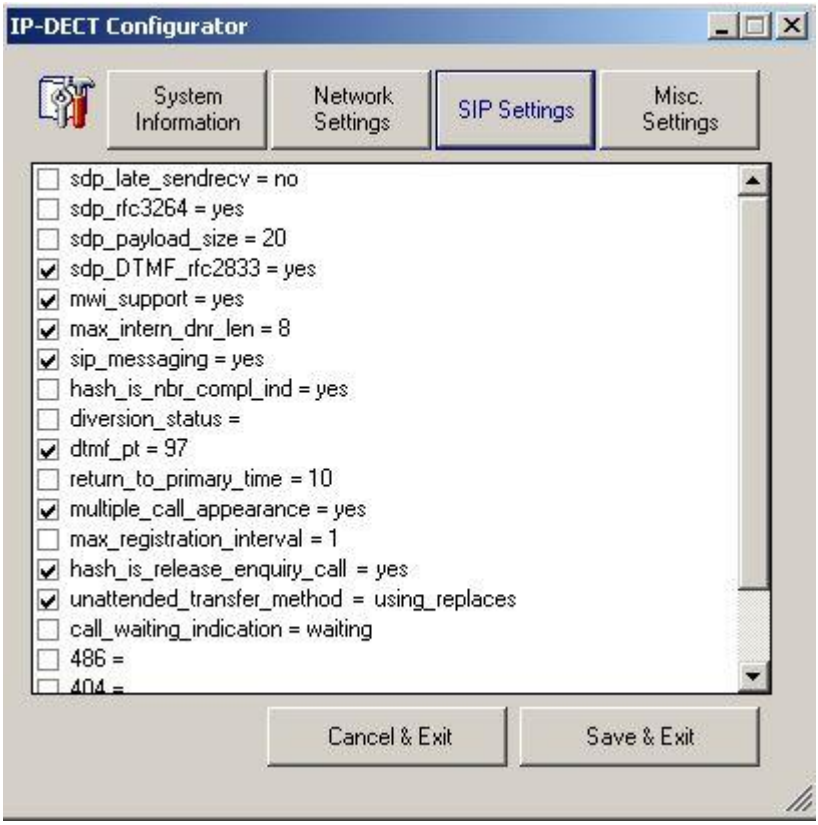
This array gives the association between the RPN and MAC address of the DAPs.

The DAP with the lowest RPN is master DAP.

The MAC address column is editable, so the association between the RPN and the MAC address can be modified.

5.3.4 SIP Settings

The following fields can be edited:



The following items can be entered or changed.

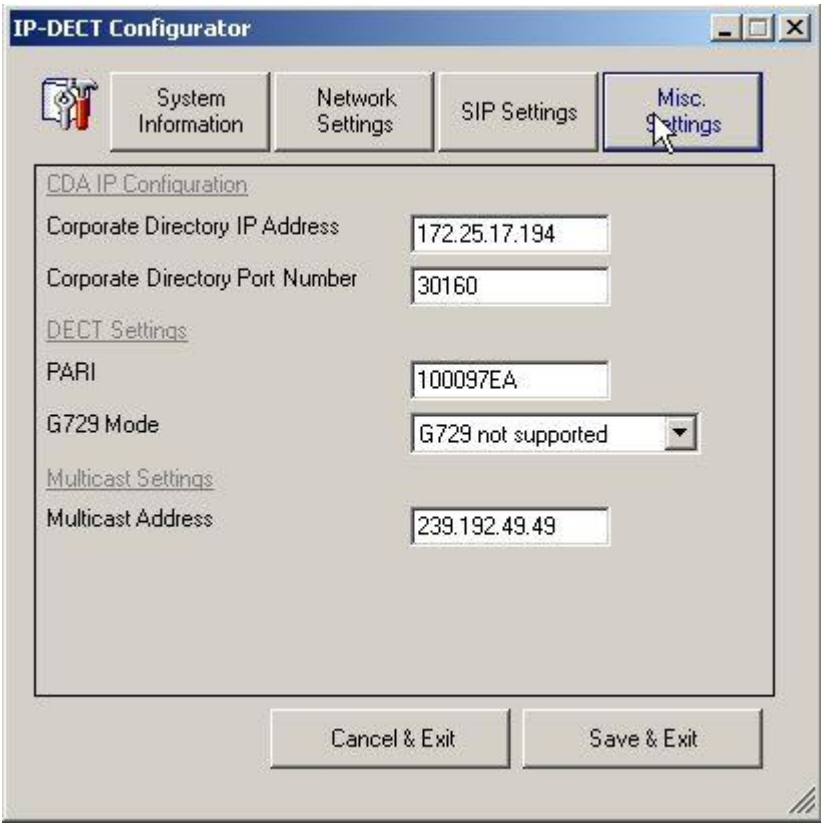
- **sdp-late-sendrecv**
  Enables the ability of the IP DECT system to issue an initial Invite without SDP (Session Description Protocol) offer.
- **sdp_rfc3264**
  Enables “Hold” according to RFC3264.
- **sdp_payload_size**
  Offered payload size in the SDP (Session Description protocol) offer (in ms). However, generally the proposed payload size of the opposite party is used.

- **sdp_DTMF-rfc2833**
  When enabled, DTMF digits are sent according to rfc2833 (in RTP). Otherwise the DTMF digits are sent as SIP “INFO” messages.
- **mwi support**
  Message waiting indication supported, yes or no.
- **max_intern_dnr_len**
  Extension numbers longer than specified here are considered as external numbers. Note that this only applies to numeric extension numbers.
- **sip_messaging**
  This option allows you to enable SIP Instant Messaging according to RFC3428.
- **hash_is_nbr_compl_ind**
  The hash button can be used to indicate number complete or can be used as part of the dialed number.
- **diversion_status**
  In this parameter, you must enter the prefix that is used to activate follow-me. The prefix should have been defined in the PBX as well and will be *21 in many countries. When you have entered the prefix, IP DECT knows when a follow-me is set on an extension and will therefore generate the diversion dial tone when going off-hook: NOT APPLICABLE for OXO.
- **dtmf_pt**
  This parameter allows you to specify the dtmf payload type for RFC2833 inplementation. Default is 96. The range is 96 ...127.
- **return_to_primary _time**
  This parameter is used for a configuration with Proxy redundancy for SIP: NOT APPLICABLE for OXO.
- **multiple_call_appearance**
  When the handset is busy and a second call comes in, you will hear a ticker tone and the display shows “waiting <cli>”. By means of the * button, you can toggle between the two calls. It behaves in a similar way as having a call on hold. Please note that the SIP Proxy must be able to support multiple call to one extension number as well.
- **Max_registration_interval**
  Maximum time between two registrations in minutes.
- **hash_is_release_enquiry_call**
  When you are in an equiry call and you end up on a device like a voice mail server, you cannot hangup the phone without losing your call. I that case you can press the # key to end you enquiry call but keep your original call.
- **Unattended_transfer_method**
  There are three options: Proxy, Cancel, Replace. The following options should be chosen for the related PBX types. For OXO, this value has to be set to Replace.
  Proxy: use for Alcatel-Lucent type of PBXs

Cancel: most commonly used for a wide range of PBX types.
Replace: used for Alcatel-Lucent PBX types.

- **Call_waiting_indication.**
  Here you can specify the call waiting indication text which is displayed when there is a call waiting.
- **486=**
  Here you can enter the text that is displayed when the SIP Proxy sends error code 486
- **404=**
  Here you can specify the text that is displayed when the Proxy sends error code 404.
- **480=**
  Here you can specify the text that is displayed when the Proxy sends error code 480.
- **t_ACK-timeout**
  After having sent the SIP 200 OK message, maximum time to wait for the ACK response before dropping the call.

5.3.5 Misc. Settings



The following fields can be edited:

- **Corporate Directory IP Address**
  The IP address of the Central Directory Server (OXO).
- **Corporate Directory Port Number**
  Port number on the Central Directory server. Default port number is 30160.
- **PARI**
  Primary Access Rights Identifier. This is the Unique DECT System Identifier. It is an 8 digit hexadecimal string. It is a worldwide Unique Identifier which you should have received together with your DECT system.

- **G729 mode**
  The following items can be selected:
  - **G.729 not supported** = never use G.729
  - **Use G729 when required** = Setting as in previous versions of IP DECT.
  - **Preferred use of G.729** = IP DECT will always issue G.729 as preferred codec over G.711.
  - **Only use G.729** = Only G.729, never another Codec

- **Multicast Address**
  Specify a Multicast IP address. If the network for your IP DECT system is used for other purposes than IP DECT as well or if the network has a connection to the company network or external network(s), you must ask the local IT manager for a multicast address. If your IP DECT system is in a closed network, you can click the button “Default IP” to use the default IP multicast address.

5.4 Save Settings and restart DAPs

When you have finished with setting up the configuration, you must do the following:

- Click the **Save & Exit** button to save the changes you have made.
  This will restart all the DAPs connected to the OXO.
- Check that the DAPs become operational.

If you don’t want to apply your modification, just click the **Cancel & Exit** button.

A SIP CONFIGURATION CHARACTERISTICS

A.1 General

Setting up the SIP configuration requires basic SIP knowledge. Make sure that you have basic SIP knowledge before continuing this Chapter and the Chapters that follow.

In the following Sections, the IP-DECT Lite SIP characteristics are described. This can be useful before you continue with the installation. However, if you are familiar with the SIP characteristics of the IP-DECT Lite system, continue with the installation of the IP-DECT Lite system.

A.2 Main Characteristics

The following overview shows the main SIP characteristics of the IP-DECT Lite system:

- **Connectivity**
  The IP-DECT Lite system is connected to OXO ..

- **SIP Extension Registration**
  - OXO acts as SIP Registrar server.
  - Digest authentication security.
  - Password can be reset via OMC.

- **Transmission**
  - High quality voice over IP, G.711& G.729,. However, you can select whether you want to use G.729 only, or never use G.729.
  - Congestion control and packet filtering.
  - Reliable UDP transport using retransmissions.

A.3 Call Handling

In the following table the SIP call handling features are given.

Feature	**Reference**
Basic Call	RFC3261 (except for TCP, IP, Multicastr. MIME and authentication)
Negotiation of most efficient CODEC based upon network information. – Supported CODECs: – G.711 a-Law – G.711 u-Law – G.729	RFC 2327 RFC 3264

Feature	Reference
Payload negotiation. Supported payload values: 20 ,30, 40, 50, 60 msec.	RFC 2327 RFC 3264
En-block (pre-dial) and overlap dialling	RFC 3578
Remote name, or if not available, phone number is displayed on the handset.	
Discrimination between internal and external calls based upon extension number length (configurable)	
Established session modification (re-INVITE)	
Call hold using re-INVITE	
Shuttle between two parties.	
Call transfer: – Attended call transfer using REFER, Refer-To and Replaces – Unattended call transfer using REFER and Refer-To	RFC 3515 RFC 3891
DTMF digit sending: – Via SIP INFO messages – In RTP stream	- RFC 2976 RFC 2833
SIP Music-On-Hold	
When connected to a FXO gateway, it switches to transparent mode to save trunk lines	
Instant Messaging to and from SIP-DECT portables	RFC 3428 (protocol supported, no application implemented)
MWI (Message Waiting Indication)	RFC 3842

Table A-1 "Supported SIP Features"

B OVERVIEW OF DEFAULT USED IP PORTS

The following table gives an overview of the **default** ports used in a IP-DECT Lite configuration.

Protocol	Interface/Device	Default Destination port	Configurable
DHCP	DHCP Server	67	no
	DAP	68	no
SIP	DAP	5059	yes (in PABX configuration tool)
RTP Media	DAP	3000-22229	no
HTTP	DAP	80	no
IP DECT proprietary signalling (IP unicast and IP multicast)	DAP	3000-22229	no
CDA/UDA (NEC proprietary protocol)	DAP	30160	yes (in DAP configurator)
TFTP	TFTP Server	69 (only for initial communication) then:1024-65535	no

Table B-1 "Default ports used in IP-DECT Lite"