IP-DECT Lite
for OXO / SMB market

Advanced Data Manual

8AL90853USAAed01 - R105 – 12/2012

Contents

Preface

This manual is valid for IP-DECT Lite system. It must be used in addition to the Customer Engineer manual for your IP DECT Lite system. It provides detailed information on various IP DECT subjects.

IMPORTANT:

This manual gives information for setting up an IP-DECT Lite system. However, the IP-DECT Lite system 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 system 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.

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.

1 WHY THIS MANUAL

This manual gives you more detailed information about your IP DECT system. It is not an installation manual. For the Installation of an IP DECT system, consult the Customer Engineer Manual for your type of IP DECT system.

Note: *This manual contains information for experienced users only.*

The manual contains the following main items:

- Networking information.
- Upgrade instructions
- Detailed performance manager items.
- Configuration files and System parameters.

2 IP DECT NETWORK ASPECTS

2.1 General

In the IP network aspects two main items are distinguished:

- **IP connectivity**
  IP connectivity means that transport of messages between all stations should be possible
- **Quality of Service**
  The network should deliver sufficient performance (QoS - Quality of service), which means that the network should provide sufficient throughput and throughput speed. The DAPs support Quality of Service and Prioritization.

Both items can depend highly to the used network topology. The network topology/configuration can vary widely, which means that there are no practical step-by-step procedures in this chapter, but only a general idea of network related issues. In 5 “PLANNING AN IP NETWORK” the practical consequences (for the IP-DECT Lite system) are explained.

The following sections give information about the two items (IP connectivity and Quality of Service) in relation to network parts like Hubs and routers.

2.2 IP Network Configuration

Network configuration is very important for IP connectivity and especially in relation to QoS aspects. Physical layout and available (long distance) connections (with limited bandwidth) do require good planning. In most situations, the IP-DECT Lite system will be implemented in existing networks. Before implementing the IP-DECT Lite system, it should be checked if the configuration is capable for this job or if adjustments are required

This requires a detailed insight in the configuration of the total network, especially on the following items:

- Organization of sub-networks
- IP DECT and HUBs
- LAN Switches
- LAN Switches hierarchy
- VPN (Virtual Private Networks)
- IP Network load.

These items are explained in the following sub-sections.

2.2.1 Sub-Network

The network is limited to a single IP address range, a sub-net. All IP network stations can reach each other directly. IP networks are defined by the lowest IP address and a network mask specifying how many bits of the network address are fixed. (e.g. 192.168.45.0/30 for a network with 30 fixed address bits: the highest address is normally used for broadcast. The lowest address is often reserved as loop back address).

2.2.2 HUBs

Although HUBs can be used for IP DECT, using HUBs is strongly dissuaded. HUB is only half-duplex, only supports the same line speed for all ports, and concurrent access will give collisions. The only benefit is that line faults are isolated. Therefore HUBs will introduce delay and should not be used.

2.2.3 LAN Switches

In twisted-pair LAN networks, Switches are used to interconnect the LAN stations in a "star" configuration. The logical configuration for these LAN Switches varies widely from a simple repeater, to "layer 4" aware switches.

Switching Hubs normally operate in a store and forward mode based upon address learning. Incoming messages are received completely, inspected for the (layer 2 MAC address) destination, and forwarded only to the related output port(s). Destinations are learned by inspecting the source address field in incoming traffic. For transparency, traffic to unknown destinations is (like broadcast traffic) forwarded to all outputs. While traffic is forwarded only to a single destination port, other ports might be used at the same time. Switches might be able to forward between port pairs even at different line speed.

Switches normally support various port settings. Also switches may support “Auto negotiation” at port start-up. The “Auto-negotiation” implementation may differ between the various Switch types.

The DAP supports auto-negotiation but not on all Switch types.

Note: *The DAPs support Auto-negotiation on a number of Switches. It is recommended to use fixed settings: 100Mb/s and full duplex.*

Switches might also support a cut-through forwarding mode, to reduce the forwarding delay. In this case, the transmission of the forwarded packet on the output port starts, as soon as the Ethernet header part is received on the input instead of waiting until the whole packet is received.

Switches might be interconnected to support larger networks. If so, Switches normally use the "Spanning Tree Algorithm" to detect (and block) loops in the network connection.

Note: *Spanning Tree Protocol must be disabled on ports that are used for the DAPs. When Spanning Tree protocol is enabled, the port may be (will be) inaccessible when the Spanning Tree protocol is trying to re-arrange the structure.*

Note: *Switches that are used for IP DECT, must support forwarding of IP Multicast packages!*

Note: *In the IP-DECT Lite system, multicast is only used for control messages and NOT for voice. This means that the IP-DECT Lite network load due to multicast, is very low.*

Note: *It is strongly recommended to set the Switch ports in "Fast Forward" mode.*

An IGMP aware Switch might use "IGMP Snooping" to discover where multicast capable hosts are, and which IP multicast address they use. Based on the information collected, using "IGMP Snooping", IP multicast packages are forwarded to ports where they are needed and blocked on ports where they are not needed. When "IGMP Snooping" misses an IGMP package, you run a risk that multicast package are not forwarded correctly to the DAPs. Therefore, read the following note: for IP-DECT Lite system, *IGMP snooping must be switched off* in the Switch.

Note; *For IP DECT, IGMP Snooping must be disabled in the Switch! If not, the system behaviour may be unpredictable.*

More and more, switches provide VLAN functionality. For (layer 2) VLAN, a switch port can be assigned to VLAN group. A LAN host can be connected to a port assigned to a VLAN group can only communicate with a LAN station connected to a port, which is assigned to the same VLAN. VLAN groups can be used over different switches. There are also VLAN switch implementations based upon layer 3. Separation is now based upon the LAN stations network addresses. Instead of assigning a port to a VLAN, switches may also support VLAN tagging. VLAN tagging means that an IP packet carries a "tag" indicating to which VLAN it belongs.

(The DAPs support VLAN Tagging.)

For IP-DECT Lite, this function can be used to separate IP-DECT Lite (multicast) traffic from other traffic. Organization of services shared by members of different VLAN groups might be more complex

2.2.4 LAN Switch Hierarchy

The optimal hierarchy for switched networks depends on the network utilization. If there is one central server, used by all networks stations, the traffic will be concentrated on this server. In this situation, the switching function of a Switching HUB does not help much, while all traffic is concentrated to the same server using the same port (and same central switch). In this case, network capacity (line speed) must be chosen higher at the top level.

If there are different servers and different client groups, traffic might be distributed over different links. Different "back-bones" can be created, by connecting the different servers to different switches (or ports). Traffic to/from one server is forwarded over a different main switch to different ports on the client switches. The resulting network load on each interconnection can be much lower, comparing to the situation where all servers are on the same backbone.

The hierarchy of interconnection switches and the location of clients and servers are very important.

2.2.5 VPN Virtual Private Network

VPN provides a secure connection between network endpoints. Strong authentication and encryption techniques are used to provide security. VPN is can be applied for IP DECT, however, make sure that the connection provides sufficient bandwidth. Also be aware that when you connect a DAP over a VPN connection, the VPN connection must support IP Multicast.

2.2.6 IP Network load

An important item is the expected total traffic over the network. Not only the total amount of data, but also the total traffic-characteristics and requirements must be known, related to the characteristics of the network to be used. Some effects itself might be (very) limited, but become more important in combination with other effects

1. Traffic bandwidth
   Total amount of data traffic averaged over time (bits/Bytes per second)
2. Traffic burstiness
   Some sources might concentrate traffic into burst with a high number of packet/byte per second. This might result in long queues in intermediate forwarding equipment with related large delay jitter.
3. Packet size
   Long packets will block the medium for the transmission time of the whole packet. For lower line speeds this might increase the delay for the next packet. Long packets might become fragmented, introducing additional processing. Small packets will, for the same amount of data to transport, result in more overhead and higher packet rates exhausting the packet forwarding rate budget.
4. Auto throttling of traffic
   Some traffic source will reduce the transmit rate if networks become (over)loaded. Examples are TCP and TFTP, which require acknowledges before continuing.
5. Multicast/Broadcast traffic
   Multicast and broadcast traffics are forwarded to the network segment where DAPs are connected.
6. Collision window
   Collision will occur if two LAN stations start transmission at the same time. This will result in a retry after a random "back-off" time. If contiguous collisions occur, the back-off time will be increased exponential. Throughput will significantly decrease if a certain level of network load is reached. Switches will often use full duplex connections in combination with store-and-forward. In this mode the number of collisions is much lower. Forwarding might still be a problem if destination port is (temporarily) overloaded.

7. Scope/Route of traffic
   Traffic source and destination, related to the routing through the network, can result in concentration or distribution of traffic over network links

8. Statistical distribution in time of traffic
   Do all different clients use the network more or less at the same time or is the load more equally spread in time.

9. Requirements for traffic
   Be aware of the requirement for different traffic types. VoIP is traffic sensitive for delay, packet loss, errors etc. File download is less sensitive for delay and can use retransmission to repair packet loss.

2.3 IP-DECT Lite Network Load

For IP-DECT Lite, the traffic load depends strongly on the used Codec standards. The IP-DECT Lite uses two 32 kbps channels (one in each direction) in the DECT (!) domain (Air interface). However, in the IP domain, the IP-DECT Lite uses either G.711 Codec or G.729A Codec. For the G.711 Codec, the payload transfer rate is 64 kbps in two directions, for the G.729A Codec, the payload transfer rate is 8 kbps in two directions.

Note: *The 4080 IP-DECT AP supports G.711 by default. The 4080 IP-DECT AP is already equipped with the daughter board adding G.729AB capabilities!*

In the following, the network load calculation is given:

- **Network load with G.711 Codec, 64 kbps, half duplex**
  If no compression nor voice activity detection is used, a single IP-DECT Lite VoIP call will use about 80 kbps in each direction (at a payload of 40 msec.). The difference between payload and network load is related to the VoIP packet overhead and is not IP-DECT Lite specific.
  Note that when there is handover between DAPs, an IP-DECT Lite call requires twice aduplex voice connection, so 4 x 64 kbps payload, therefore 4 x 80 kbps network load (320 kbps).
  In the following you see a more precise network load calculation for a simplex voice connection with G711 coding (PCM - 64 kbps):
  For 40 mSec VoIP packets the payload is 320 Bytes, the packet overhead (Ethernet header/trailer, IP Header, UDP Header, RTP Header) is 66 Bytes. Resulting bandwidth is 386/0.040 = 9650 Bytes/Sec = 77.2 kbits/sec.

- **Network load with G.729A Codec, 8 kbps, half duplex**
  In the following you see network load calculations for a simplex voice connection with G729A coding:
  For 40 mSec VoIP packets the payload is 40 Bytes, the packet overhead (Ethernet header/trailer, IP Header, UDP Header, RTP Header) is 58 Bytes. Resulting bandwidth is 98/0.040 = 2450 Bytes/Sec = 19.6 kbits/sec.

2.4 IP-DECT Lite Codec Selection

The IP-DECT Lite system supports two Codec types: G.711 and G.729A(B). The selection mechanism is based on a setting in the IP DECT Configurator integrated in OMC.

2.5 Network QoS (Quality of Service)

Network load and network capacity must match to allow a network service with a sufficient QoS level. For small light loaded networks, the "native" network capacity might be sufficient. Larger, more complex networks, which are more heavily loaded, might require additional QoS actions to allow handling of both "normal" data traffic and IP-DECT Lite VoIP traffic concurrently, without interference.

IP-DECT Lite supports QoS (DiffServCodePoint - DSCP) and Prioritization. However, be aware of the fact that there can be sources (any source!) that use the same mechanisms to give itself high priority. Any source can set those flags to any value.) High-end LAN switches might provide QoS features.

3 PLANNING AN IP NETWORK

3.1 General

The IP connectivity must be planned. Normally an IP-DECT Lite system will use existing IP network infrastructure and facilities for the network connection.

For IP connectivity, the network should be set-up in such a way that, ALL IP-DECT Lite components:

- should be equipped with unique IP addresses.
- can reach all the required services.
- can be reached by all their clients/counterparts.

Enough unique IP addresses must be available both for all IP-DECT Lite components. For local traffic, private IP addresses might be used. IP addresses and routing should be consistent to deliver the required transparency.

This must be the case for normal unicast traffic as well as for the required multicast traffic.

3.2 Plan fixed IP network address

One fixed IP address needs to be planned in advance for the PABX / Gate Keeper used with the IP-DECT Lite system.

Note: *It is possible to store the IP address of the DAP into its Flash memory. This means that you need to have the DHCP server only at the first time start-up and after that the DAP has its own IP address. (see Chapter 7 "USING DAPs WITHOUT DHCP/TFTP SERVER").*

3.3 Plan Dynamic IP network addresses

Network stations, which do not act as server (PC workstations as well as DAPs), can use dynamic IP addresses assigned by DHCP. For dynamic IP addresses, there is no need to specify the MAC addresses of all the network stations in the DHCP server.

The DHCP server must be configured to assign IP addresses from a certain range to "unknown" MAC addresses. Drawback is that any unknown LAN station will get a valid IP address, which might be a (small) additional network security issue. To overcome this drawback, you could use the Vendor Class ID in the DHCP server. In that case the DHCP server will only issue IP addresses to the devices that has the Vendor Class ID of the DAPs. However, the DHCP server must be capable of making a distinction in Vendor Class IDs. The Vendor Class ID of the DAPs is: "D(ECT)AP 49".

For the IP-DECT Lite system, all DAPs will use dynamic IP addresses.

The OXO embedded DHCP server should be used, if possible, to serve the dynamic IP addresses to the DAPs.

3.4 Plan Multicast Addresses

Multicast is used in the IP-DECT Lite system for three functions:

1. Communication between IP DECT network components to locate/address a handset. The main reason is that in the DECT environment, you don't know where a handset is. If a handset must be reached, the request must go to all DAPs simultaneously. .

   Example:
   The "page" function during an incoming call. A single multicast message to all DAPs is used to find the DAP for this handset in fast and efficient way.

2. Seamless handover from one DAP to the other.
   If inter-cell handover is necessary, the media path must be re-directed from the existing DAP, to another DAP. A handover is always initiated by the handset. The handset does a request on another DAP (not the DAP where the connection is at the moment). This DAP issues a multicast on the network to find out on which DAP the existing voice connection is. The DAP with the existing voice connection will respond and then the connection can be re-directed from the DAP with the existing voice connection to the new DAP.

3. Communication between the DAPs about their position in the synchronization structure. If there is no multicast between the DAPs, DAPs will not be able to synchronize.

For IP-DECT Lite, a unique multicast address will be shared by all DAPs. UDP port number is used to separate multicast traffic in an early stage. All intermediate equipment, must support forwarding of multicast. IGMP is used by the DAPs to set-up and maintain multicast routing.

The DAP Configurator proposes a default multicast IP address (239.192.49.49). This is a multicast address in the "private multicast IP address range" which can be used in private IP networks. If you are not sure that you are allowed to use this address, contact the local IT manager.

3.5 Reliability

Telephony is an important service, where a high level of availability is expected. A VoIP telephony system, like IP-DECT Lite, is not monolithic, but is realized using a large number of systems and functions. The total chain is as weak as the weakest link. Availability of all system parts (switches, DHCP server, TFTP server etc.) must match the requirements for the expected utilization.

3.6 Improving Network Reliability

System reliability/availability depends on many details. However, the following items should be considered to improve the reliability.

- **UPS** (Uninterruptible Power Supplies)
  You could consider using a UPS (Uninterruptible Power Supplies) for all critical elements: Switches/Hubs, DAPs, PABX (OXO) etc.
- **Redundancy for critical functions**
  Critical functions, like DHCP (if external to OXO) etc. in the network might be duplicated. Also Routing (multiple routes with auto re-configuration) can be considered. Duplication of the DAP Server,as well as the PABX (OXO) is not possible (yet).

.

4 DAP CONFIGURATION FILE

4.1 General

For proper operation of the DAP, it requires a configuration file which is uploaded via TFTP. This file is called: `dapcfg.txt`.

Note; *The DAP Configurator tool creates this file automatically.*

Generally the content of this file is correct after using the IP DECT Configurator tool. However, you can check the content yourself. In the following subsections the content of this file is explained.

4.2 The "dapcfg.txt" file

The `dapcfg.txt` file contains the main configuration data for the DAPs but also for the DAP Controller/Manager. The DAPs read the file via the TFTP server. The file is read at start-up of a DAP. If the TFTP server cannot be reached or is down, the DAP will try to reach the TFTP Server at a one minute interval.

Note that this file must be present in the "root" directory for TFTP in the TFTP server.

The following gives an *example* of the `dapcfg.txt` file:

```
;
; Created by DapConf on 2011-07-28 16:40:42
;
[DAP-IMAGEFILE] ; Start of DAP image file section
4910XXxx.dwl

[DS]   ; Start of DS address section
172.25.17.194   28000-28017 ; Address of DDS and min and max port

[DAP]  ; Start of DAP address section
239.192.49.49  3000-22229 1; DAP Multicast Address min and max
port and time to live (ttl)

[GK] ; start of Gate Keeper address section.
172.25.17.194 5059
```

```
[CDA]
172.25.17.194 30160

[XDS]; Start of XDS section
realm1=172.25.17.194
user1=%s
pwd1=~kz99ljEMwPJp2Oc
web_usr=dapwebadmin
web_pwd=~1*_X#+#?e]!
sdp_DTMF_rfc2833=yes
mwi_support=yes
dtmf_pt=97
multiple_call_appearance=yes
hash_is_release_enquiry_call=yes
unattended_transfer_method=using_replaces
t ACK timeout=32

[CONFIG] ; Start of static config section
CONFIGFILE=replace ; What to do with static config file
IPCONFIG=replace ; What to do with IP configuration
```

The file is an editable ASCII file and contains the following sections:

- **Image File section**
  This section specifies which firmware should be uploaded to the DAP. Note that when you specify a file here, the DAP will get this file from the same directory as where the `dapcfg.txt` file resides, the TFTP root directory.
  The file specification is as follows: `4910<vv><ll>.dwl`
  e.g. `4910bXxx.dwl;` for 4080 IP-DECT AP running on SIP Proxy
  Note that the part behind the "**;**" is comment field and will be ignored by the DAP.
  It is possible to load an "image" file to individually specified DAP. In that case the line should start with the MAC address of this DAP.
  e.g. `08:00:6f:82:00:5c 4910bXxx.dwl; location 1`

- **DS section**
  The DS section contains the IP address and port numbers on the DAP Controller. By means of this, the DAP knows where to contact the DAP Controller/Manager.
  The syntax is as follows:
  `<IP_Address> <min._port_number>-<max._port_number>`
  e.g. `192.168.1.1 28000-28017;DAP controller`
  Note that the part behind the "**;**" is comment field and will be ignored by the DAP.

- **DAP section**
  The DAP section contains the IP Multicast address for the DAPs (it is also used by the DAP Controller/Manager). It also contains the port numbers used for the RTP (Real-time Transport Protocol).
  The syntax is as follows:
  `<IP_Address> <min._port_number>-<max._port_number>`
  e.g. `239.192.49.49 3000-22229 1; DAP Multicast Address, min and max port and time to live`
  Note that the part behind the "**;** " is comment field and will be ignored by the DAP.
  The "1" following the port number range, is the TTL (Time-To-Live) applicable for the Multicast address. The TTL value has a different meaning in IP Multicast, compared to normal IP packages. Do **not** fill in a "0". When you fill in a "1" it means that the IP Multicast packages remain within the local network segment and will not cross a Router. If higher than a "1" the IP Multicast packages will cross a Router (if the Router is multicast capable).

- **GK section**
  The GK section contains the IP address of the Gate Keeper, which is the IP address of the PBX. It also contains the port number on the PBX.
  The syntax is as follows:
  `<IP_Address> <port_number>`
  `e.g. 172.25.17.194 5059; IP Address and port number`
  Note that the part behind the "**;** " is comment field and will be ignored by the DAP.
  Note that the port number differs per type of PABX. e.g., for SIP, it will be 5059 by default.

- **XDS**

  The XDS section contains PBX specific parameters. *This means that the list of parameters will* **be adapted for OXO**..

  Note that the part behind the "**;** " is comment field and will be ignored by the DAP.

- **CONFIG section**
  The Config section contains parameters for storing the IP Address and the configuration file (dapcfg.txt) in the FEPROM of the DAP.

- **QoSGLOBAL**
  In this section, the Quality of Service parameters are specified. The following items are specified:
  – DSCP
    DiffServCodePoint.
  – UP
    Priority setting on Layer 2.
  – VID
    Virtual LAN ID.

Note: *Parameters should comply with the IP network requirements of your LAN environment.*

5 CODEC SELECTION

5.1 Generic

IP DECT supports Codecs G.711 and G.729AB. However, this depends on the DAP type that you use.

The 4080 IP-DECT AP supports G.711 by default and G.729AB by means the G.729AB daughter board

The DAPs that support G.729, support G.729AB, where the "B" stands for "voice (in-)activity detection". IP DECT will negotiate about the Codecs and if the PABX does not support G.729AB but only G.729A, then IP DECT switches to G.729A.

Codec selection depends on a setting in the IP DECT Configurator, under “Misc Settings”:

5.2 G.729 Setting in the IP DECT Configurator

In IP DECT you can select the behaviour of G.729 in the IP DECT Configurator, in the window “Misc Settings”. The following behaviour can be selected:

- **G.729 not supported (default)**
  IP DECT will never use G.729.
- **Use G.729 when required (default)**
  This is offers the Codec selection as explained in Section 5.1 “Generic”.
- **Preferred**
  IP DECT offers G.729 as first Codec. If the other party has G.729 as preferred Codec IP DECT will select G.729.
- **G.729 only**
  IP DECT offers G.729 only.

Note: *If the G.729 codec is the codec selected (but not the only codec) in the IP DECT configurator, it is recommended to choose “**Use G.729 when required”** for G.729 mode rather than “Preferred use of G.729”.*

5.3 “Use G.729 When Required”

This option has no effect in the IP DECT Lite solution, as voice traffic always remains the same subnet and in that case, G.711 is preferred.

6 E. xxx CODE LIST

The Registration status of a handset can be retrieved from the DAPs. This Registration status can be Registered, Absent or a certain E.xxx code. This E.xxx code represents an error condition. The following list shows the possible error codes and their meaning.

Code	Meaning
1	No handset ID data in the PABX
2	Un-authorized or Restricted to register
3	Double assignment (other equipment already registered on the same number)
5	Illegal LEN
7	PH card/function un-available
9	Illegal equipment type
15	PH could not provide all requested channels
16	Exceeded registration license capability
17	Resource un-available
18	Message contains error “Contents parse error”
100	Registration pending
101	Registration pending timed out
253	Socket error
254	Time out on PABX connection. Can be a registration problem for a handset or no connection at all to PABX.
4xx	SIP only! Client Failure responses from the SIP Server. For more info consult the SIP Error explanation of you SIP Server or on the Internet.
5xx	SIP only! Server failure responses from the SIP Server. For more info consult the SIP Error explanation of you SIP Server or on the Internet.
6xx	SIP only! Global Failure Responses. For more info consult the SIP Error explanation on the Internet

Table 12-1 :”E Code list”

Note: *E codes 1...18 are only possible if the PABX supports it. E codes 100...254 are commonly used and supported for almost all PABX types.*