Business Mobility IP DECT CE Manual for SIP Connectivity

Release date : 07/May/2007

PREFACE

This manual is valid for Business Mobility IP DECT Software Release 4

IMPORTANT:

This manual gives information for setting up a Business Mobility IP DECT system. However, the Business Mobility IP DECT 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.

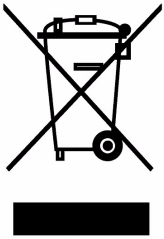
The Business Mobility IP DECT is also a wireless data communication system. This requires knowledge of radio signal propagation. The radio signal propagation in Business Mobility IP DECT requires a different approach than for the traditional DECT systems. The success of the installation also depends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

It is strongly advised to follow the Business Mobility IP DECT CE training at NEC Philips Unified Solutions.

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.

At www.nec-philips.com/weee you can find information about separate disposal and environmentally sound recycling.

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. 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 Business Mobility IP DECT system connected to the SIP Proxy via a 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 Business Mobility IP DECT 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 PABX." shows a general IP DECT Solution. It shows the basic system setup for the Business Mobility IP DECT system.

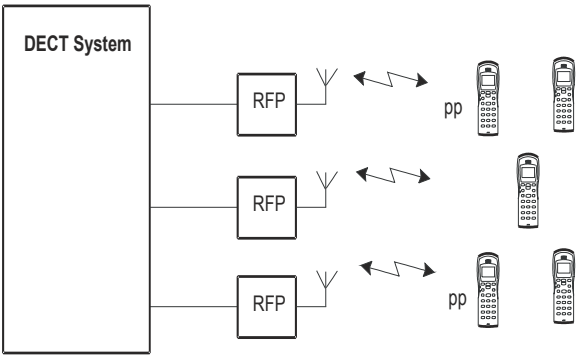


Figure 1-1 DECT System parts (General)

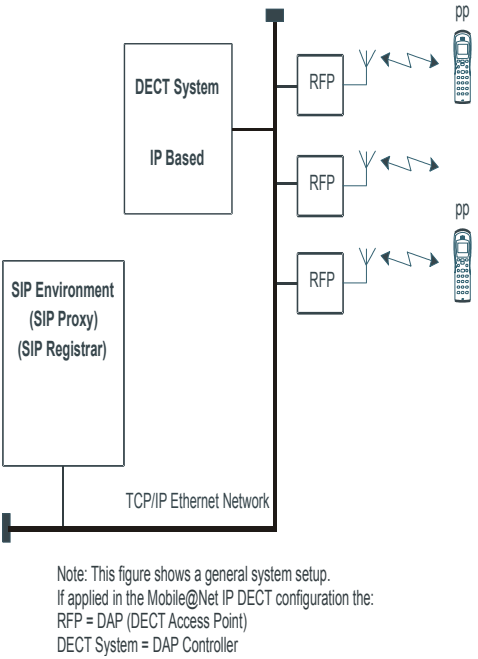


Figure 1-2 DECT System Parts in an IP Solution as Add-on to a PABX.

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 Business Mobility IP DECT supports up to 12 simultaneous calls, depending on the licences.)

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.".

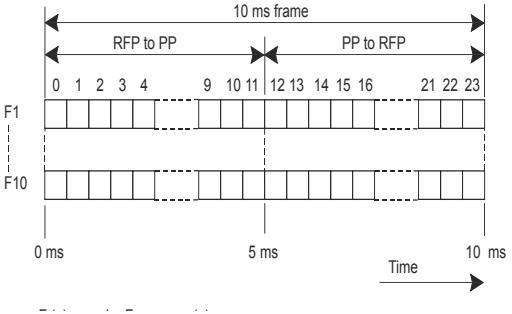


Figure 1-3 Carriers and Timeslots in the DECT Air Interface.

Figure 1-4 "DECT Time Frame and Time slot Structure." shows a time frame and a time slot. 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 1-5 "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.

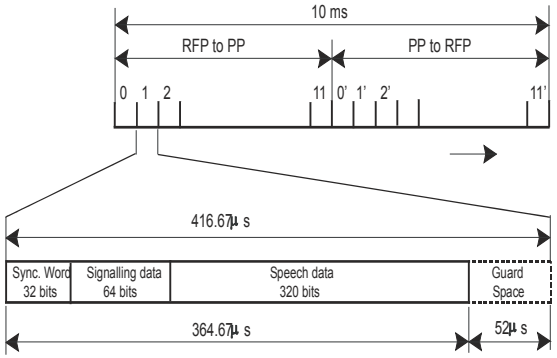


Figure 1-4 DECT Time Frame and Time slot Structure.

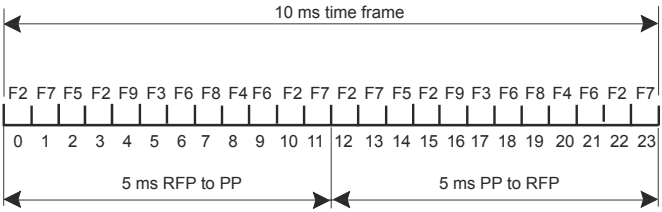


Figure 1-5 Each time slot can use any of the 10 Carrier Frequencies.

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 DECT application in the Business Mobility IP DECT, 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 to 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 Business Mobility IP DECT system to the SIP Proxy. (The voice onnection 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 stand alone 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 digitized 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. The Figure 1-6 "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, 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.

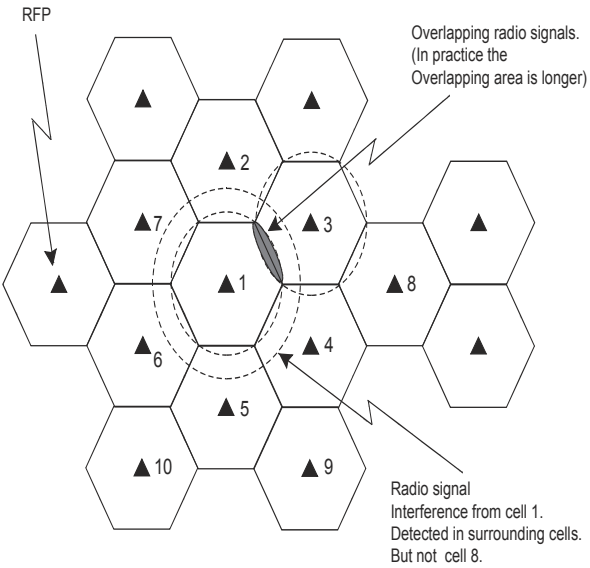


Figure 1-6 Cluster Arrangement

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:

1. 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.**
2. 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.
3. **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:

1. Use the other antenna (antenna diversity). The PP does not notice the change.
2. Tell the PP that a handover is necessary. The PP always initiates the handover after selecting the best channel as seen from the PP.
3. 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), SARI (Secondary Access Rights Identifier)
  The PARI is a worldwide unique identifier for an individual DECT system. When stored in the handset, it is called the PARK. A DECT system can transmit a second "ARI" (Access Rights Identifier), called the SARI. The SARI is explained in 1.9. "Secondary Access Rights Identifier (SARI)". The unique DECT system identifier (PARI, and sometimes also the SARI) 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)

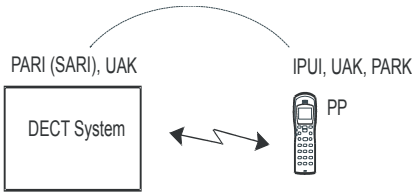


Figure 1-7 UAK Relation between the IPUI and the PARI

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, seeFigure 1-7 "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 info on the SARI, consult 1.9. "Secondary Access Rights Identifier (SARI)".)

For the subscription procedure the WEB interface for Management must be used. This WEB interface provides access to the configuration settings in the DAP Controller/Manager, which is the Server that controls the DECT System. In the WEB interface for DECT Management, one or more extension numbers can be created and then selected to start the subscription procedure the (these) extensions (PP). Also one or more existing extension number(s) can be selected to subscribe a handset to. Then the DAP Controller/Manager generates a code ("PIN code" or also called "Authentication Code") which is visible via the WEB Interface. 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. (Assumed that the handset is known and registered in the PABX as well.)

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 WEB interface for DECT Management can be used to de-subscribe ("terminate" or "disable") the PP. Such a service condition of a PP can always be displayed at the WEB interface for DECT Management.

A portable which has been "terminated", still contains the subscription data, but cannot gain access to the system. (If the PP supports a "reset" and this is executed at the PP, the subscription data in the portable is removed also.) The Administrator (user of the WEB interface for DECT Management) can use the "terminate" command (remove subscription) in case the portable has been lost or damaged.

A portable which has been "disabled" via the WEB interface for DECT Management has been put on the blacklist in the DAP Controller/Manager. When the PP is or becomes within reach of the radio signals, the DAP Controller/Manager 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 cannot reach the PP and complete the de-subscription, the "terminated" command can be used after the "disable" command.

1.9. Secondary Access Rights Identifier (SARI)

The SARI (Secondary Access Right Identifier) has the same function as the PARI, but it is used as a second identifier in case the PARI does not match between the DECT system and the PP.

The PARI is a unique number belonging to one DECT system only. The SARI can be the same identifier, used in more than one DECT system. The DECT system transmits both PARI and SARI as identification signals.

If the PP detects a DECT signal in the air, it checks whether the PARI in that signal matches with its own PARI data in the subscription record. If so, the PP "locks" to that signal. If not, the PP does a second check but now on the received SARI. If that matches, the PP "locks" to that signal.

The Secondary Access Rights (SARI) is used in case you want to use your PP on more than one DECT system (no handover possible between the systems!). The PP uses the same subscription record (comprising the PARK, IPUI and UAK) in the handset for PARI or SARI. For using a SARI, you must subscribe your PP to one system, and copy the subscription record to other systems, all having the same SARI. You don't need to subscribe that PP anymore to the other systems.

Figure 1-8 "Using SARI in three DECT Systems" gives an example of three different DECT systems (three different PARIs) and one SARI. In this example the PP is subscribed to the SARI of system X. This SARI is not unique because the other systems have the same SARI. Therefore the subscription record can be copied from DECT System X to the other DECT Systems. (The DECT Manager allows you to copy the subscription record from one DECT System to another.) When the PP receives radio signals from system Y or system Z, it first checks the PARI of that system and if that doesn't match with its PARK it will do a check for the SARI of that system. The SARI matches with the PARK in the PP, and because the subscription data was copied, the UAK will also match. So. the PP can also be used on systems Y and Z.

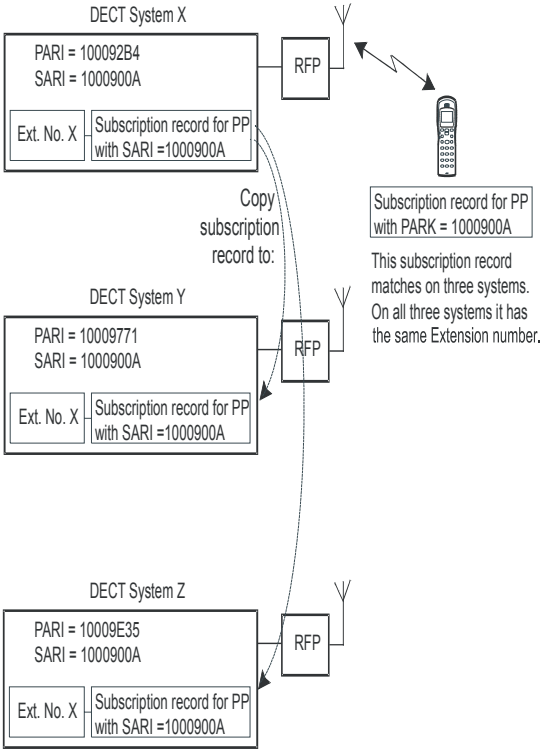


Figure 1-8 Using SARI in three DECT Systems

2. DECT IN IP NETWORK

2.1. System Architecture

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

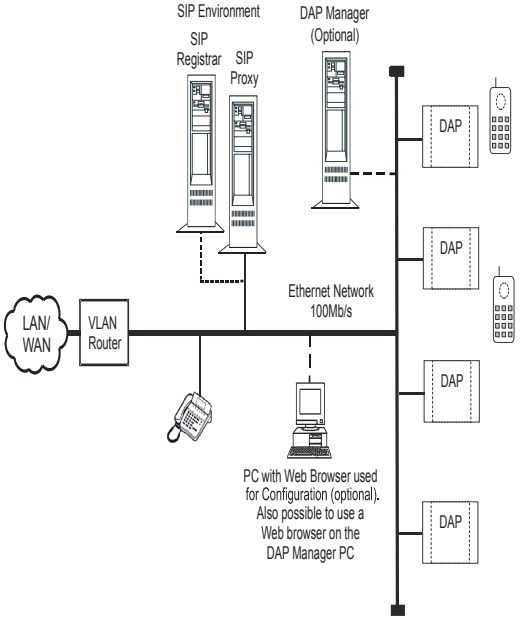


Figure 2-1 Business Mobility IP DECT - System Configuration.

The main parts in the Business Mobility IP DECT system are:

- **DAP**
  The DAP (DECT Access Point) is the actual DECT transmitter/receiver. The current types of DAPs are the AP200 and the AP200S.
  The AP200 supports up to 12 simultaneous calls. However, default, the AP200 supports 2 simultaneous calls, working in single cell mode. The number of simultaneous calls can be increased in steps of two via the License mechanism in the DECT Manager Interface. When you increase the number of simultaneous channels available to 4 or more, the AP200 switches over to a multi-cell behaviour and thus allowing handover between DAPs.

The AP200S is used in the license free version of IP DECT SIP. It supports 12 simultaneous calls and does not require licenses for channels.
The power provision can be done via the Ethernet interface (PoE) or via a local power supply. Note that if the power provision takes place via the Ethernet network, the network cabling and infrastructure must be capable for this.
Besides radio traffic, the DAPs takes care of subscription control and call control data handling to/from the SIP Proxy. For subscription handling, a DAP has the DDS (DECT Data Server) installed and for call control data handling, the DAPs has the SDS (SIP Data Server) installed.

- **DAP Controller/Manager**
  The DAP Controller/Manager has two main functions: WEB Server for Management (CDS) and Subscription distribution (DDS).
  The WEB server provides a WEB interface which allows you to maintain and configure the system from a PC with a WEB browser (Internet Explorer 6.0 or higher). It is based on IIS (Internet Information Server) which is a Microsoft Windows component. The Business Mobility IP DECT Management software is installed in this IIS environment and is called CDS (Control Data Server).
  The Subscription distribution is handled by DDS (DECT Data Server) which runs as a service under MS Windows.
  When the Business Mobility IP DECT system is up-and-running and management actions are not needed, the DAP Manager can be disconnected and is not needed anymore. However, the following system configurations always require an up-and-running DAP Manager:
  - Business Mobility IP DECT configuration with branch offices.
  - Low Rate Messaging Services (LRMS).
- **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.

Note: *The SIP Registrar and SIP Proxy are logical "roles" in the SIP structure that can be played by separate devices but also by one device. For the purpose of clarity, in the figures in this chapter the two roles are depicted on separate devices.*

Note: *In this manual you will only see the SIP Proxy server and the SIP Registrar server and no other SIP servers like a SIP REditrect server or SIP Location server. The reason for this is that the IP DECT sytem (holding the SIP UA's) communicates with the SIP and Proxy and SIP Registrar and not to other SIP server types. The other SIP servers work on a different level in the SIP configuration.*

- **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 Business Mobility IP DECT 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 **WEB Browser**
  Via the WEB Browser, you can access the DAP Manager. Via this WEB interface, you can subscribe handsets and change configuration settings. Note that the WEB browser must be Internet Explorer 6.0 or higher!

Note: *The WEB Browser is shown in the picture as a separate PC. However, the WEB browser on the DAP Controller PC can be used as well! This means that a separate PC with WEB browser is not necessary.*

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).

However, before you can establish a call, the handset must have been subscribed and registered in the SIP Registrar. If the handset is subscribed in the IP DECT system but not in the SIP Registrar, it is no problem because the registration will automatically take place. It is also possible to setup calls without registration in a Registrar server. In that case you must setup the Business Mobility IP DECT system, to communicated with the SIP Proxy only.

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

2.2. Handset Subscription/Registration

Before you can use a handset, the handset must be subscribed to the Business Mobility IP DECT system. Besides that the handset must be registered as UA in the SIP Registrar server. Subscription requires manual intervention, registration is done automatically. Figure 2-2 "Phases in the Subscription Process." shows the phases in the subscription process.

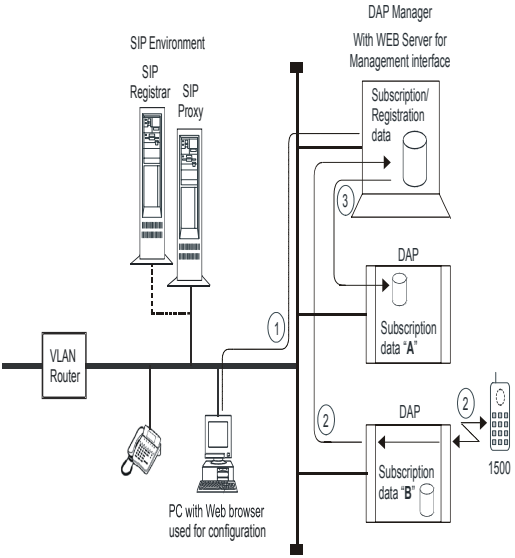


Figure 2-2 Phases in the Subscription Process.

The following phases are distinguished in the subscription process.

1. The administrator starts a subscription process via the DECT Manager WEB page. This WEB page is accessible from a WEB browser in the network.
   The administrator "enables" a subscription, which means that the subscription process is started. The Business Mobility IP DECT System is now waiting for action from a handset.
2. Now the subscription must be executed from the handset. The handset user must enter the PIN code that is displayed on the DECT Manager WEB page. When the PIN code is entered on the handset, the subscription record is created in the DAP Manager Database.
3. The DAP Manager will distribute the subscription data to one of the DAPs (AP200). Distribution has the following characteristics:

- The DAP Manager tries to distribute the subscription records equally over the DAPs.
- The maximum number of subscription records per AP200 is 25.
- Once a subscription record is stored into an AP200, it will normally not be moved to another AP200 anymore. There are two exceptions on this: If you "Delete" an AP200 manually from the DAPs list in the DECT Manager, the subscription records of that AP200 will be distributed over the remaining AP200s. If the handset moves to/from a branch office, the subscription record moves with the handset to/from the branch office. Moving subscription between main site and branch office(s) is activated when the handset does a "location registration" in the main site or branch office. Note that the DAP Manager must be active to make this moving possible.
- If DAPS are connected in a Branch office, the Branch office is regarded as a subscription island. The subscription record for a handset is either in a DAP at the main site or in a DAP at (one of) the branch office(s). When a handset executes a "location registration" at the main site or one of the branch offices, the subscription record is moved to the island where the location registration was done.

After the subscriptions are executed, each AP200 contains a number of subscription records. The DAP Manager contains subscription data of all handsets in the system. If the DAP Manager is disconnected, the system remains operational.

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

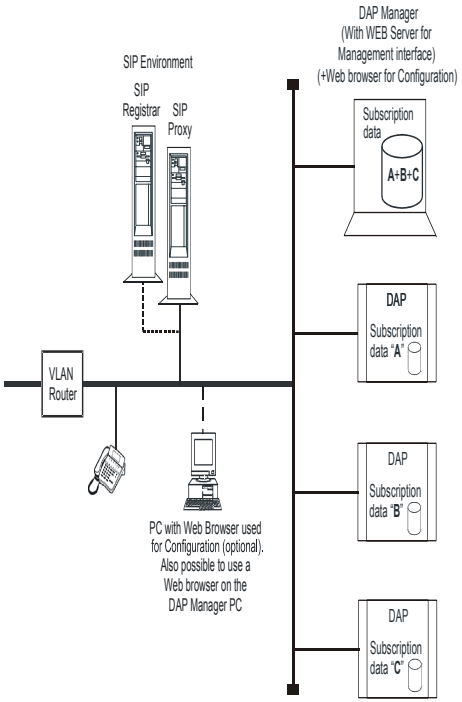


Figure 2-3 Subscription locations.

2.3. Automatic Distribution When DAP Down

When DAP Goes down, the subscription records in that DAP are not accessible anymore., and therefore, the associated handsets cannot be used anymore. However, in Release 4, the subscription records of a broken DAP are automatically distributed over other DAPs after 10 minutes down time.

This automatic distribution requires that the DAP Manager must be up and running. If not, automatic distribution does not take place!

When you connect the DAP Manager after a DAP went down, the timer starts from the moment that the DAP Manager is up and running. This means the you can replace the faulty DAP with a new one, with moving the original subscriptions to the new DAP within those 10

minutes. For replacing a DAP, consult Section 14.2. "Replacing DAP, new DAP Available".

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. You can specify the registration time period in the Business Mobility IP DECT configuration. This time period is issued to the Registrar server. The Registrar server normally accepts this time period, but may also change the time period a bit. The Registrar tells the Business Mobility IP DECT system the stored time period (in the "ACK" message). When the time expires, the registration is removed from the Registrar. However, the Business Mobility IP DECT system knows when the timer expires and will execute a register again for a certain time period.

An IP DECT handset registers itself:

- at subscription
- when the DAP holding the subscription record of an extension (UA) starts up
- when the registration time period expires.

Note, that the Registrar should always authenticate the Register request. This means that you must assign a username and a password to the Business Mobility IP DECT system and the same user name and pasword in the configuration of the Registrar server.

A SIP Location Service or SIP Proxy service makes use of the Registrar database information in order to locate a UA in a network.

Note: Note that it is not always necessary to do a registration to a Registrar service. Depending on the SIP servers configuration and the SIP Proxy type, registration can be done implicitely via a call setup (INVITE) request from the UA to the SIP Proxy. In that case no Registrar server is used and no registration expiry timer is used.

2.5. Call Setup

A call can be setup from a UA (it is the originator, so it is called "User Agent Client" = UAC) somewhere in the network (LAN/WAN) to an IP DECT handset (destination and therefore called: UAS = User Agent Server). Also a call can be setup from an IP DECT handset to any other UAS in the LAN/WAN. The following common rules are applicable:

- The originator is always refered to as UAC.

- The destination is always refered to as UAS
- The Business Mobility IP DECT system does the call control communication with one SIP Proxy only. Therefore, in this section, only the call control messages between the Business Mobility IP DECT system and the SIP Proxy are described, not the call control behind the SIP Proxy.

In the following subsections the setup procedures for these calls are described. This section does not describe a handover. The handover procedure is described in section 2.6. "Handover Mechanism"

- **Initial Call Setup from the SIP Proxy to a DECT handset**
  See Figure 2-4 "Initial Call Setup from the SIP Proxy to a DECT handset." as example. In this example you see a call setup from an IP SIP phone to a handset on the Business Mobility IP DECT system. The IP SIP phone goes dails extension number 1500 and goes off-hook. As result it issues an "INVITE" (call setup request) to the SIP Proxy; in the figure: (1). This "INVITE" contains the UAS information: the extension number and the domain/ realm where the extension is located. The SIP Proxy may respond to this "INVITE" with a request for authentication (407 Proxy Authentication Required). If so, the "INVITE" is send again but now with an Authorization header (user name and password). The SIP Proxy accepts the "INVITE" and sends back an OK message. The SIP Proxy tries to discover where the UAS is located. In this example it is located on DAP 3 because the *subscription* record for extension 1500 resides in DAP 3. Therefore the socket IP address for extension 1500 is the IP address of DAP 3. It forwards the "INVITE" to DAP 3; in the figure (2). DAP 3 (AP200) receives the "INVITE" for extension 1500 (UAS), but it does not know in which radio cell the handset is. It will issue an IP multicast to all DAPs; in the figure (3). As depicted in the figure, extension 1500 is in the environment of DAP 4, which means that DAP 4 will send relevant information back to the DAP 3. DAP 3 forwards the call setup request (INVITE) using a proprietary protocol and handset 1500 will start ringing. DAP 3 sends back a "RINGING" message to the SIP Proxy who forwards this to the originator (UAC). When the handset goes off hook, an "OK" message is sent to the SIP Proxy and negotiation about parameters (codec, payload, etc.) takes place. When negotiation is finished and accepted, the UAC sends an "ACK" message to the DAP 3 (via the SIP Proxy). The speech path is set up between the originating extension and **DAP 4**. See Figure 2-5 "Call established between IP SIP extension and a DECT handset". Note that the Signalling-end-point for this call is DAP 3 but the Voice connection-end-point is DAP 4. (the DAP where the handset is at that moment of call setup).

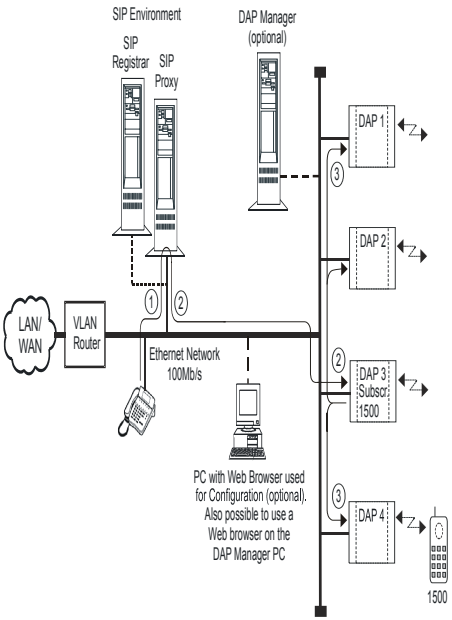


Figure 2-4 Initial Call Setup from the SIP Proxy to a DECT handset.

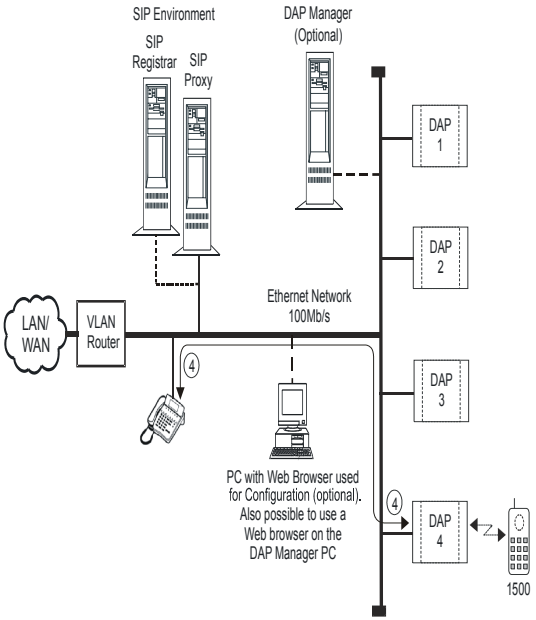


Figure 2-5 Call established between IP SIP extension and a DECT handset

The actual voice (RTP) connection (4) is set up between a socket (IP address + port number) on the IP SIP extension and a socket (IP address + port Number) on the DAP. Both socket numbers are unique and therefore the speech connection is unique. Note that the socket numbers that are used for this connection are applicable for this call only. When the connection is disconnected, the socket numbers are no longer reserved and can be used for a new connection.

Note, that the DAP Manager was not involved in the call setup process!

- **Initial Call Setup from a DECT Handset**

  A call setup from the DECT handset to another extension uses the same type of procedures, as a call setup to a DECT handset, but now the opposite way.

  When the DECT handset goes off-hook, the DAP on which the handset is locked issues a (multicast) request to find out on which DAP the subscription record of the handset resides. When the subscription record is found, a confirmation is set to the DAP on which the handset is locked. The DAP will generate dial tone. Note that this process is an internal process in the Business Mobility IP DECT system. No SIP involved so far.

The handset user dials the destination extension number. Note that the “number complete” is detected based on an “overlap” timer. At entering a digit, the timer is restarted. When no digits are enter within the specified time, the timer expires and the Business Mobility IP DECT system assumes a number complete. Then, the DAP on which the subscription record resides issues an “INVITE” (call setup request) to the SIP Proxy. The SIP Proxy may respond to this “INVITE” with a request for authentication (407 Proxy Authentication Required). If so, the “INVITE” is send again but now with an Authorization header (user name and password). The SIP Proxy accepts the “INVITE” and sends back an OK message. The SIP Proxy tries to discover where the UAS is located and will forward the “INVITE” to the destination (directly or via other Proxy/Proxies). The destination sends back a “RINGING” message to the DAP. When the destination UAS goes off hook, an “OK” message is sent to the DAP and negotiation about parameters (codec, payload, etc.) takes place. When negotiation is finished and accepted, the DAP (UAC) sends an “ACK” message to the destination (UAS).

Note: *Tones for a DECT handset is generated by the DAP on which the handset is locked.*

- **Call setup between DECT Handsets**
  A call setup from one DECT handset to the other, is a combination of an initial call from a DECT handset and a call setup to a DECT handset extension. .
  Note that there are two SIP signalling (INVITE etc.) paths: and the SIP Proxy and between the UAS DAP and the SIP Proxy. The actual speech connection is directly
  - for the originating side, between the UAC DAP where the subscription record of the originating handset resides.
  - for the destination side, between the UAS DAP where the subscription record of the destination handset resides.

  When the destination handset answers the call, an RTP speech path is established between the DAP where the originating handset is locked and the DAP on which the destination handset is locked (peer-to-peer). See Figure 2-6 "Speech connection between two DECT handsets"

Note: *The signalling end point (DAP) for a handset my differ from the RTP (Speech) end point (DAP). The signalling path is on the DAP where the handset subscription record resides. The RTP connection is on the DAP where the handset was locked at the time of call setup.*

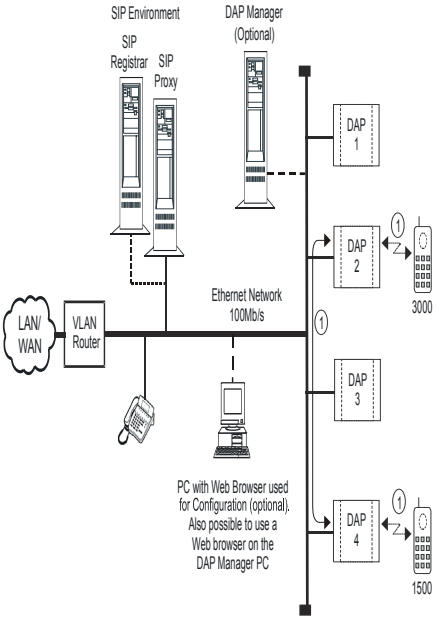


Figure 2-6 Speech connection between two DECT handsets

2.6. 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 figure Figure 2-7 "Call connection before handover." a call is depicted between a SIP IP telephone and a DECT handset with extension number 1500. The speech path is a peer-to-peer VoIP connection between the SIP IP extension and DAP 4.

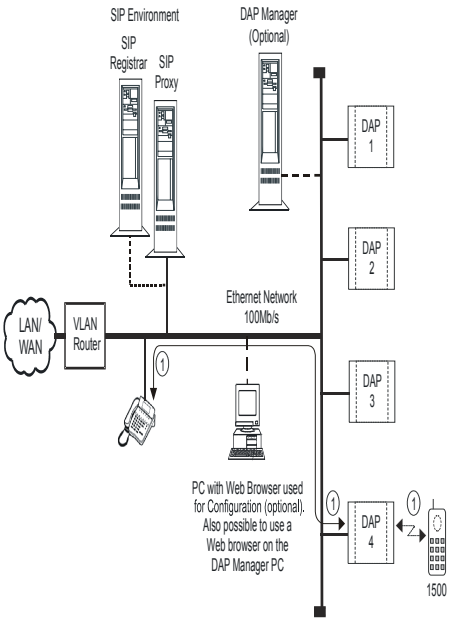


Figure 2-7 Call connection before handover.

However, handset 1500 moves from DAP 4 to DAP 3. See Figure 2-8 "Handover action started."The handset searches for a better radio signal, and detects a DAP 3. It issues a request for handover to DAP 3. However, DAP 3 does not know where the existing voice connection to handset 1500 resides so it multicast (2) a request for searching previous connection to handset 1500 over the network with DAPs. DAP 4 will respond to this request because the call was initially be set up via this DAP.

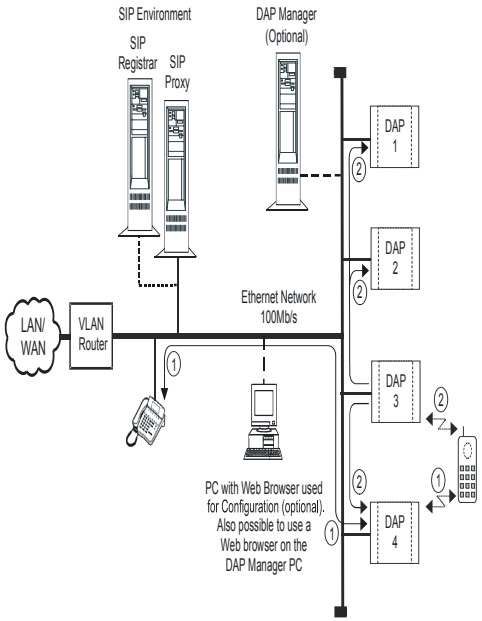


Figure 2-8 Handover action started.

After this the connection is diverted (3) from DAP 4 to DAP 3. See Figure 2-9 "Handover taken place, new connection active." DAP 4 will release the radio connection to the handset and diverts it over the IP network. Note that the original connection is not removed from DAP 4, but DAP 4 "relays" the connection to DAP 3. DAP 4 cannot release the IP voice connection, because the IP voice connection between the SIP IP extension and the DAP 4 is established, based on a combination of sockets. This combination is fixed during the connection.

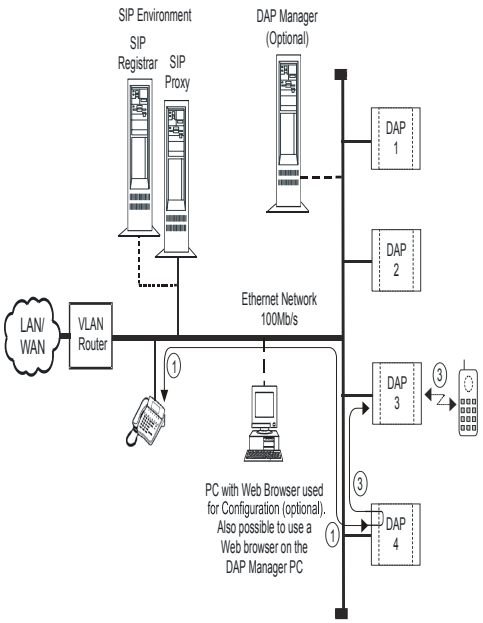


Figure 2-9 Handover taken place, new connection active.

If a second handover takes place, DAP 4 will still be relaying the call, but now to another DAP.

2.7. Detailed Insight

The Business Mobility IP DECT system is based on three Data Servers:

- **SDS** (SIP Data Server)
  The SDS takes care of call setup handling between the DAP and the SIP Proxy. The SDS is therefore installed in each DAP in the Business Mobility IP DECT system.

- **DDS** (DECT Data Server)
  The DDS has a *twofold* function. It takes care of call setup handling to/from the handsets and does subscription management. Depending on where the DDS is installed, the one of the functions is activated. The DDS will be installed in:
  - AP200
    The DDS is automatically installed in the AP200. In the AP200, it takes care of call

handling for DECT handsets.

- DAP Manager
  In the DAP Manager, the DDS is automatically installed. (The DAP Manager is not always needed.) The DDS in the DAP Manager takes care of subscription handling. If you subscribe a handset, the DDS in the DAP Manager is needed and therefore the DAP Manager is needed for subscription. The DDS in the DAP Manager is also needed, when your system comprises one or more branch offices with DAPs. It takes care of automatically moving subscription records between islands when handsets move between the islands.

- **CDS** (Control Data Server)
  The CDS is a set of files in the IIS environment in the DAP Manager. It is used the DECT Manager WEB interface.

Figure Figure 2-10 "Server processes in the Business Mobility IP DECT structure"shows the structure:

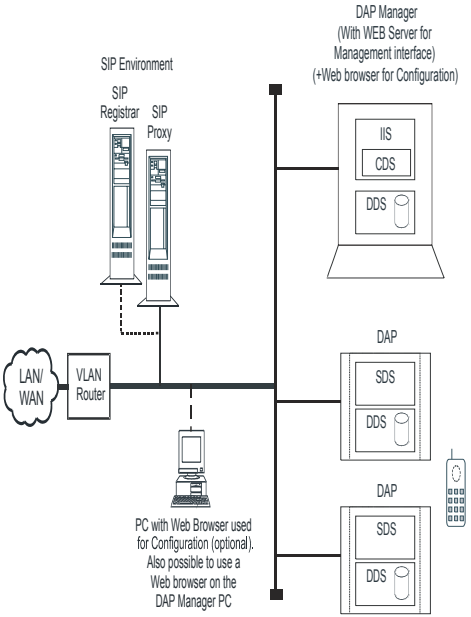


Figure 2-10 Server processes in the Business Mobility IP DECT structure

2.8. Is DAP Manager Required?

The DAP Manager is not required for call handling. A simple Business Mobility IP DECT system will therefore look like Figure 2-11 "Simple Business Mobility IP DECT configuration without DAP Manager."

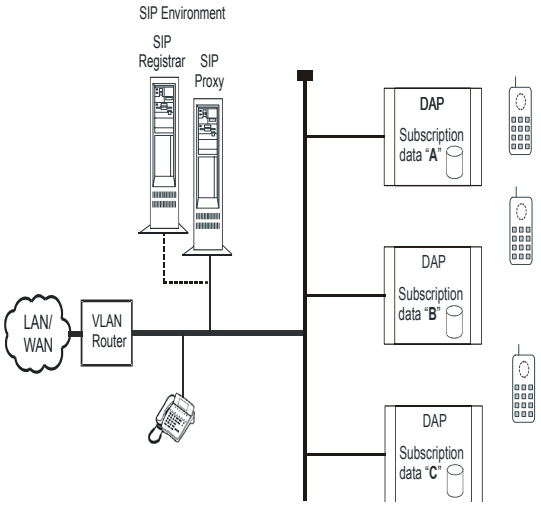


Figure 2-11 Simple Business Mobility IP DECT configuration without DAP Manager.

The subscription data is stored in the DAPs.

The DAP Manager is temporary needed in the following cases:

- **During installation**
  During installation the DAP Manager is needed to enter licence information, extension numbers, to subscribe handsets etc.
- **Management**
  For any system management action the DAP Manager is needed
- **Replacing a DAP (AP200)**
  When you replace a DAP (AP200) be aware that it may contain subscription data. Therefore, you need to open the DAP Manager WEB interface and execute a delete DAP. Then the subscription data that was in this DAP is put into the remaining DAPs. If you put a new DAP in place, initially it will not contain subscription data. Only after executing a

subscription procedure, it may contain subscription data.

Note: *Be aware of the fact that in a number of system configurations, the DAP Manager is always needed.*

In the following cases, the DAP Manager is **always** needed:

- **Branch office configuration**
  If your Business Mobility IP DECT system comprises a Main site and one or more branch offices over a router using unicast, these DECT islands require the DAP Manager for automatically moving subscription data when a handset moves from one island to another (island = main site or (one of) the branch office(s)). The DAP Manager is not necessary for call handling.
  Also the DAP Manager is needed for backup of subscription data. If there are branch offices in the DAP Controller configuration, the subscription records are stored in RAM in the DAPs. If a DAP goes down and starts up again, the DAP will get the subscription data from the DAP Manager! If there are NO Branch office DAPs the subscription data is stored in FEPROM in the DAPs. In that case, the DAP Manager is not needed as subscription database.
- **Low Rate Messaging Service (DECT Messaging)**
  DECT Messaging always require the DAP Manager.

2.9. Radio Synchronization

2.9.1. 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.

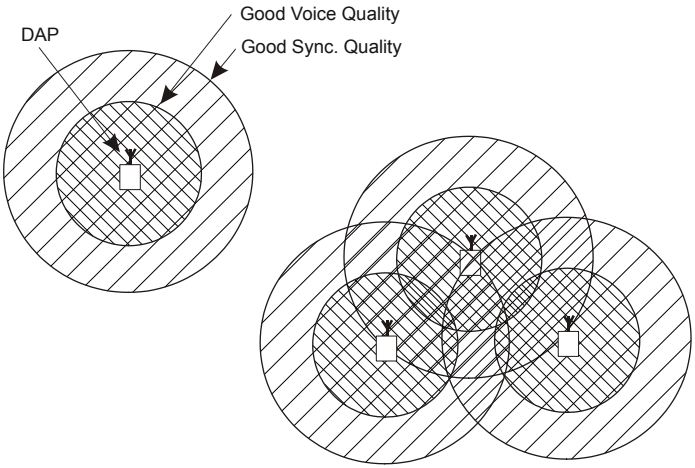


Figure 2-12 Radio Synchronization.

A DAP (Radio) cell can be seen theoretically as a circle around the DAP. In Figure 2-12 "Radio Synchronization." 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).

2.9.2. 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.

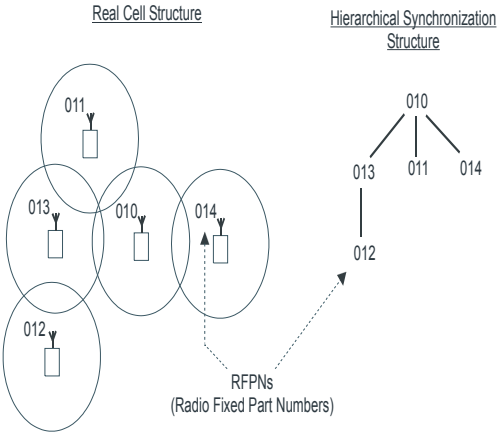


Figure 2-13 Synchronization Structure.

In Figure 2-13 "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 010 it means that it will become the synchronization source! The DAPs with RPNs 011, 013 and 014 will synchronize to RPN 010. However, RPN 012 will synchronize to RPN 013 although RPN 013 is a higher number. Finding a synchronization source is not limited to one level deep only. DAP 012 knows that DAP 013 is synchronized to a DAP (010) that has a lower number than itself. Therefore DAP 012 will synchronize to DAP 013, because it is aware that DAP 013 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.

The DAP Controller keeps track of the synchronization structure. 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 DECT Manager WEB interface.

The automatically assigned RPNs start at:

- **10**
  The automatic assignment of RPNs starts at 10 when the IP DECT system is setup as Distributed DAP Controller
  Manually assigned numbers can be in the range 00 . . . 0F.

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

2.9.3. 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 2-14 "Signal Strength considerations."

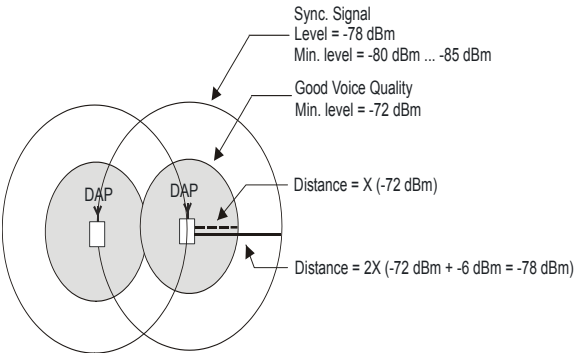


Figure 2-14 Signal Strength considerations.

- 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 then for speech. (50% frame loss is still exceptable).

Practice has indicated that coverage measurements for traditional DECT can also be applied for Business Mobility IP DECT.

2.10. IP Port Number Assignments

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

In the DAP Controller, there is a predefined "pool" of IP port numbers. This is specified in file `dapcfg.txt`. You can access the data is this file using the DAP Configurator tool (see chapter 8. "CONFIGURATION - DAP CONFIGURATOR TOOL") and adapt the port number range to your wishes.

2.11. AP200S Characteristics

Note: *The AP200S is a dedicated SIP DAP, which must be used in a license free IP DECT system for SIP connectivity. It does not support the G.729 codec.*

The AP200S is the SIP release of the DAP for the Radio Traffic. It has the following main characteristics:

- **Features**

Note: *The features in the following list are AP200S features. If the SIP environment does not support these features, then they are not available!*
  - DECT GAP and CAP compatible.
  - DECT Seamless handover.
  - DECT Low Rate Messaging Service (LRMS) (Max. number of characters depends on the type of handset used.)
  - CLIP and Name Display.
  - Enquiry
  - Call Progress tones.
  - DTMF tones.
  - Message Waiting indication.
  - AP200S Software downloadable.
- **Capacity**
  - Max. number of simultaneous calls: 12
  - Max. number of simultaneous relay calls: 12
  - Max. number of AP200S per network: 255
  - Max. number of simultaneous calls per network: depening on network configuration and available AP200S 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
  - DTMF generation: H.245
  - Call control protocol: Proprietary.
  - IP protocols: DHCP and TFTP
- **Environmental Conditions**
  - Storage temperature range: -25° to +55° Celsius

- Operational temperature: 5° to +40° Celsius

Note: *The operational temperature range is 5° to 40° Celsius. When you use the AP200 outdoor, and you install it in an outdoor box which is NOT isolated, make sure that there is a heater, or cooler in the outdoor box.*
However, there is an isolated outdoor box available. Installing the AP200(E) in this type of outdoor box, the allowed temperature range is -20° to 50° Celsius.

2.12. AP200 Characteristics

The AP200 is the General release of the DAP for the Radio Traffic. It has the following main characteristics:

Note: *If you connect one or more General DAP versions to the IP DECT system , the license mechanism is enabled and you need to have licenses as explained in Section* 2.14. "Licences"

- **Features**

Note: *The features in the following list are AP200 features. If the SIP environment does not support these features, then they are not available!*
- DECT GAP and CAP compatible.
- DECT Seamless handover.
- DECT Low Rate Messaging Service (LRMS) (Max. number of characters depends on the type of handset used.)
- CLIP and Name Display.
- Enquiry
- Call Progress tones.
- DTMF tones.
- Message Waiting indication.
- AP200 Software downloadable.

- **Capacity**
  - Max. number of simultaneous calls: 12
    However, the actual maximum number of simultaneous calls depends on the number of channel licenses assigned to the DAP.
  - Max. number of simultaneous relay calls: 12
  - Max. number of AP200s per network: 256
  - Max. number of AP200s with DAPs in Branch Offices: 750
  - Max. number of simultaneous calls per network: depening on network configuration and available AP200 channels.
  - Max. number of handsets per network: 6000

- **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 (aLaw PCM) and/or G729.
    Note that the number of simultaneous G729 calls per AP200 is licensed. The license can be set or changed via the DECT Manager.
  - DTMF generation: H.245
  - Call control protocol: Proprietary.
  - IP protocols: DHCP and TFTP

- **Environmental Conditions**
  - Storage temperature range: -25° to +55° Celsius
  - Operational temperature: 5° to +40° Celsius

Note: *The operational temperature range is 5° to 40° Celsius. When you use the AP200 outdoor, and you install it in an outdoor box which is NOT isolated, make sure that there is a heater, or cooler in the outdoor box.*
However, there is an isolated outdoor box available. Installing the AP200(E) in this type of outdoor box, the allowed temperature range is -20° to 50° Celsius.

2.13. DAP (AP200 / AP200S) Power Provision

A DAP can be powered on two different ways:

- Line powering
  The AP200/AP200S supports Line powering according to specification IEEE802.3af. It support both versions: "phantom power" as well as "power over spare wires".
  The voltage at the patch panel should be between 42 Volts and 60 Volts.
  Note that the distance depends on the cable type and the voltage at the patch panel.
- External Power Supply
  External Power supply connected to the Power Connector on the AP200. This power supply should meet the following requirements:
  - AC/AC Power adapter
  - Secondary voltage: 40 V AC, +10%/-10%
  - Maximum power consumption: 10 Watts

2.14. Licences

Note: *This section is only applicable when you have one or more AP200 General version in your IP DECT System. If you have only AP200S DAPs in your system licenses are included in the product and the license mechanism is disabled.*

2.14.1. Licenses with AP200S

In a system with AP200S DAPs only, the license mechanism is disabled for a general system configuration. If one or more AP200 DAPs are connected to the system, licenses are required!

However, licenses are required if you want to expand your system with the following items:

- Use of G.729 Codec over routers
- Multi-site subscriptions based on a SARI.

This requires that the License mechanism must be enabled. To enable the License mechanism, connect one or more AP200 (without suffix "S") to the system.

2.14.2. Licenses with AP200

For Business Mobility IP DECT Release 3 with AP200 General version, the following licences are required:

- **Handset licences.**
  This is the maximum number of handsets that you can subscribe to the Business Mobility IP DECT system. This licence type was already used in previous releases of the Business Mobility IP DECT system.

- **2 Channel Upgrade License (DAP Channel Licence)**
  Without having a "2 Channel Upgrade Licence", each AP200 can use 2 radio channels. You can upgrade the number of available channels by means of this "2 Channel Upgrade licence". The maximum number of radio channels in the system is therefore the sum of the two licence-free radio channels of each AP200 and the "2 Channel Upgrade License".

Note: *When an AP200 does not have extra channels enabled via the "2 Channel Upgrade Licence", it operates with the default of two channels available. However, in this mode it operates as a single cell radio and does not synchronize with other DAPs! Handover is not possible! So, you always require sufficient "2 Channel Upgrade Licences" in the system, in order to enable the AP200s for handover!*

In the DECT Manager, the number of channels that become available via the "2 Channel Upgrade Licence" mechanism, must be "spread" over the AP200s in the system. This is

done by enabling a number of channels on each individual AP200. The maximum number of channels per AP200 can be set to 12.
For the AP100 the number of available radio channels is a fixed value of 4. The AP100s in the system are excluded from this licence mechanism.

- **G.729 Licences**
  This is the maximum number concurrent/simultaneous G.729 channels in use in the system.

- **Multi-site PPs Licence**
  This is the (maximum) number of handsets that are used in a multi-site environment. Multi-site handsets (PPs) are used on more than one DECT system, using a SARI. This means that the handset carries only one subscription record for more than one DECT system. Consult section 1.9. "Secondary Access Rights Identifier (SARI)" for more information about using a SARI.

- **Number of Branch Office DAPs**
  This is the number of DAPs that are in Branch Offices, connected via a router using unicast only (no multicast over the router).

- **PABX Type**
  The PABX type is not a real licence but a qualifier on the licence that you have. A Business Mobility IP DECT system licence is created for a specific PBX system type and cannot be used for a Business Mobility IP DECT system that is connected to another type of PBX. When you open the DECT Manager WEB interface, you see the PABX type already filled in and greyed out. This means that you cannot change the PABX type in the Licence menu in the DECT Manager WEB interface.

The DECT Manager interface allows you to:

- change the licences.
- read out the licence values.
- read out the currently occupied licences.

All of these licenses must be set via the DECT Manager interface.

Note: *The License items in the DECT Manager are only visible, if one or more AP200 (without suffix "S" are connected to the IP DECT system.*

2.15. More than 255 DAPS

IP DECT Release 4 allows you to setup an IP DECT System with more than 255 DAPs. To

achieve this, you must assign RPN number ranges to DAPs in the branch offices. For more info, see Section 2.15. "More than 255 DAPS"

2.16. RPN Number Ranges per Branch Office

In IP DECT Release 4, you can specify the range of RPN numbers that you want to use in the Head Quarter and in the individual Branch Offices. That allows you to use up to 750 DAPs in one IP DECT installation. Per Branch Office, the maximum number of DAPs is 256. Also in the Head Quarter, the maximum number of DAPs may not exceed 256.

The Branch office DAPs are not allowed to “see” DAPs of other Branch Offices or the Head Quarter.

Because the RPN number range is related to the Head Quarter or to Branch Offices, the RPN number range is related to an IP network segment.

The DAP Configurator lets you set up the configuration in a very simple way, by means of assigning RPN numbers to a Branch Office.

The RPN numbers in the DAP Manager, Release 4, exist of three digits instead of two. The RPN number that is displayed in the handset (in special mode) consists of the two least significant digits of the RPN number in the DAP Manager.

The configuration is stored in a file: `bo_adm.txt`.

3. NETWORK CONFIGURATIONS

3.1. Typical Configurations

The IP DECT system must be implemented in a company infrastructure. As mind setting tool, this chapter gives you four typical configurations with the advantages and disadvantages. All configurations are based on using one IP DECT system (DECT Cluster) in the network. You should consider which configuration you must implement at the customer site. In the IP DECT Advance Data Manual, you will find more informtion about the syatem behavior over a router, in chapter “System Behavior over Router”.

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).

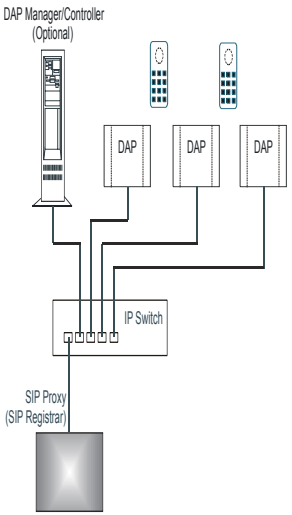


Figure 3-1 Example of Simple IP DECT network configuration.

The general characteristics of a simple configuration are as follows:

- Seamless handover is supported between all DAPs.

3.3. Branch Office Solution

Figure 3-2 "Example of an IP DECT configuration with Branch Offices." shows an example of a Branch Office configuration with a main office (head quarter) and two Branch Offices. Main Office and Branch Offices are in different subnets connected via routers. Routers can be connected over the WAN.

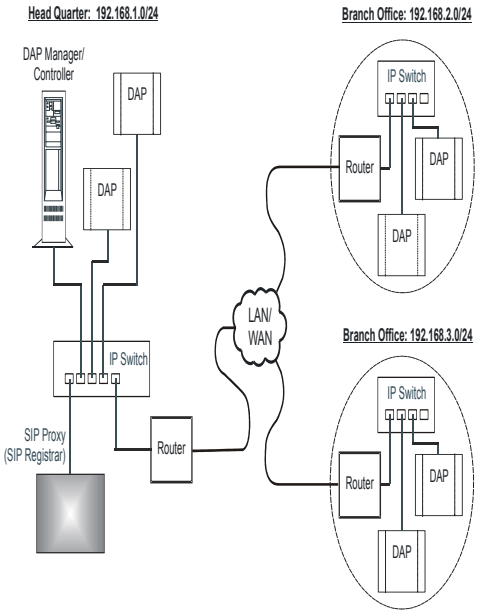


Figure 3-2 Example of an IP DECT configuration with Branch Offices.

The general characteristics of an IP DECT configuration with Branch Offices are as follows:

- Allows interconnections with limited bandwidth between Head Quarter and Branch office(s).
- Allows interconnections with poor QoS between Head Quarter and Branch office(s). (Radio Links, ADSL etc.)
- No PBX needed in Branch Office(!).
- Seamless handover is supported in Branch Offices and in Main Office.
- No handset handover between Head Quarters and (individual) Branch Offices.
- Head Quarter and individual Branch Offices must be in separate subnets (router(s) needed).
- No IP multicast support required for Routers.
- Multicast TTL = 1, which means that IP multicast packages does not cross a router.
- DAPs in Branch Offices need a licence.

3.4. Routed Head Quarter

Figure 3-3 "Example of an IP DECT Routed Head Quarter configuration." shows an example of a Routed Head Quarter configuration with a head quarter and two subnets connected via one or more routers. The subnets in the network are part of one company network.

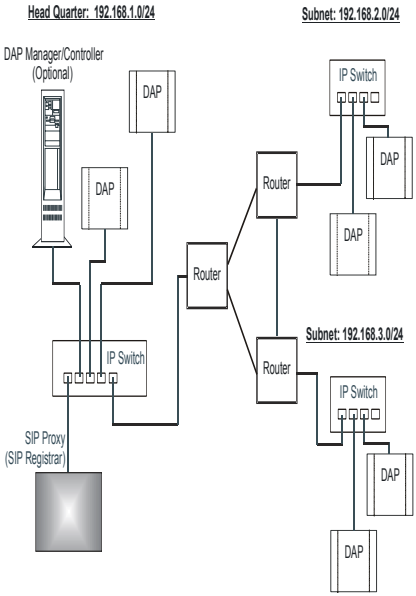


Figure 3-3 Example of an IP DECT Routed Head Quarter configuration.

The general characteristics of an IP DECT Routed Head Quarter configuration are as follows:

- Used for a Large Campus network that is split up into different (geographical) subnets.
- The network supports QoS and IP connectivity all over the Campus.
- IP DECT configuration behaves as one large IP DECT system.
- Full support of seamless handover between all DAPs in the IP DECT system.
- Routers must support IP Multicast routing.
- The IP Multicast address for IP DECT is the same in all segments.
- Multicast TTL > 1, which means that the routers pass on the IP multicast packages.
- In the IP DECT configuration, you must enter the subnet mask that is needed to cover all networks.(e.g. 255.255.248.0) for up to four subnets as in the previous example.

3.5. Routed Head Quarter with Branch Offices

Note: *The Branch Office solution is only available when you use the Licensed version of the IP DECT system, which means you must have the AP200 General version of the DAPs and you must have sufficient licenses.*

Figure 3-4 "Example of an IP DECT Routed Head Quarter configuration with Branch Office." shows an example of a Routed Head Quarter configuration with a head quarter, one subnet connected via one or more routers and a Branch Office. The subnets in the network are part of one company network, the Branch Office is connected over the WAN (or low troughput LAN).

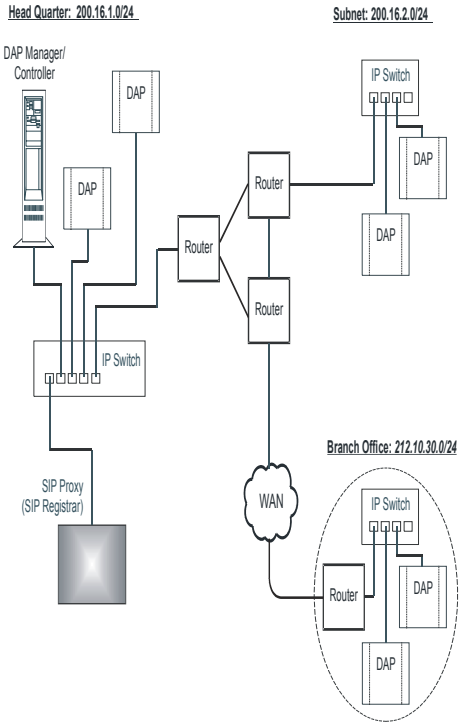


Figure 3-4 Example of an IP DECT Routed Head Quarter configuration with Branch Office.

The general characteristics of an IP DECT Routed Head Quarter configuration with Branch

Office(s) are as follows:

- Hybrid of Routed Head Quarter and Branch Offices (see previous sections).
- Used for a Large Campus network that is split up into different (geographical) subnets in combination with (remote) Branch Offices.
- In the Routed Head Quarter part, all characteristics which are mentioned previously for the Routed Head Quarter are applicable.
- For the Branch Office, all characteristics which are mentioned in the section covering the Branch Offices are applicable.
- In the Head Quarter the Multicast TTL > 1, in the branch Office the Multicast TTL = 1(!).
- Edge Router, connected to the WAN, should not forward Multicast packages to the WAN.
- Full support of seamless handover between all DAPs in the Head Quarters configuration with the subnet.
- Routers in the Head Quarter must support IP Multicast routing.
- In the IP DECT configuration, you must define which subnets are in the Head Quarters and which subnet(s) is/are Branch Office subnets. You must do that by means of specifying the subnet mask that is needed to cover all Head Quarters subnetworks.(e.g. 255.255.248.0 for up to four subnets as in the example.).

4. DAP INSTALLATION ITEMs

4.1. General

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

- DAPs must be installed in vertical position, bacause 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 can be powered locally via an RJ11 connector. However, they also support Power over Ethernet, the so called PoE (laid down in IEEE802.3af specification).

For redundancy reasons, it is possible to choose for both types of power provision on the same DAP. The power provision that provides the highest voltage will be active. If one of the power inputs fail, the other will smoothly take over.

4.2.1. Local Power Provision

Local Power Provision is done via an RJ11 connector at the DAP.

In Figure 4-1 "DAP AC Power connector for local power supply.", the RJ11 layout is depicted.

RJ11 Connector on DAP

Legend;

1 = AC2 (or DC2)
2 = AC1 (or DC1)
3 = AC1 (or DC1)
4 = AC2 (or DC2)

Figure 4-1 DAP AC Power connector for local power supply.

The AC voltage must be 40V (+/- 10%). Use an AC adaptor that can provide at least 10 Watts.

4.2.2. Power Provision via Ethernet

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 60 Volts.
- Connector: Standard RJ45 connector, using the spare wires pins (wires). See Figure 4-2 "Pin Layout Ethernet Connector RJ45 on the DAP."
- Maximum cable length: 100 meters

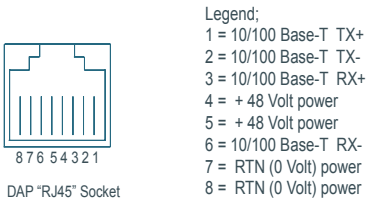


Figure 4-2 Pin Layout Ethernet Connector RJ45 on the DAP.

4.3. DHCP and TFTP Requirements

The DAPs must get their IP addresses, configuration file and firmware from the IP network using a DHCP Server and a TFTP Server.

4.3.1. DHCP Server

When a DAP starts up, it tries to contact a DHCP server on the network. It should get the following items from the DHCP server:

1. IP Address
2. Subnet Mask
3. Default Gateway IP address
4. Next Boot Server IP address. This is the IP address of the TFTP Server (DHCP option 066).
5. Configuration file name (`dapcfg.txt`) available via the TFTP server (DHCP option 067).

The easiest way to provide the DAPs with the correct data from the DHCP server, is using the DHCP server that comes with the DAP Controller installation software. The DAP Configurator tool allows you to setup the required DHCP server configuration easily.

Note: *The DHCP Server that comes with the installation of the DAP Controller/Manager is by default installed when you do the installation for "Multiple System". If you do the*

installation for "Single System", the DHCP server is not installed by default. However, if you select "Custom" installation you can choose to install or not install the DHCP server. See installtion procedure in Section 7.2. "Installing the DAP Manager"

However, if you don't want to use the DHCP server that comes with the DAP Controller installation, e.g. because there is DHCP server already in the network, you can use a DHCP server of your choice. But make sure that the required parameters are delivered to the DAPs.

4.3.2. TFTP Server

The configuration file and the firmware are uploaded to the DAP(s) using a TFTP server. The DAP Controller software includes a TFTP Server. You can select that TFTP server using the DAP Configurator. When you use the TFTP server that comes with the DAP Controller, the TFTP Server configuration is automatically setup correctly.

Note: *The TFTP Server that comes with the installation of the DAP Controller/Manager is by default installed when you do the installation for "Multiple System". If you do the installation for "Single System", the TFTP server is not installed by default. However, if you select "Custom" installation you can choose to install or not install the TFTP server. See installtion procedure in Section 7.2. "Installing the DAP Manager"*

However, it is also possible to use a TFTP server of your choice.

4.3.3. Operation without DHCP or TFTP Server

If your DHCP server and or TFTP server is not permenently connected, you can store the IP address and the configuration file in the DAPS in Flash memory. Note that the firmware is alsways stored in Flash memory in a DAP.

To store the IP address configuration in Flash memory in the DAP, the following two requirements must have been met:

- The DHCP server must issue an "Infinite" lease time. (The DHCP server that comes with the DAP Controller issues such a lease time by default!)
- In the configuration setup, you must select "Replace" from the drop down menu for IP Confguration in the boot options in the DAP configurator screen. See section 8.5.2. ""IP Settings"".

After this the DAP does not need a DHCP server anymore.

To store the Configuration file in Flash memory in the DAP, the following two requirements must have been met:

- The DHCP server must issue an “Infinite” lease time. (The DHCP server that comes with the DAP Controller issues such a lease time by default!)
- In the configuration setup, you must select “Replace” from the drop down menu for DAP Confguration in the boot options in the DAP configurator screen. See section 8.5.2. ""“IP Settings”"".

When IP configuration and configuration file are stored in the DAP, the DAP does not need to have a DHCP server nor TFTP server anymore in the startup processes.

Note: *When a DAP starts up, it still does a DHCP request and TFTP request. If it gets valid data from the DHCP Server and TFTP server, and a valid configuration file with boot options set to “erase” or “Repalce” it will either erase or replace the stored data. If it doesn’t get those three items (DHCP, TFTP and valid file) the DAP ignores the data that it has got, and starts up with the stored data.*

4.3.4. Using other DHCP and/or TFTP Servers

Note: *If you install the DAP controller/Manager software as “Single System” the DHCP and TFTP server are normally not installed. This means that you must use your own DHCP or TFTP server. Consult the “Business Mobility IP DECT Advanced Data Manual”, Chapter “Other DHCP/TFTP Servers” for examples of other servers.*

It is possible to use a DHCP server or TFTP server of your choice. However, the DHCP server must provide the five parameters as mentioned in 4.3.1. "DHCP Server". Also mind the lease time specification if you want to store IP configuration and/or DAP configuration data in the DAP(s).

The TFTP server must be capable of handling as many simultaneous TFTP request as there are DAPs. Remember, if the DAPs starts up simultaneously, they do a TFTP request simultaneously.

In the IP DECT Advanced Data Manual, you find examples of how to setup other DHCP and TFTP servers.

5. PREPARING YOUR DAP MANAGER PC

5.1. Hardware Requirements

The PC that is used for the Business Mobility IP DECT software must comply with the following requirements:

- CPU speed: 2,4 GHz or higher
- 256 Mb RAM or more
- CD-ROM drive
- 1Gb harddisk space free

5.2. Software Requirements

The operating system for the DAP Controller/Manager PC should be as follows:

- Windows 2000 Professional or Windows 2000/2003 Server. Windows 2000 requires SP4.
- Windows XP Professional, SP2.

Note: *The DAP Controller/Manager supports the International (English US) version of the above mentioned MS Windows operating systems. Other MS Windows language versions are not explicitly tested but are not expected to show any problems. In case of problems please contact ypur IP DECT Supplier, and clearly indicate which MS Windows version is used and the nature of the problem.*

Besides the operating system, the Windows WEB server, called IIS (Internet Information Services) must be installed. This is described in Section 5.4. "Installing IIS".

5.3. Firewall in MS Windows

Windows XP Professional and Windows 2003 Server are provided with a build-in firewall.

Note: *By default the firewall under Windows XP Professional does not allow incoming access. However, the DAP Configurator will automatically change the firewall settings, if necessary. However, it is wise to check the changes after the installation!*

5.4. Installing IIS

5.4.1. General

The DAP Controller/Manager runs as a service under Windows. The management interface is available via a WEB interface. Therefore you must install the WEB Server "IIS".

The following procedure guides you through the IIS installation process for Windows XP Professional, Windows 2000 and Windows 2003. Note that you need to have the Windows installation CD-ROM for this.

Note: *In Windows 2000 Professional, Windows XP Professional and Windows 2003 Server, IIS is not installed by default. In Windows 2000 Server, IIS is always installed by default.*

To install IIS, go to the appropriate subsection in this section.

5.4.2. Installing IIS under Windows XP

The DAP Manager requires that Internet Information Services is installed on your computer.

Note: *The Procedures in this section are applicable for Windows XP Professional.*

Use the following procedure to check if IIS is installed and up-and-running on your computer.

PROCEDURE: Checking IIS

Actions

1. Open Internet Explorer on the computer where you want to install the DAP Manager.
2. Enter the following URL: `http://localhost/localstart.asp`.
3. Check that the following window is displayed:

4. If the page is not displayed, continue with the following procedure to install IIS on your computer.
   If this page is displayed correctly, IIS is installed and up-and-running. Close the window and continue with the next chapter.

PROCEDURE: Installing IIS under Windows XP Professional

Actions

1. From the **Start** go to the **Control Panel**.
2. Double click **Add/Remove Programs** to open it.
3. Click on the **Add/Remove Windows Components**.
4. *Select* **Internet Information Services**. Note: do *not* check the checkbox!
5. Click the button **Details**
6. In the details window, check the check box **World Wide Web Service**.
7. Click **OK**.
8. Click **Next**.
9. Insert the **Windows XP Professional CD** when the system asks for it and click **OK**.
   If the "Welcome to Microsoft Windows XP" window pops up, it is a result of the "auto run" on the CD. Click "Exit" in the bottom left corner of the window.
10. In the Windows Components wizard, click **Finish**.
11. Close the **Add/Remove Programs** window and close the **Control panel** window.
12. If present remove CD/DVD and/or floppy from your system. Close all windows and **Restart** your computer
13. After the computer is restarted, check that IIS is up-and-running. If not, consult the Microsoft web site.
    To check if IIS is up and running, return to the previous procedure: PROCEDURE: "Checking IIS"

5.4.3. Installing IIS under Windows 2000

PROCEDURE: Installing IIS under Windows 2000

Actions

1. From the **Start** go to **Settings** menu and open the **Control Panel**.
2. Open **Add/Remove Programs**.
3. Click on the **Add/Remove Windows Components**.
4. In the components window, check the check box **Internet Information Services**.
5. Click **Next**.
6. Insert the Windows CD-ROM when the system asks for it.
7. Finish the procedure via the instructions on the screen.

8. Close the **Add/Remove Programs** window and close the **Control panel** window.

Note: *After having installed IIS, you must re-install Windows 2000 Service Pack 4 (or higher) again.*

To check the proper functioning of IIS under Windows 2000, execute the following procedure:

PROCEDURE: Checking IIS functions under Windows 2000

Actions

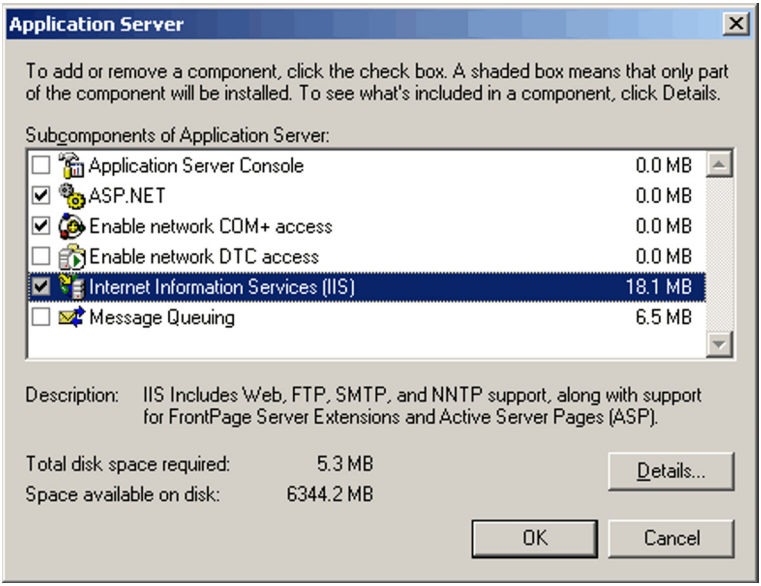
1. Open "Internet Explorer" on the PC where you have installed the IIS. In the address bar in IE, enter the following line: **http://localhost/iisHelp/** and then press "enter". Now you will see the documentation (Help Information) of IIS displayed. This proves that your IIS is up and running. If you want to learn more of IIS you can use this information. The topic you have searched for is available in the IIS on-line help.
   If you cannot reach the WEB server via the Internet Explorer, check the Windows Help and search for IIS. You will find a description to check whether IIS is started or not. If it seems that IIS is not started, go to the next step and check whether it runs or not and start IIS if necessary.
2. You can start Windows Internet Information Services by clicking "Start", pointing to "Settings", and clicking "Control Panel". Double-click "Administrative Tools" and then double-click "Computer Management". Expand the "Services and Applications" node in the console tree of the Microsoft Management Console (MMC) and select "Internet Information Services".
   If you right mouse click on the "Internet Information Services", you can restart the services. If you right mouse click on the lower levels of the "Internet Information Services", you can stop or start the individual services.

5.4.4. Installing IIS under Windows 2003

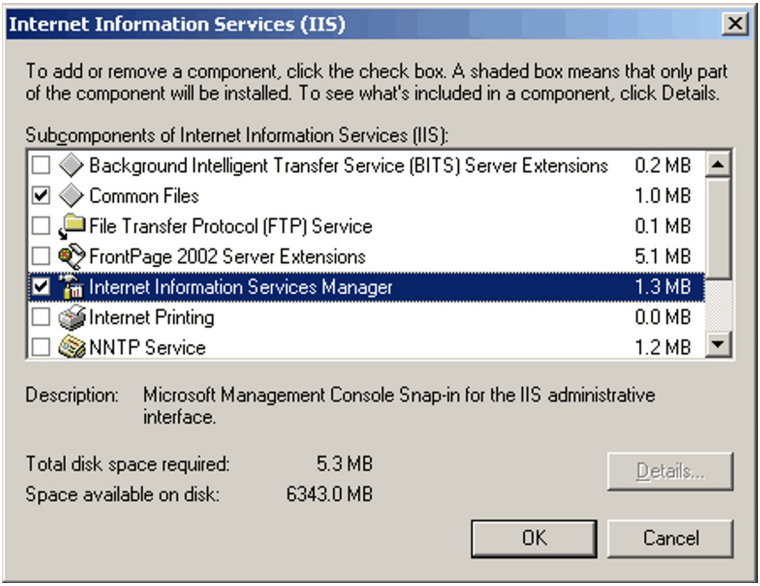
PROCEDURE: Installing IIS under Windows 2003

Actions

1. From the **Start** go to the **Control Panel**.
2. Open **Add/Remove Programs**.
3. Click on the **Add/Remove Windows Components**.
4. In the components window, double click **Application Server**
5. In the components window (see screen capture), check the check box **ASP.NET.** Then select **Internet Information Services** and click **Details**.



6. The following window is displayed. In this window, make sure that the check boxes are checked for **Internet Information Services Manager** and **Common Files**. Leave remaining check boxes as they are.



7. Click **OK** and again **OK**.
8. Follow the instructions on the screen and insert the Windows CD-ROM when the system asks for it.
9. Finish the procedure via the instructions on the screen.
10. Close the **Add/Remove Programs** window and close the **Control panel** window.

PROCEDURE: (Re)Start IIS

Actions

1. Go to **Start** and click **Control Panel**.
2. Click **Administrative Tools** and then click **Computer Management**.
3. Expand the **Services and Applications** node in the Microsoft Management Console (MMC) and select **Internet Information Services**.
4. Right mouse click the Internet Information Services and select **All Tasks**. In All Tasks, select **Restart**. IIS is now (Re)started.

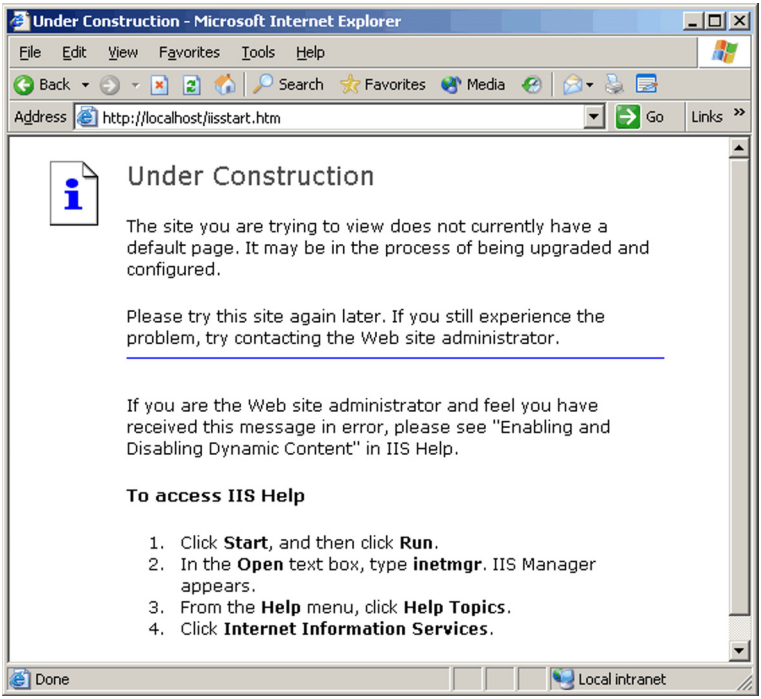
To check the proper functioning of IIS under Windows 2003, execute the following

procedure:

PROCEDURE: Checking IIS function under Windows 2003

Actions

1. Open "Internet Explorer" on the PC where you have installed the IIS. In the address bar in IE, enter the following line: **http://localhost/iisstart.htm** and then press "enter". You will see the following web page displayed.



2. If IIS is not running, properly you can execute a (re)start, see PROCEDURE: "(Re)Start IIS"

6. SIP CONFIGURATION CHARACTERISTICS

6.1. 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. The SIP implementation differs between the various types of SIP Proxy/Registrar servers. It is important to know the basic characteristics of the SIP Proxy/Registrar server to which you want to connect the SIP IP DECT system.

In the following Sections, the Business Mobility IP DECT 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 Business Mobility IP DECT system, continue with the installation of the Business Mobility IP DECT system, see Chapter 7. "INSTALLING THE DAP Controller/ Manager" and onwards.

6.2. Main Characteristics

The following overview shows the main SIP characteristics of the Business Mobility IP DECT system:

- **Connectivity**
  The Business Mobility IP DECT system can be connected to many SIP types of commercial, open-source or freeware SIP Proxy server, SIP Registrar server, SIP Gateways, SIP IP-phones, SIP softphones, SIP IP enabled PBX's etc.
  The Business Mobility IP DECT system can also be connected directly to a DSL line for small branch and home offices.

- **SIP Extension Registration**
  - Usage of SIP Registrar server is supported (optional).
  - Detached portables are unregistered from the SIP registrar server. (Portables can be detached automatically, when they support sending a "Detach" signal and "switches off". Also when they support "Detach" signal and put in the charger in "Silent Charge" mode a Detach signal is send.
  - Digest authentication security.
  - SIP URL configurable: sip:phone-number@ip-address e.g. sip:2500@192.168.1.1 or sip:"phone-number"@host-domainname e.g. sip:2500@sipproxy.test.com.
  - Username and/or password configurable.

- **Transmission**
  - High quality voice over IP, G.711 when the call remains within the LAN segment, or G.711/G.729 when the peer-to-peer connection crosses a router.

- Congestion control and packet filtering.
- Reliable UDP transport using retransmissions.

6.3. Call Handling

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

Feature	Reference
Basic Call	RFC3261 (except for TCP, IP, Multicastr. TLS/ MIME and authentication)
Negotiation of most efficient CODEC based upon network information. - Supported CEDECs: - G.711 a-Law - G.711 u-Law - G.729	RFC 2327 RFC 3264
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 6-1 Supported SIP Features.

6.4. Configurable Items in IP DECT SIP

The following table gives an overview of the items that can be configured in the SIP IP DECT configuration, in order to adapt to the SIP Proxy Server and, if present, SIP Registrar. Note that this gives an overview only, the actual settings must entered during the installation of the Business Mobility IP DECT software when asked for. It is always possible to change the settings after the installation.

Parameter	Default Value	Description
proxy_address	no default	The IP address of the Proxy server
proxy_port	5060	The port number on the Proxy server
registrar_addr	[proxy_address]	The IP address of the Registrar server. IP4, dotted format. If nothing specified, this address is equal to the specified Proxy server address.
registrar_port	[proxy_port]	The port number on the Registrar server. If nothing specified, this address is equal to the specified Proxy server address.
sip_domain	[proxy_address]	SIP Domain. If nothing specified, this address is equal to the specified Proxy server address.
max_intern_dnr_len	6	Extension numbers longer than this value, are considered as “extenal”. Only applicable for nummeric extension numbers.
local_port	5060	Local SIP port on the DAPs.
proxy_packets_only	no	If set to “yes”, the IP DECT accepts packets from the Proxy only
realm1 ... realm5	[empty]	Up to five authentication realms (for both, www and Proxy) can be specified.
user1 ... user5	[empty]	Up to five authentication users (for both, www and Proxy) can be specified. Note: in case “%s” the DNR (extension number) will be used instead.
passw1 ... passw5	[empty]	Up to five authentication passwords (for both, www and Proxy) can be specified.
sdp_late_sendrecv	no	Enables/disables the ability of the SIP DECT to issue an initial invite without SDP offer.
sdp_rfc3264	yes	Enables/disables “Hold” according to RFC3264
sdp_MoH	no	When enabled, no local tone is generated when DECT portable is put in “recv only” (hold) mode.
sdp_payload_size	20	Offered payload size in SDP offer (in msec.) However, the proposed payload size of the other party is used.

sdp_DTMF_rfc2833	no	When enabled, DTMF digits are sent according to RFC2833 (in RTP). Otherwise, the DTMF digits are sent as SIP INFO messages.
mwi_support	no	Enables/disables Message Waiting Indication.

Table 6-2 Configurable Items in SIP IP DECT.

7. INSTALLING THE DAP Controller/Manager

7.1. Preconditions

Before you start the actual installation of the Business Mobility IP DECT software, make sure that you have installed and setup the following software:

- IIS (Internet Information Services)

You need to have the following components as well:

- A DHCP Server is required as well. However, the DAP Controller software Release 4 includes a DHCP Server which is automatically configured when you run the DAP Configurator tool. You may also use an existing DHCP Server in the Network, or your own DHCP Server. For more info on other types of DHCP Servers, consult chapter "Other DHCP/TFTP Servers" in the IP DECT Advanced Data Manual.
  However, make sure that the DHCP Server has correct settings for the Business Mobility IP DECT and reference to the TFTP Server. Also make sure that you have specified an default gateway/router address in the DHCP server, that is within the subnet address range of the DAPs.
- TFTP Server
  This can be an existing TFTP Server in the Network, or your own TFTP Server or the TFTP Server that is included in the IP DECT software

Also make sure that the network components (Switches, Routers) are correctly configured for VoIP and IP multicast. Be fully aware of the network topology! Make sure that the network supports IP Multicast between all network components that are used for Business Mobility IP DECT.

7.2. Installing the DAP Manager

The software is available on CD. To execute the installation, follow the steps in the following procedure.

Make sure that you have the following minimum versions of software:

- DAP Controller/Manager software: Release 4.
- DAP Firmware: 4910c**4xx**.dwl.

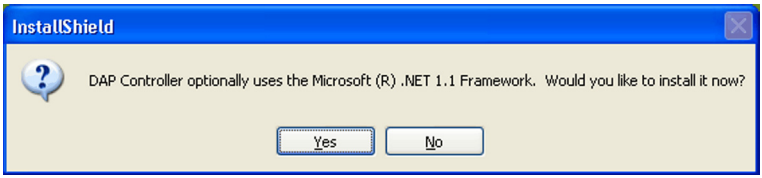
Note: *You only need to execute this procedure once because the installation can be used for as many system configurations as you want. Changing settings can be always be done later.*

PROCEDURE: Installation

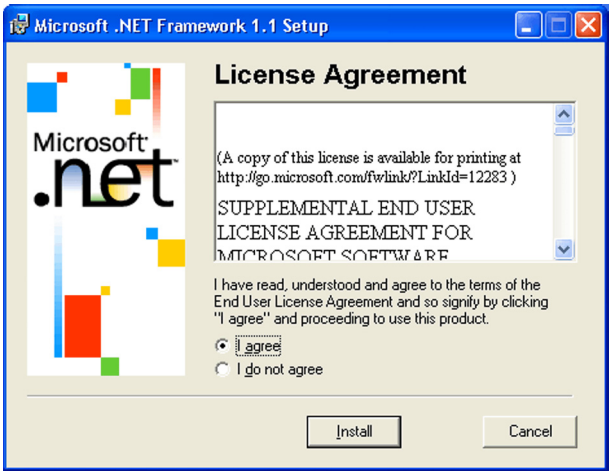
Actions

Note: *Before starting this procedure, make sure that you have setup the IP addressing on the network adaptor properly.*

1. Insert the CD-ROM in the CD drive and run **setup.exe**. Depending on the directory structure on the CD-ROM, the `setup.exe` file may be found in a directory: `Disk1`. You will see a window called "InstalledShield Wizard" displayed. This window remains visible during the installation of the DAP Controller components and gives you information about the installation progress. Also you will see the following window:
2. Now there are two possibilities: either "Microsoft .NET Framework 1.1" is already installed or "Microsoft .NET Framework 1.1" is not yet installed.
   If the "Microsoft .NET Framework 1.1" software is already installed you will see the window "Welcome to the InstallShield Wizard for DAP Controller". Continue with step 6.
   If the "Microsoft .NET Framework 1.1" software is not yet installed you will see the following window displayed:



3. Click **Yes** and wait until you see a window popping up .
4.



Click **I agree** and then **Install**.

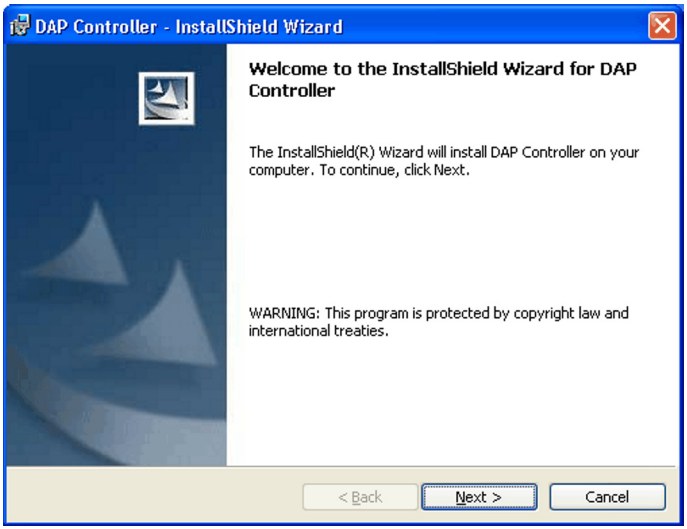
5. After the "Microsoft .NET Framework 1.1" is successfully installed, you will see the following window displayed:

Note, that the installation and configuration of the ".Net Framework" is not finished, even though you have clicked "OK". As long as the configuration process is on-going, the window "DAP Controller - InstallShield Wizard" shows activity in the progress bar. Wait. (This can take several minutes.)

6. When the process is finished, you are asked to restart the PC. click **OK** to restart the PC.

After the PC is restarted, it automatically continues with the DAP Controller installation.

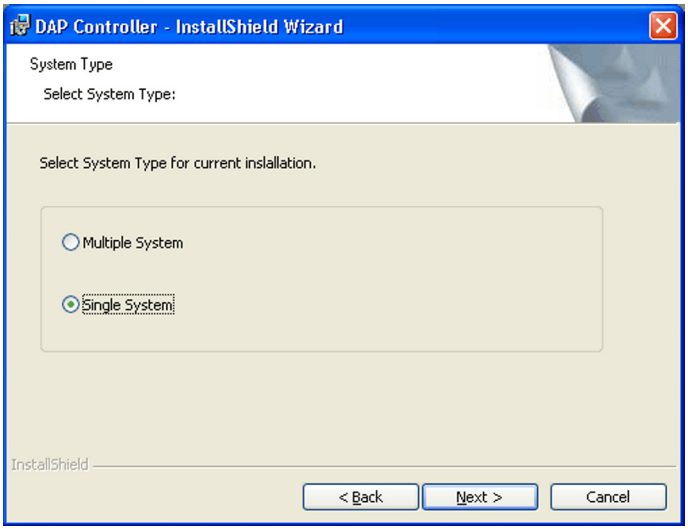
7. The window "DAP Controller - InstallShield Wizard" is displayed with the "Welcome to ...." screen. Click **Next**.



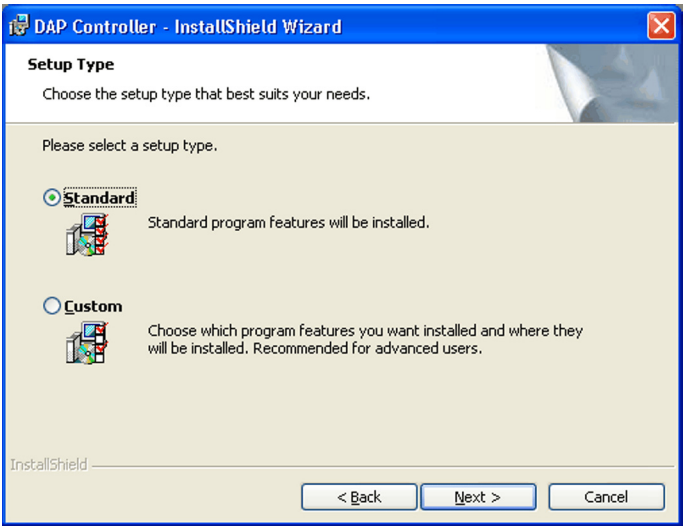
8. The window "DAP Controller - InstallShield Wizard" is displayed with the "System Type" selection screen. Select "**Single System**" if you want to mange only one system, or **Multiple System** if you want to manage more than one IP DECT system with your PC.

Click **Next**.

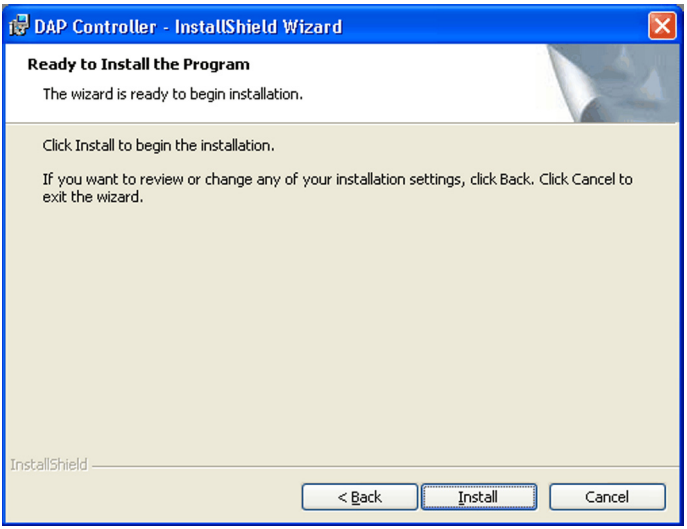
Note: *If you select "Single System" the DHCP Server and TFTP Server are not installed (by default). However, if you want to install them anyway, select the option "Custom" in step 9, and select DHCP Server and TFTP Server to install.*



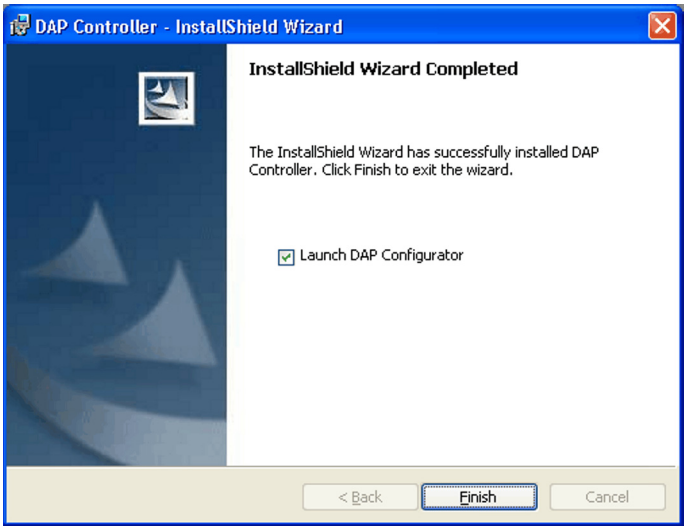
9. The window "DAP Controller - InstallShield Wizard" is displayed with the "Setup Type" screen. Select "**Standard**" and click **Next**. Note that if you want to fine tune the installation you should select "Custom".



10. The system has collected sufficient information to start the actual installation. Click **Install** to start the actual installation.



11. The window “DAP Controller - InstallShield Wizard”, “InstallShield Wizard Completed” is displayed. Click **Finish**.
    Automatically the DAP Configurator is started, which allows you to configure your IP DECT system.


DAP Controller - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed DAP Controller. Click Finish to exit the wizard.
Launch DAP Configurator
< Back
Finish
Cancel

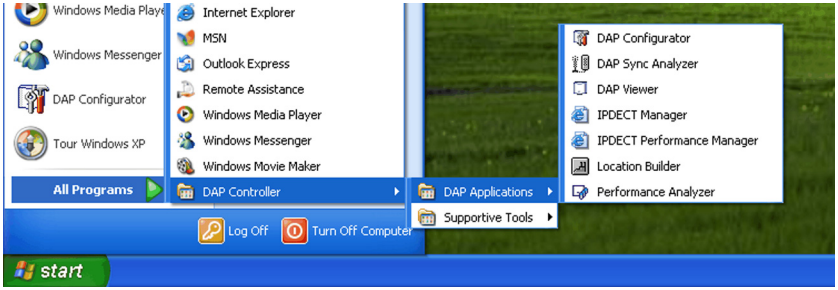
8. CONFIGURATION - DAP CONFIGURATOR TOOL

8.1. General

The DAP Configurator is an tool for creating the configurations files for the DAP Manager and DAPs. It is automatically installed when you install the DAP Controller/Manager. It is also automatically started up during the installation of the DAP Controller/Manager.

After you went through the DAP Configurator windows and you have entered the correct data, a number of configuration files are created.

You can always start-up the DAP Configurator tool using the shortcut to the DAP configurator tool in the "Programs" menu. See screen capture below.



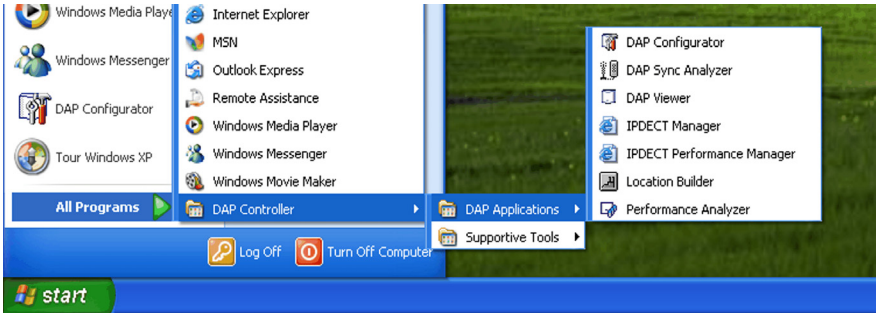
8.2. Using the DAP configurator

PROCEDURE: Setting up the Configuration

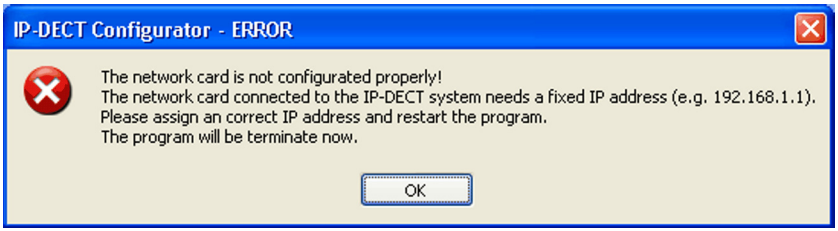
Actions

1. Make sure that the installation of the DAP Manager was successfully executed. If you selected to start the DAP Configurator automatically after the installation, continue with step 3 in this procedure. If not, continue with the next step in this procedure.

2. Start the DAP configurator tool, via **Start**, **All programs**, **DAP Controller**, **DAP Applications**, **DAP configurator**.



3. If you did not assign a fixed IP address to your network card, you will see the following message. This means that you have to assign a fixed IP Address to the network card in your DAP Manager PC. If you do not see this message, continue with the next step in this procedure.



4. If you start-up the DAP Configurator for the first time, you will see the following window displayed.

Note that there are three sections in this window:

- *System Control* section at the left side.
- *Settings Buttons* at the top part of the window.
- *Data information* part in the middle of the window.

If you start-up the DAP Configurator after configuring a system, you will see one or more extra buttons highlighted.

Note: *The way the buttons are greyed out, may be different in your system.*

5. In the System Control section (left side) click the button that is applicable to your need.

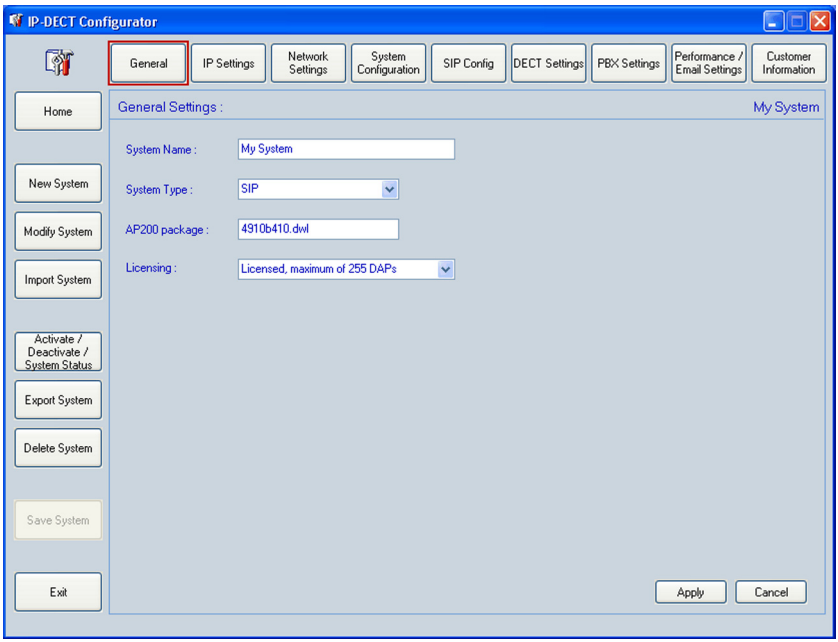
For a new installation it will be **New System**.

Note: *If you don't want to start a new system installation, consult Section 8.3. "System Control Section" for more information on the buttons.*

Note: *If you want to change system settings, you must use the buttons in the top part of the window. These buttons are described in Section 8.5. "Settings Buttons".*

6. Continue with the section that is applicable for your situation.

Note: *The following two sections, Section 8.3. "System Control Section" and Section 8.4. "Single Site / Multi Site" contains important information, however, the configuration procedure continues in Section 8.5. "Settings Buttons".*



8.3. System Control Section

8.3.1. General

The System Control section is located at the left side of the IP DECT Configuator window.

Using one PC, you can manage more than one IP DECT system. For such an IP DECT system you must setup a configuration on you PC. For each individual system, you can change settings, using the buttons in the top part of the window. However, you can have only one IP DECT system configuration active at the time. Therefore, you can start or stop an IP DECT system.

Note: *When you "Stop" an IP DECT system, the DAPs remain up-and-running. This means that you can still make and receive phone calls. However, the DAP Controller/Manager function is stopped, which means that some functionality (e.g. messaging or moving between Branch Offices) does not work anymore.*

The System Control part consists of the following buttons:

- **Home**
  Brings you back to the "start" screen.

- **New System**
  Allows you to create a new system configuration on your PC.

- **Modify System**
  Allows you to Select a system configuration, and then manipulate or modify the system.

- **Import System**
  Allows you to import a system configuration that has previously been exported. You can import individual files from the exported `.zip` file or you can import the exported `.zip` file in one go.

- **Activate - Deactivate - System Status**
  The system status button leads you to a window in which you can control the system status. See Section 8.3.2. "System Status Window". Note that you must select a System (configuration) first, using the "Modify System" button.

- **Export System**
  Allows you to export a system configuration. The exported file is always a `.zip` file and contains all relevant system configuration files, including subscription data, DAP configuration, DHCP data etc. The generated file can be imported later or can e imported on another PC that you want to use as DAP Controller/Manager PC. Note that this file can

be used as a backup of your entire system configuration. Note that you must select a System (configuration) first, using the "Modify System" button.

- **Delete System**
  This removes a System (configuration) from your PC. Note that you must select a System (configuration) first, using the "Modify System" button.

- **Save System**
  This saves the changes that you have made on a System (configuration) to files on your PC. Note that after you saved the System (configuration), you can go to the System Status button and then make the system active.

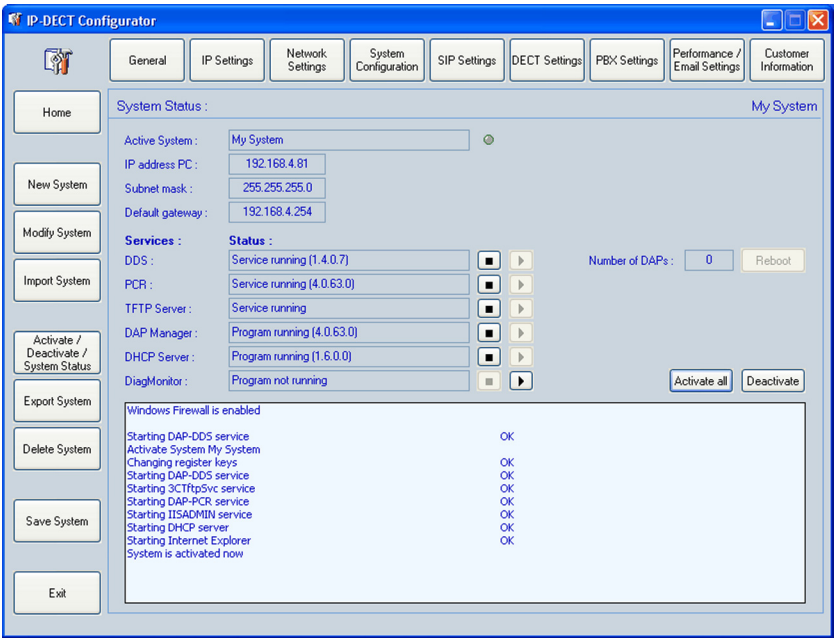
8.3.2. System Status Window

The window below is displayed when you click the "System Status" button. Note that when you have more than one IP DECT system (configuration) you must selected a System first, using the "Modify System" button. and that you have saved your new configuration before starting it.

Note: *Make sure that you have stopped a previously running system.*

Note: *If you have made a new configuration, or if you have changes configuration settings, make sure that you have saved the configuration first, using the "Save System" button.*

Note: *Starting or stpping the system, only starts o stops the services and applications running on the DAP Manager PC. This means that the DAPs remain operational. Basic call handling is still possible if the DAPs are up and running.*



The following services can be started or stopped:

- **DDS**
  DDS (DECT Data Server) takes care of all DECT processes to and from the DAPs.

- **PCR**
  PCR (Performance Counter Retrieval) must be running to retrieve performance data files and to enable sending an e-mail when performace thresholds are exceeded or when a DAP goes down.

- **TFTP**
  The TFTP Service refers to the TFTP server that was automatically installed with the DAP Controller/Manager software.. Note that this is not the MS Windows TFTP server. A TFTP Server must be running when one or more DAPs startup. The TFTP server supplies the DAPcfg.txt configuration file to the DAP(s). Note that there can be only one TFTP server running on your PC. If you start the TFTP service make sure that there is no other TFTP server running on your PC.

- **DAP Manager**
  Starts up the WEB service for IP DECT in IIS and opens the WEB Page of the DAP Manager in Internet Explorer.

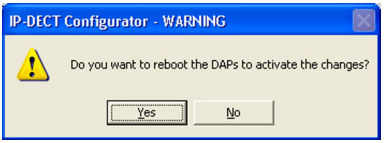
The following *programs* can be started or stopped:

- **DHCP**
  The DHCP server runs as an application. It can be started or stopped. Make sure that you are allowed to use a DHCP server on the Network .

- **DiagMonitor**
  The DiagMonitor is used to collect diagnostics data.

In addition to the services and applications on the PC, you can also reboot the DAPs.

When you start a System, the IP DECT configurator asks you if you want to reboot the DAPs as well. Note that this can be necessary, because the configuration changes must be uploaded to the DAPs as well. This requires a reboot!



8.4. Single Site / Multi Site

If you use the DAP Manager PC to manage one IP DECT system only, you can create a single site system. If you want to use your DAP Manager PC to manage more than one IP DECT system you can setup the DAP Configurator to manage more than one site, “multi site”. You have made a selection during the installation, see Section 7.2. "Installing the DAP Manager".

However, if you want to change the single site or multi site setting, execute the following precedure:

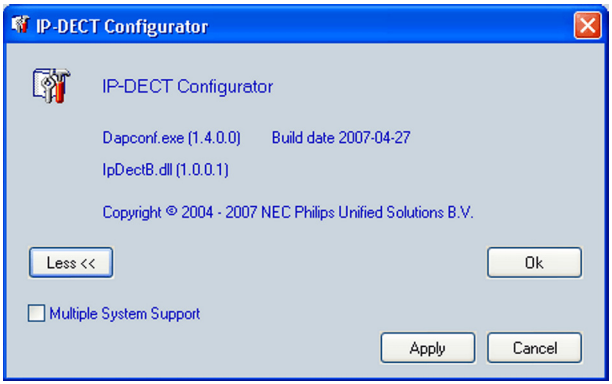
PROCEDURE: Switching between Single Site and Multi Site

Actions

1. Make sure that the IP DECT Configurator is open. If not open the IP DECT configurator/ DAP Configurator. See Section 8.2. "Using the DAP configurator".

2. Left mouse clikc the top left IP DECT configurator icon. See icon below.

3. In the window that is opened, click **More**. You should see the window below.



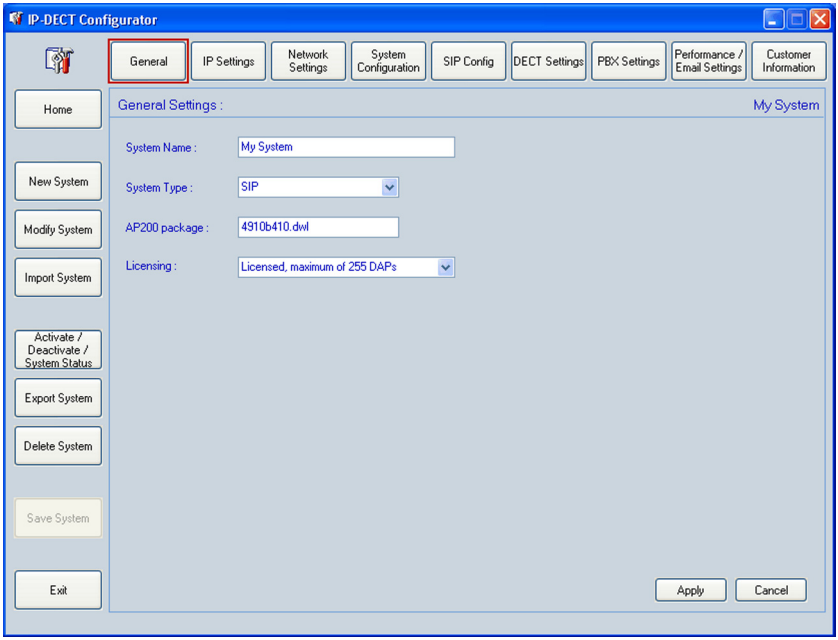
4. You can switch to "Multiple system Support" or "Single System" by means of the check box in the window. Click **Apply** or **OK** to activate your selection.

8.5. 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.

8.5.1. "General"

When you click the "General" the following window is displayed:



The following items must be entered:

- **System Name**
  Can be any given name. Note that this name will be used for a directory on the hard disk. This means that the name must comply with the requirements for Windows directory names.

- **System Type**
  Select the platform to which the IP DECT system is (going to be) connected. In this case it will be "SIP".

- **AP200 Package**
  Here you must enter the firmware file specification for the firmware package for the AP200. For SIP, the file name should look like this: `4910bxyz.dwl` (e.g. `4910b410.dwl`).

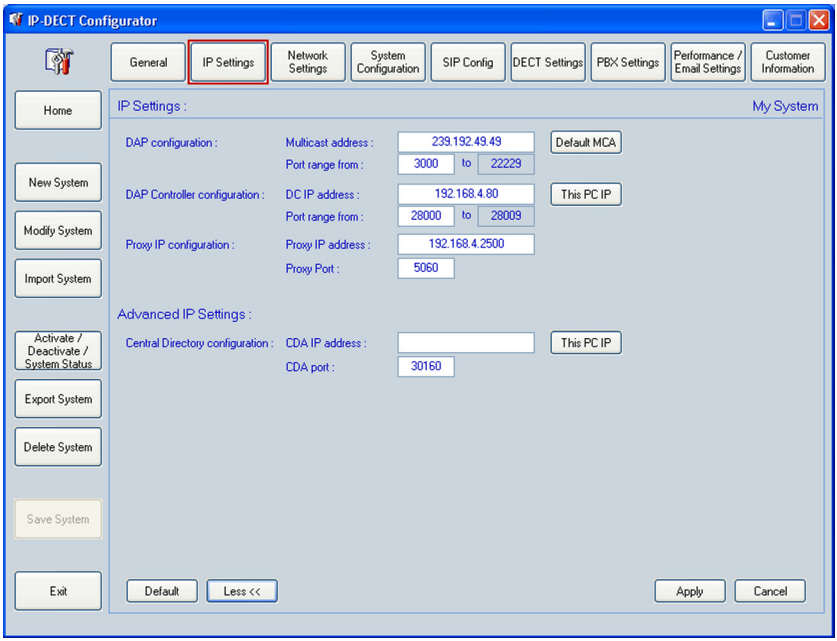
- **Licensing**

Select the license type that is applicable for your system. When you are using IP DECT with SIP interface and you have only AP200S type of DAPs, you must select “Unlicensed”. If you have an IP DECT System with SIP interface and AP200 DAPs, you must select “Licensed, max. 255 DAPs”.

When finished, click “Apply” and continue with clicking button “IP Settings”.

8.5.2. “IP Settings”

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



The following items can be configured:

- **DAP Configuration**
  - **Multicast IP 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.

- **Port Range from:**
  By default the port range on the DAPs will start at port 3000. However, you can change the start port address.

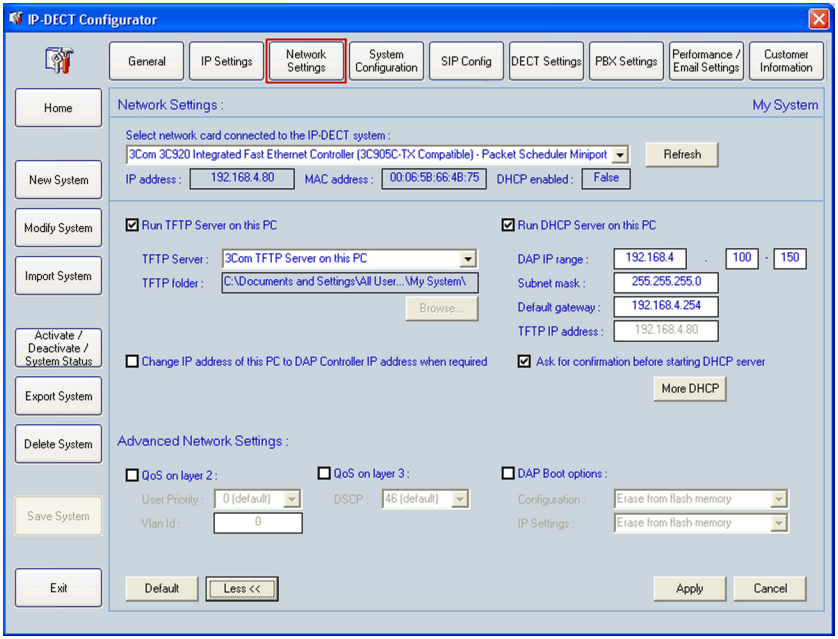
- **DAP Controller Configuration**
  - **DC IP Address**
    DAP Controller/Manager PC IP address. You can easily click the button "This PC IP" to copy the IP address of your PC into this field.
  - **Port range from**
    Start of port range in use for IP DECT on the DAP Controller/Manager PC.

- **Proxy IP configuration**
  - **Proxy IP Address**
    PBX IP address.
  - **Proxy Port**
    SIP port on the Proxy server. The default port is 5060.

- **Advanced IP Settings**
  You will have access to the advanced IP Settings, if you click the "**More**" button
  - **Central Directory - CDA IP Address**
    The IP address of the Central Directory Server (if applicable)
  - **Central Directory - CDA port**
    Port number on the Central Directory server. Default port number is 30160.

8.5.3. "Network Settings"

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



The following items can be entered/changed:

- **Select Network card connected to the IP-DECT System**
  If your PC has more than one network card, select the network card that is connected to your IP DECT configuration.

- **IP Address**
  Actual IP address on the network card.

- **MAC Address**
  MAC address on the network card

- **DHCP enabled**
  Indicates if the network card should receive its IP settings from a DHCP server or not.

- **Run TFTP Server on this machine**

If this box is checked, a TFTP Server will be running on your PC as “Service”.
The settings for the TFTP Server are automatically set correct for your configuration.
Note that a TFTP Server is needed when a DAP starts up, unless the configuration file is stored in the DAP.

- **TFTP Server**
  Select the TFTP Server that you want to use for the IP DECT Configuration.
  If you select the “3Com Tftp Server on this PC” it enables the TFTP server that is part of the DAP Controller/Manager software package. When enabled, it runs as “Service” under MS Windows. The settings are stored in the file `3CTftpSvc.ini`

- **TFTP Folder**
  Automatically filled in. The TFTP folder is the folder where all system information is stored. Default folder is: `C:\Documents and Settings\All Users\Application data\Philips\DAP Controller\<system name>`

- **Change IP address of this PC to DAP Controller IP address when required.**
  If this box is checked, the IP address of your network card is autoamtically changed to the DAP Controller IP address that you have specified in Sub-section 8.5.2. ""“IP Settings”"

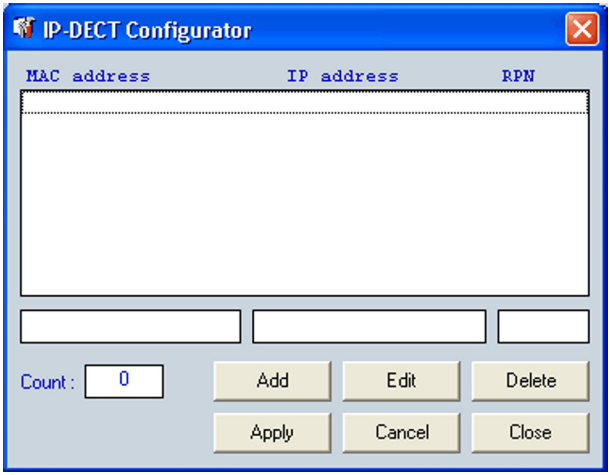
- **Run DHCP Server on this PC**
  If you check this box, the DHCP Server that is installed on your PC for IP DECT will be activated. Note that this DHCP Server accepts DHCP requests from DAPs only. It will ignore other DHCP requests. When you use the DHCP Server it will issue addresses in the range that you specify in the “DAP IP Range”.
  When enabled, it runs as an Application under MS Windows. The settings are stored in the file `dhcpsrv.ini`
  The following items can be set:
  - **DAP IP Range**
    Specify IP address range that will be issued to the DAPs.
  - **Subnet Mask**
  - **Default Gateway**
  - **TFTP IP Address**
    This is the IP address where a DAP can find the TFTP Server.

Note: *The builtin DHCP server responds to DAP requests only. Requests from other network hosts are ignored. The issued lease time is “unlimited”.*

- **Ask for confirmation before starting the DHCP Server**
  Self explaining.

- **More DHCP**

This opens the user interface of the DHCP server. See following screen capture.



In this window, you can delete/change/add the releationship between MAC addresses and IP addresses.

- **Advanced Network Settings**
  - **QoS on Layer 2**
    Here you can enable Quality of Service on Layer 2. If enabled, you must specify the Priority level for Layer 2 (IEEE802.1p) and the VLAN ID (IEEE802.1Q). The Priority value is a three bit value which must be entered as decimal value 0 ... 7, where 7 is the highest priority.
  - **QoS on Layer 3**
    Here you can enable Quality of Service on Layer 3. If enabled, you must specify the DiffServCodePoint (DSCP) value in decimal, in the range 0 ... 63. Note that this is not the AF (Assured Forwarding) class selector/service level or EF (Expedited Forwarding) class selector/service level. This means that if you want to apply the “EF” class selector/service level (53), you should enter the DSCP decimal value “46” (binary 101110).
  - **DAP Boot options**
    This allows you to store the IP address data and Configuration data into Flash memory in the DAP. When stored, a DAP does not need a DHCP/TFTP server anymore. Note that you can “Store” or “Erase” data. Also note that you can store/erase IP address

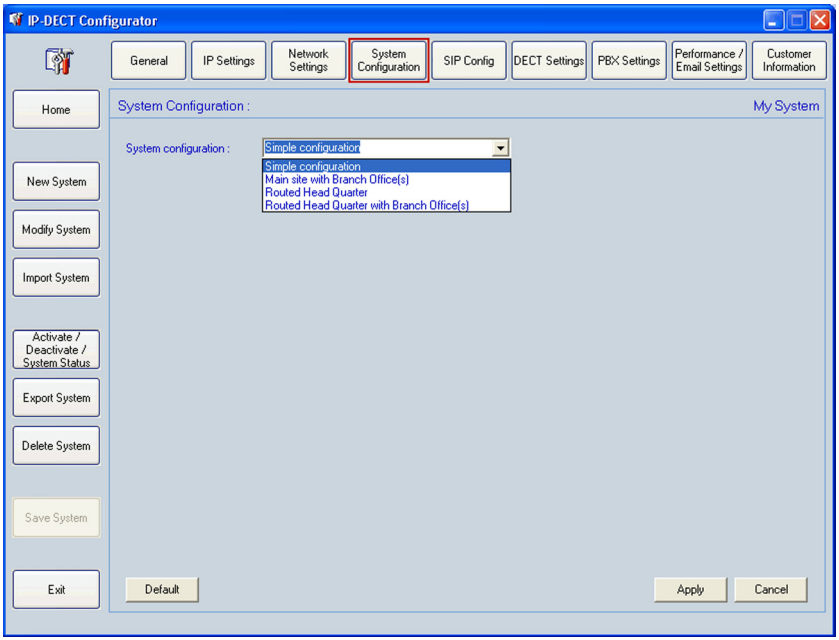
data and/or configuration data.

Note: *Data is stored when you have selected to store data AND when the DHCP server issues an "Infinite" lease time.*

When finished, click "Apply" and continue with clicking button "IP Settings".

8.5.4. "System Configuration"

When you click the "System Configuration" button, the following window is displayed:

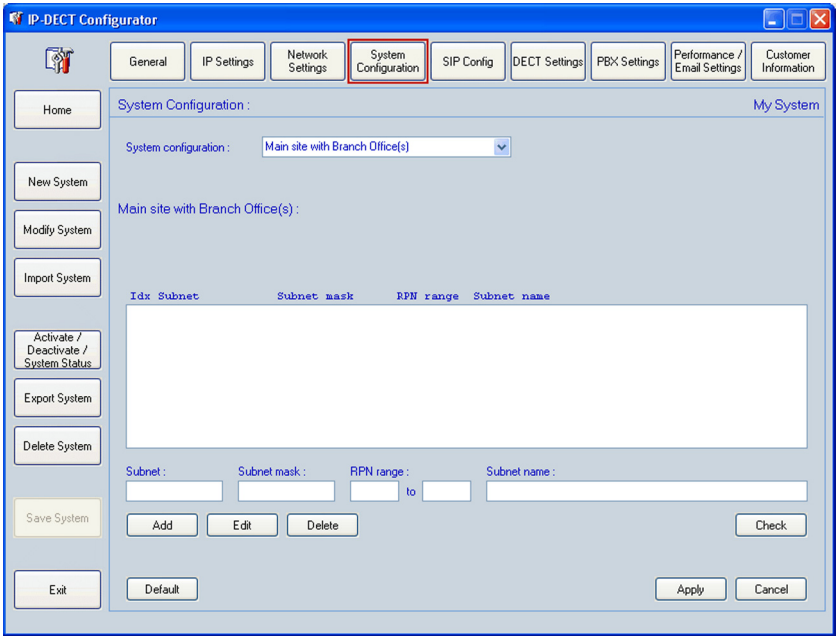


You can select the type of system that you want to use. Consult 3. "NETWORK CONFIGURATIONS" for more information.

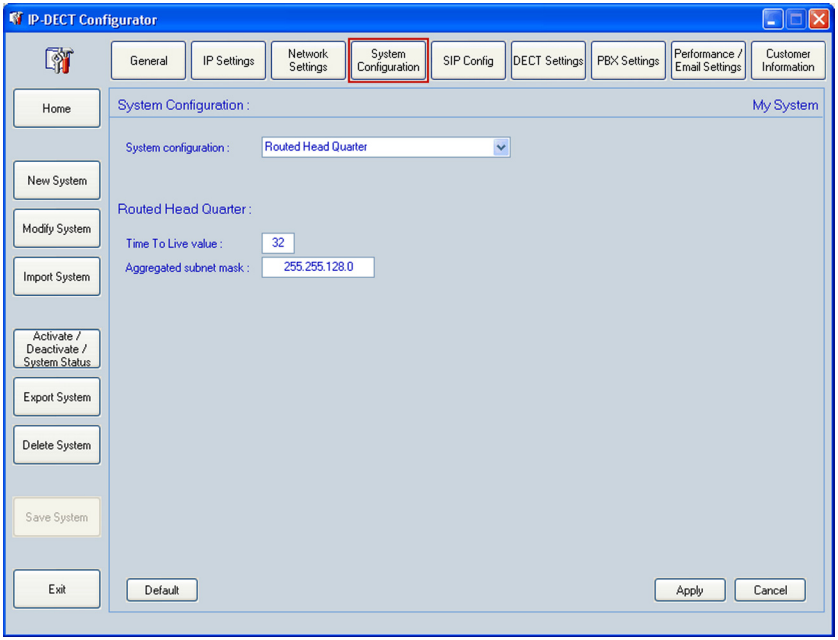
The following options are available:

- **Simple Configuration**
  A simple congfiguration consists of one network segment. All IP DECT components are in that segment, including the PBX.

- **Main side with Branch Office(s)**
  This configuration consists of a Main side as one network segment. The PBX is in the Main side. Beside the Main side, there are Branch Offices. The Branch Offices are in one or more different network segments as the Main side.
  The window "Main site with Branch Office(s)" offers the possibility to specify a certain RPN range per Branch Office Subnet. Note that if you do not specify a range per Branch Office, the DAP Controller/Manager assigns RPN number automatically but there is no arrangement in it. Therefore it is strongly recommended to specify a range per Branch Office. Note that you should set the RPN range wide enough to allow future system expansion. if you expect system expansion, it is strongly recommended to specify the RPN ranges according to the expected system expansion.
  The following items can be specified:
  - **Subnet**
    This is the subnet address. It is the first address in the subnet range, e.g. 192.168.4.0.
  - **Subnet mask**
    Mask to specify the subnet boundaries.
  - **RPN range**
    Lowest RPN and highest RPN in this Branch Office.
  - **Subnet name**
    Can be any given name. It is used to identify the Branch Office.



- **Routed Head Quarter**
  In this configuration, there are more than one network segments in the Head Quarter. The routers in this configuration must forward IP Multicast packages.

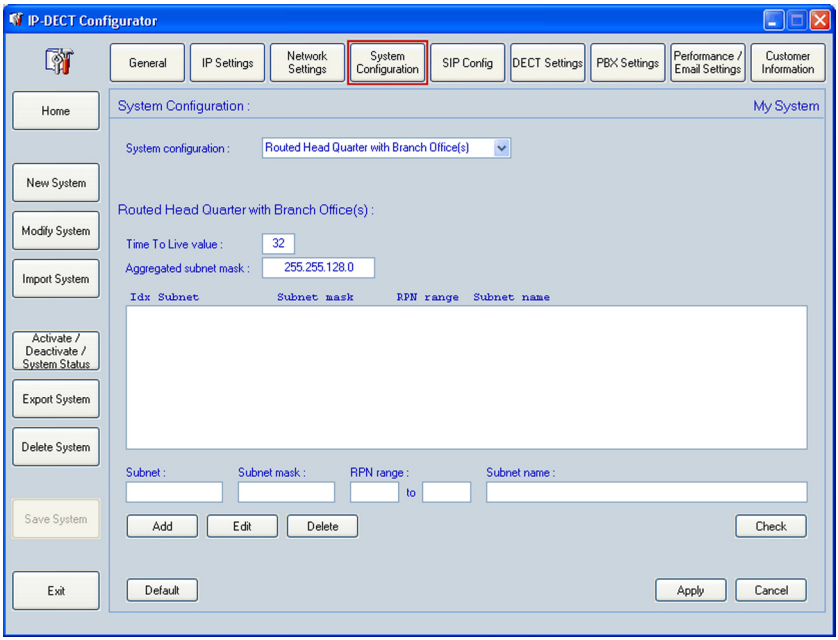


The following settings can be entered/changed:

- **Time to Live value**
  The Time to Live value is used for the Multicast traffic. If the Time to Live for the Multicast is set to "1", multicast traffic will not be forwarded by a Router. If the Time to Live is higher than "1", multicast packages might be forwarded by the Router, depending on settings in the Router. If the "Time To Live (TTL)" (for the multicast packages) in the field below is set to "1" you must leave this "Agg. subnet mask" empty. If the "Time To Live (TTL)" (for the multicast packages) in the field below is set to a value higher than 1, you must fill in this "Agg. subnet mask" to tell the system which smaller subnets are connected together as one subnet via a router supporting IP multicast.
- **Aggregated Subnet mask**
  The "Agg. subnet mask" is the subnet mask for the DAPs to determine the network boundaries for an IP DECT Network in which seamless handover is possible and G.711 should be used. It should cover the network segments that are connected together using routers that supports IP Multicast. If there are DAPs outside this Aggregated Subnet Mask, the DAP(s) is/are regarded as in a Branch Office. Note that

the IP address of the PBX is compared with the IP address(es) of the DAP(s) using this subnet mask. If in different subnets according to this mask, the DAP(s) is/are supposed to be in a Branch Office. If the IP addresses are in the same Aggregated Subnet, according to this mask, the system assumes that they are in the same subnet. The term "Aggregated" means that the subnet consists of smaller subnets which are connected over a router, but according to the subnet mask, all behaving as one subnet. This is applicable for the "Routed Head Quarter" network solution either with or without Branch Offices, see Section 3.4. "Routed Head Quarter" and Section 3.5. "Routed Head Quarter with Branch Offices".

- **Routed Head Quarter with Branch Offices**
  Routed Head Quarter is a combination of the Routed Head Quarter and a Branch Office configuration.

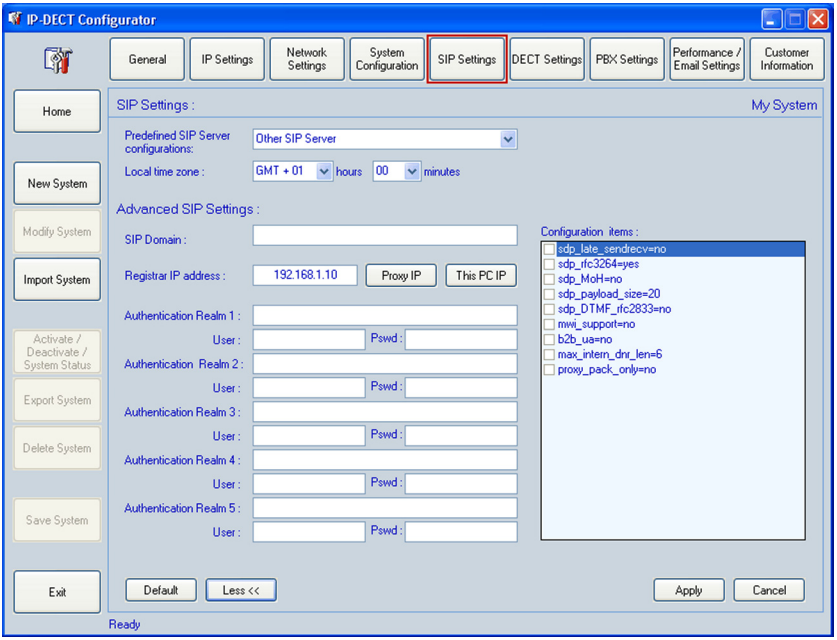


For the settings, consult the sublist in the previous bullet.

When finished, click "Apply" and continue with clicking button "IP Settings".

8.5.5. "SIP Configuration"

When you click the "SIP Configuration" button, the following window is displayed:



The following items can be entered or changed.

The window shows three panes with parameters that can be filled in or changed.

- SIP configuration.
- SIP Advanced SIP settings for Realm authentication.
- SIP Server specific Configuration Items

Note: *This window does not show a field for the SIP Proxy address. The SIP Proxy IP address must be specified in the "IP Configuration" window.*

In the following bullet list, with hyphenated sublist, the parameters are explained.

- **SIP Settings**
  - **SIP Domain**

Here you must specify the Registrar IP Address (IP4, dotted format) or host name. Note that if you do not specify an address here, the value of "Proxy IP address or host name" is used.

- **Local time zone**
  Specify your time zone. Normally this setting is OK. You only need to change this setting if you want to deviate from the Windows time zone settings.
- **SIP Server**
  Select your SIP Server type.

- **Advanced SIP Settings**
  - **Registrar IP Address**
    IP address of the Registrar server.
  - **Realm for user1** . . . **Realm for user5**
    Up to 5 authentication realms can be specified. Note that if the Proxy requests for authentication, it issues the realm name. On receiving the Realm name, the IP DECT system compares the received Realm name with the ones in this list. If the Realm name matches, the "username" and the "Password" are sent to the Registrar for authentication check.
  - **Username**
    The username is the name for login on the Proxy/Registrar server.
    Note that you can fill in an actual username OR a `%s` . When you enter `%s` , the IP DECT system sends the extension number of the handset making a call. This makes the username extension specific. (Some SIP Proxies/Registrar servers requires the extension number as username.that the username is the subscribed number is sent as username).
  - **Password**
    Password for authentication in the Proxy/Registrar.

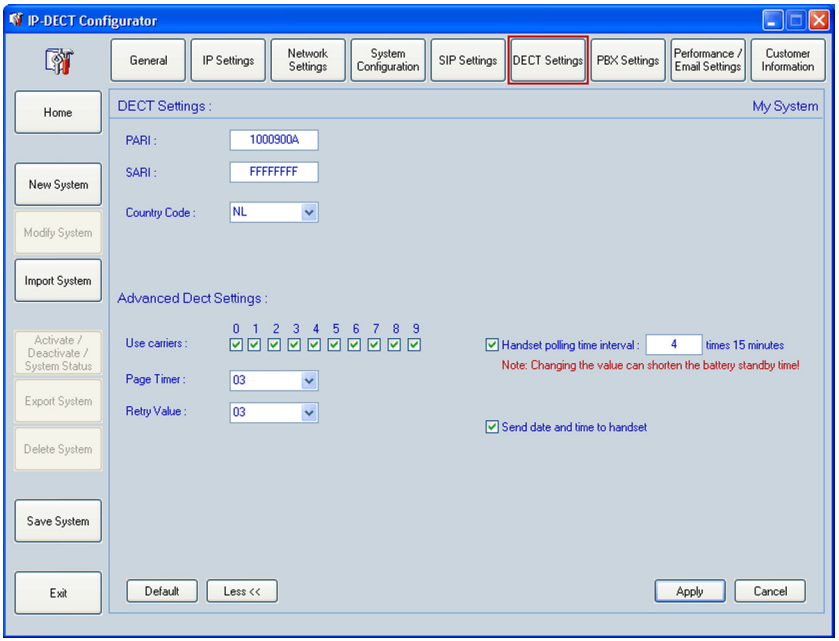
- **Configuration Items**
  - **Proxy_pack_only**
    If "checked" the DAP accepts packets from the SIP Proxy only. (E.g this means that packets from a Redirect server are not accepted.) Note that it even does not accept packets coming from another Proxy then the one specified in the DAP Configurator.
  - **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_MoH**
    When enabled, no local tone is generated when the IP DECT handset is on "hold" (recvonly mode).

- **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.
- **b2b_ua**
  Back-to-Back User Agent. Necessary for an un-attended transfer in an iS3000 SIP server configuration. Must be set to "yes" for iS3000. Must be set to no in all other cases.
- **max_int_dnr_length**
  Extension numbers longer than specified here are considered as external numbers. Note that this only applies to numeric extension numbers.

When finished, click "Apply" and continue with clicking button "DECT Settings".

8.5.6. "DECT Settings"

When you click the "DECT Settings" button, the following window is displayed:



The following options can be set/changed:

- **DECT Settings**
  - **Pari**
    Primary Access Rights Identifier. This is the Unique DECT System Identifier. It is a 8 digit hexadecimal string. It is a worldwide Unique Identifier which you should have received together with your DECT system.
  - **Sari**
    The SARI is the Secondary Access Rights Identifier, which is only needed if you use Multi-Site subscriptions. If you do not use multi-site Subscriptions, leave this field to the default "FFFFFFFF".
  - **Country Code**
    The Country code specifies the tone plan for IP DECT.

- **Advanced DECT Settings**
  - **Used carriers**
    By means of this field you can enable/disable the DECT carriers. Leave all carriers

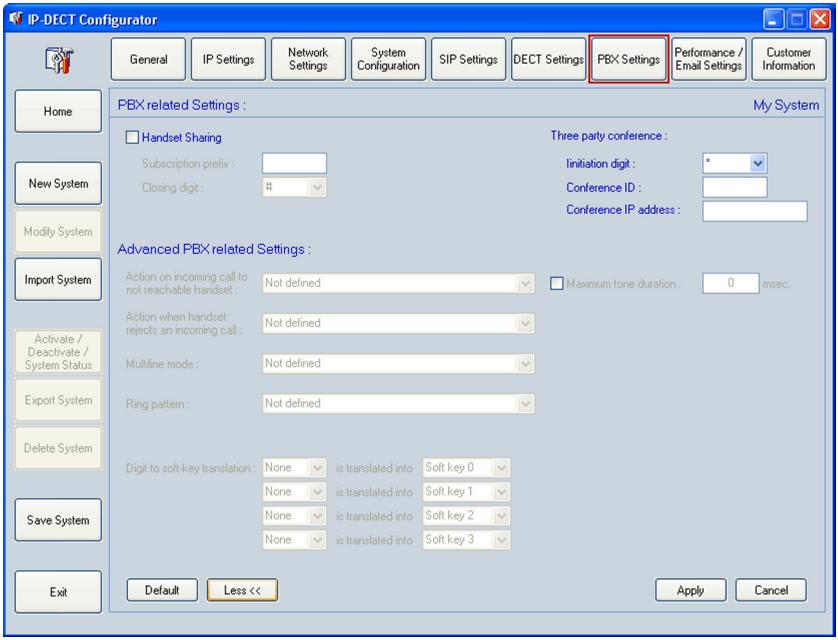
enabled to make sure maximum bandwidth is available.

- **Page Timer**
  The Page Timer specifies the time in seconds between two page requests (retries).
- **Retry Value**
  The Page Retry Value specifies the maximum number of paging retries that are issued, if paging a handset fails.
- **Handset Polling Time Interval**
  Handsets are polled with an interval of 15 minutes, to detect if they are still reachable. This is done with a polling counter. If the handset does not respond to the polling after the specified counter value, IP DECT issues a Logout to the PBX. The default time is 15 minutes. The counter value can be specified in this field.
- **China frequency**
  Enable DECT frequency range for China.
- **Send date and time to portable**

When finished, click "Apply" and continue with clicking button "PBX Settings".

8.5.7. "PBX Settings"

When you click the "PBX Settings" button, the following window is displayed:



The following items can be set/changed:

- **Handset sharing**
  Checking this box, enables Portable sharing, see Chapter 11. "PORTABLE SHARING"
  - **Subscription prefix**
    First digit(s) of the subscribed number. If the first digit(s) of a subscription matches with the digit(s) defined here, the handset is enabled for portable sharing.
  - **Closing digit**
    Digit that must be entered on the handset after entering the extension number at login. Default is "#". Normally there is no need to change this digit.

- **Three party conference**
  - **Initiation digit**
    Digit that must be dialled to start the three party conference.
  - **Conference ID**
    The unique ID for the conference.
  - **Conference IP Address**

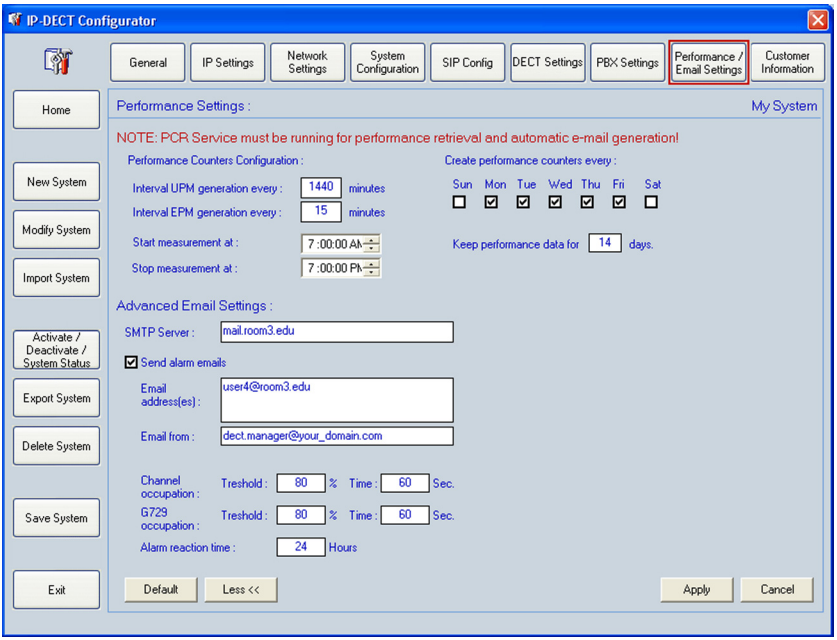
The IP address of the Conference server. (Used for RTP Speech path.)

- **Advanced PBX Related settings**
  There is only one option available in an IP DECT system with SIP connectivity. The grayed out options are applicable for non-SIP PBX types.
  - **Action when handset rejects an incoming call.**
    Select the prefered action in case the handset rejects an incoming call.

When finished, click "Apply" and continue with clicking button "Performance / Email Settings".

8.5.8. "Performance / Email Settings"

When you click the "Performance / Email Settings" button, the following window is displayed:



There are two panes in this window with parameter settings.

- **Performance Settings**

- **Interval UPM generation every:**
  With this interval, User Performance Measurement files are generated. Default value is 1440 minutes (one day)
- **Interval EPM generation every:**
  With this interval, Equipment Performance Measurement files are generated. Default value is 15 minutes.
- **Start measurement at:**
  Each day performance measurement should take place, the performance measurement will start at the time specified here.
- **Stop measurement at:**
  Each day performance measurement should take place, the performance measurement will stop at the time specified here.
- **Create Performance counters every:**
  Specify the days that performance counter retrieval should take place.
- **Keep Performance data for . . . days**
  Number of days that the performance data should be kept on the Hard Disk.

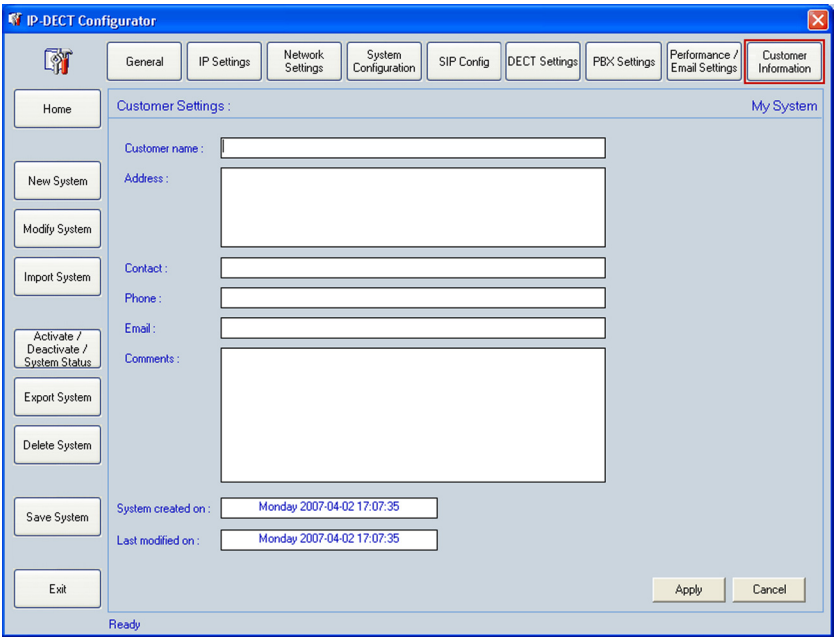
• **Advanced Email Settings**
  Emails can be send automatically when a DAP goes down or when the channel occupation threshold is exceeded for more than a number of seconds. Note that this will only work when the DAP Controller/Manager is up-and-running. The PCR service must be running on the DAP Controller/Manager PC.
  - **SMTP Server**
    Enter the DNS name or the IP address of the SMTP mail server.
  - **Send alarm emails**
    This check box enables sending emails.
  - **Email addresses:**
    Enter the destination email address(es). Note that you can enter more than one email address.
  - **Email from:**
    Enter the originators email address. Note that normally the SMTP server does not check the originators email address, which means that you can enter any email address here.
  - **Channel Occupation**
    Here you define the conditions for generating an email on DAP channel occupation.
  - **G729 occupation**
    Here you define the conditions for generating an email on G.729 channel occupation.
  - **Threshold / Time**
    If the channel occupation is higher than this percentage of the available channels for a specified time period, an email is generated. The threshold is specified in percentage, the time is specified in minutes.

- **Alarm reaction time**
  Time interval for sending emails. Default 24 hours, which means that the time interval between two emails will be 24 hours. Note that this is not a repetition timer. Once an email is send, it will not be repeated anymore.

When finished, click “Apply” and continue with clicking button “Customer Information”.

8.5.9. “Customer Information”

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



In this window, you can enter customer information. It is only for administrative purposes. The system does not use this information.

When finished, click “Apply”. Continue with Subsection 8.5.10. "Save System and Start System"

8.5.10. Save System and Start System

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

Note: *If you use another TFTP server or DHCP server than the build in TFTP/DHCP server, consult Chapter 9. "USING OTHER TFTP SERVER" first.*

1. Click the **Save System** button, to save the changes you have made.
2. Copy the firmware file `4910bvxx.dwl` into the TFTP directory. This will normally be the following directory: `C:\Documents and Settings\All Users\Application Data\Philips\DAP Controller\<customer name>\`
3. Activate the system, using the **Activate** / **Deactivate** / **System Button**.
4. Check the System Status in the System Status Window.
5. Check that the DAPs become operational.

For more information, see section 8.3. "System Control Section"

8.6. Finishing Advice

When the system is running correctly, generate a `visadm.txt` file and analyse the file, using the SyncAnalyser tool, see Chapter 16. "MAINTENANCE TOOLING - SYNC. ANALYZER".

If necessary, re-arange the synchronization structure.

9. USING OTHER TFTP SERVER

9.1. General

The previous sections assume that you are using the built in TFTP Server in the DAP Controller/Manager Software. That is the easiest way because pathes etc. are automatically set correct. However, if you have chosen to use another TFTP server, pathes must be set correct and files needs to be copied into the TFTP root directory. Consult the following section.

9.2. Prepare files for TFTP Upload to DAPs

The DAPs will only become operational if they can load the required files via TFTP. This requires that the DHCP server and the TFTP server are up-and-running with the correct configuration and it requires that the files for the DAP are available in the TFTP directory.

PROCEDURE: Copying files to the TFTP directory

Actions

1. Determine which TFTP Server you are using. There are four options:
   - 3com TFTP Server on this PC.
   - Windows TFTP Server on this PC.
   - Other TFTP Server on this PC.
   - Other TFTP Server running on other PC.

2. In the following steps you must copy the firmware file (and configuration file) to the upload directory of the TFTP Server. Therefore, you must know the path settings of the TFPT Server that you are using. In the following table an overview is given of the TFTP Servers and the path settings.

TFTP Server	Default Path	Preferred Path
3com	C:\Documents and Settings\All Users\Application Data\Philips\DAP Controller\<customer name>\	C:\Documents and Settings\All Users\Application Data\Philips\DAP Controller\<customer name>\
Windows	C:\tftpdroot\	C:\tftpdroot\
Other	unknown	C:\Documents and Settings\All Users\Application Data\Philips\DAP Controller\<customer name>\
Other on other PC	unknown	unknown

Table 9-1 Overview of TFTP Servers.

The two files that needs to be in the TFTP directory are:

- Firmware file: `4910bvxx.dwl` (the one that you have specified in Section 8.2. "Using the DAP configurator".
- The configuration file: `dapcfg.txt`.

Copy the firmware file to the TFTP directory of the TFTP Server that you are using.
If you are using the 3com TFTP server that came with the IP DECT installation (default!) the default path equals the preferred path.

3. The `dapcfg.txt` file is by default stored in the directory: `C:\Documents and Settings\All Users\Application Data\Philips\DAP Controller\<customer name>\`. This is the default directory for the "3com TFTP" server that came with the installation of the IP DECT system. If you are using the "3com TFTP" server, no manual action is needed anymore. However, if you are using an other TFTP server, copy the `dapcfg.txt` from the directory `C:\Documents and Settings\All Users\Application Data\Philips\DAP Controller\<customer name>\` to the TFTP directory that your TFTP Server is using as upload directory.

4. Make sure that the option "Next Boot Server" in the DHCP Server that you are using, points to the IP address of the PC where your TFTP Server is running.

5. The DAPs should be able to start-up now.

10. OPENING DAP MANAGER WEB INTERFACE

You can open the DAP Manager window using Internet Explorer 6.0 or higher.

PROCEDURE: Opening the DAP Manager WEB Interface

Actions

1. Open the MS Internet Explorer WEB browser on your DAP Controller/Manager PC. Enter an URL that points to the `/CDS/` directory/file on the DAP Controller/Manager PC. (e.g. `http://127.0.0.1/CDS/`)
   It is also possible to open the WEB interface from another PC in the network. However, you must know the right path. This could be e.g. `http://192.168.4.80/CDS/`, where "192.168.4.80" is the IP address of the DAP Controller/Manager PC.

2. Now, you should see the "DECT Manager" main screen. If not, then check if your IIS is running on the DAP Controller/Manager PC. Also check if the `default.aspx` file is present in the `C:\Inetpub\wwwroot\CDS` directory.

3. If you have a licensed configuration with AP200 (without the suffix "S"), assign licenses to your IP DECT system via the DECT Manager interface.

Note: *The DECT Manager interface is described in the IP DECT DECT Manager Administrator Guide.*

4. Enter the extension number range via the DECT Manager interface.

5. Check that the DAPs are operational.

6. Subscribe the handsets. Check that you can make phone calls.

11. PORTABLE SHARING

11.1. What it is

Portable Sharing allows the user to give the portable (handset) an extension number via a "login" procedure.

When a portable is enabled for Portable Sharing, you will get a "Login" message when you go off hook after one of the following conditions:

- after the handset was subscribed.
- after the handset was switched on.
- after the handset was taken from the charger with silent charging switched on.

In this "login" mode, you must enter the extension number that you want to activate for the handset. This extension number must already be present in the SIP Proxy. After you entered the extension number, you must terminate the login with a closing digit. By default, "#" is the closing digit. However, this can be changed. After entering the closing digit, the handset is active for the extension number that you have entered. Only after a "logout" the handset displays the "login" again.

How and when does a handset a Logout? A Logout is executed automatically, when the handset sends a "Detach" signal to the DECT System. Sending a "Detach" signal is done automatically at the following manual action:

- Switching off the handset
  The handset types C922, C933, C944, i600, C124, G355 and G955 send a "Detach" signal when they are within reach of the IP DECT system AND when the user switches off the handset!

- Putting the handset in charger with silent charging enabled.
  The handset type C933, C944, i600, C124, G355 and G955 send a "Detach" signal when they are within reach of the IP DECT system AND when the user puts the handset in the charger in silent charging mode.

Note: **-** *When a handset type C922, C933, C944, i600, C124, G355 or G955 goes out of range, no Detach signal is sent! Therefore "login" is not activated when the handset comes within range again.*

- *This Portable Sharing mechanism is supported for C922, C933, C944, i600, C124, G355 and G955 only. Depending on the type of handset, on other handsets, support*

of Portable Sharing is not available at all, or you can login only once because there is no "Detach" possible.

Portable Sharing is disabled by default for the IP DECT system, but can be switched on using the DAP Configurator.

When enabled, you must designate a certain number range in the subscription numbers that is used for Portable Sharing. The numbers in this range may NOT exist as extension numbers in the SIP Proxy. These number must start with the same "prefix". This prefix must be specified in the DAP Configurator and could be e.g. "00".

11.2. Portable Sharing and the DAP Manager

The DAP Manager PC is always needed for handling the Login information and for providing the login information to the DAPs (e.g. when a DAP restarts). This means that the DAP Manager should always be connected and should be up-and-running. However, it is not "Single point of failure", which means that if the DAP Manager is down, you can still make and receive calls.

The login information is stored in a file `dds-login.txt` on the harddisk of the DAP Manager PC.

12. MAINTENANCE AND DEBUGGING

12.1. DAP LED Indications

The DAP is equipped with one LED. The LED can indicate 6 different statuses of the DAP. The following indications may occur.

- **Off**
  No power.
- **0,5 seconds On - 0,5 seconds Off**
  Loading software/firmware.
- **Short flash every 0,25 seconds**
  IP Network error (not connected, no DHCP/TFTP server, no DAP Controller)
- **Fast blink**
  DAP operational, but trying to synchronize to another DAP.
- **Continuous fast blink**
  Hardware error.
- **Steady On**
  DAP operational (and synchronized to other DAP or is the synchronization master).

12.2. TCP/IP Tools

On TCP/IP level, the following common tools are available. Because these tools are commonly used, they are not described here in detail.

- Ethereal
  This software tool is a so called "sniffer" and is used to capture data on a TCP/IP link. It allows you to analyse the traffic on the TCP/IP link in detail.
- WinPrintF
  WinPrintF is a tool from NEC Philips Unified Solutions. It is available on the "Service CD-ROM". This tool allows you to see messages from the DAPs. The messages are available on port 2050 on each DAP.

13. SWITCHING BETWEEN SYSTEMS

13.1. General

When you use your DAP Controller/Manager PC to manage more than one IP DECT System, there is the need to be able to switch between systems. If you have chosen to setup your DAP Configurator in Multi Site mode (see Section 8.4. "Single Site / Multi Site") you can store more than one system configuration on your PC. However, if you have chosen to use your DAP Configurator in Single Site mode, it might be necessary to use the Export and Import feature to swap easily from one system configuration to another.

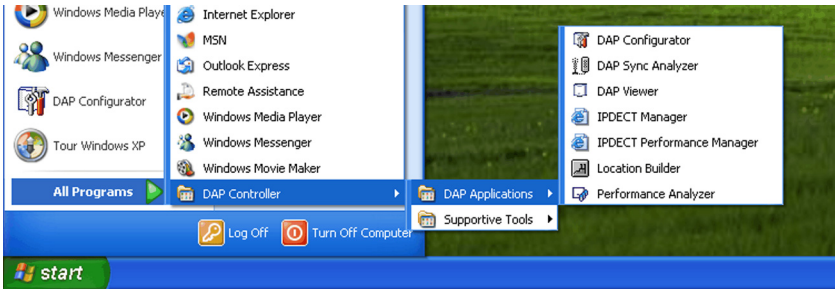
When you execute an "Export System", all the relevant system settings including all customer data are exported to a compressed (zip) file. If you want to return to this configuration you can easily import the compressed file and then your entire system configuration including customer data like handset subscriptions is back again on your DAP Controller/Manager PC.

13.2. Export System

PROCEDURE: Export a System Configuration

Actions

1. Start the DAP configurator tool, via **Start**, **All programs**, **DAP Controller**, **DAP Applications**, **DAP configurator**.



2. The following screen will be displayed.
   Click the button **Activate** / **Deactivate** / **System Status**. In the window that is displayed, clck the button **Deactivate**. Note that this doesn't bring the system down, the DAPs remain operational.

3. Wait till the system is deactivated. At the left hand side, click **Export System**.

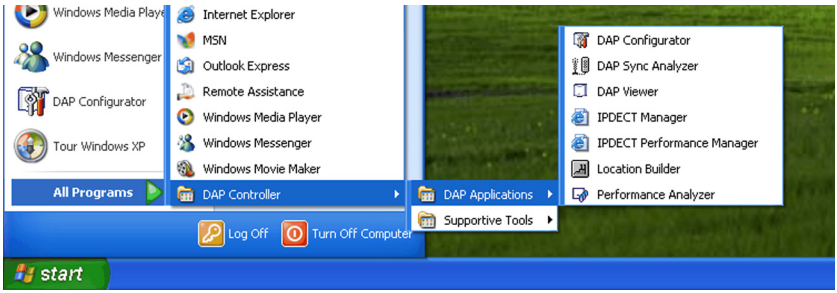
4. A window is opened which allows you to store the file on a location of your choice. You can specify a file name.

13.3. Import System

PROCEDURE: Import a System Configuration

Actions

1. Start the DAP configurator tool, via **Start**, **All programs**, **DAP Controller**, **DAP configurator**.



2. The following screen will be displayed.

3. Click **Import**.

Note: *The buttons highlighted in this window may differ in your system.*

4. Browse to the file that contains the system that you want to import. Note that you can import the exported "zip" file in one go, or you can import separate files form the exported zip file.

5. Finish the procedure, following the instructions on the screen.

14. REPLACING A DAP

14.1. General

When a DAP is broken, it needs to be replaced. However, there are two things that makes the DAP specific:

- Its RPN number. This means that the synchronization structure might change if the new DAP has a different RPN then the replaced DAP. To avoid this problem, you must use one of the two procedures, either in Section 14.2. "Replacing DAP, new DAP Available" or in Section 14.3. "Replacing DAP, no new DAP Available"
- The subscription records in a DAP. If you want to have the same subscription records in the new DAP, you must follow the procedure in Section 14.2. "Replacing DAP, new DAP Available". Note that when the DAP Manager is up-and-running, subscription records of the broken DAP will be automatically moved to other DAPs in the system. (For more info, see Sub-Section 2.3. "Automatic Distribution When DAP Down").

If a DAP is broken and the DAP Manager is not up-and-running, *the handsets that have their subscription records in the broken DAP are **not usable** anymore*. This means that immediate intervention is needed, even if you don't have a new DAP available. The procedure to follow is different for having a new DAP available or not. Therefore, there are two sections in this chapter describing the replacement procedure:

- Replacing a DAP with new DAP Available.
- Replacing a DAP without new DAP Available.

14.2. Replacing DAP, new DAP Available

To make sure that the newly installed DAP behaves in the same way as the replaced DAP, execute the following procedure for replacing a DAP.

PROCEDURE: Replacing a DAP

Actions

1. Before you start, make sure that the DAP Manager is up-and-running.

2. Also make sure that the DHCP server and the TFTP server are up-and-running in the IP network.

3. Open the DECT Manager WEB interface.

4. Click “Access Points”.

5. **Disconnect** the DAP that needs to be replaced! Do not continue this procedure until the DECT Manager indicates that the DAP is not “Working”.

6. Connect the new DAP. Wait until you see that the new DAP is up-and-running (in the DECT Manager interface).

7. Click the “Edit” button for the new DAP.

8. Change the RPN number of this DAP to the RPN number of the replaced DAP and click “OK”.

9. The new DAP will reboot. When the DAP is up-and-running again, it should have the RPN of the replaced DAP.
   Now the subscriptions that were active in the replaced DAP will be automatically installed in the new DAP. This can take a few minutes. Check that the the subscriptions of the replaced DAP are on the new DAP.

Note: *After the subscription records are placed in the new DAP, switch the handsets associated with these records, off and on, to make them operational again.*

10. Check that you can make phone calls using the new DAP.

14.3. Replacing DAP, no new DAP Available

When a DAP goes down in an IP DECT system, radio coverage is reduced and the handsets that have their subscription records in this DAP, cannot be used anymore. This requires immediate engineer intervention, even if there is no new DAP available. Execute the following procedure for replacing a DAP.

PROCEDURE: Removing a DAP

Actions

1. Make sure that the DAP Manager is up-and-running.

2. Open the DECT Manager WEB interface.

3. Click “Access Points”.

4. **Disconnect** the DAP that is broken, or that needs to be replaced! Do not continue this procedure until the DECT Manager indicates that the DAP is not "Working".

5. Write down the RPN of the DAP to be replaced. Select the DAP when it is not "Working" anymore.

6. Click "Delete" to delete the DAP. Note that this can take a few minutes! The system will distribute the subscription records that were on the broken DAP, to operational DAPs.

Note: *After the subscription records are distributed to operational DAPs, switch the handsets associated with these records, off and on, to make them operational again.*

7. All handsets should be operational again.Wait until you have a new DAP, then continue with the procedure in this Section.

PROCEDURE: Installing the new DAP

This procedure describes how to install a new DAP as replacement for a previously removed DAP (see previous Section.)

Actions

1. Make sure that the DAP Manager is up-and-running.

2. Make sure that the DHCP server and the TFTP server are up-and-running in the IP network.

3. Open the DECT Manager WEB interface.

4. Click "Access Points".

5. Connect the new DAP. Wait until you see that the new DAP is up-and-running (in the DECT Manager interface).

6. Cick the "Edit" button for the new DAP.

7. Change the RPN number of this DAP to the RPN number of the replaced DAP (which you have written down) and click "OK".

8. The new DAP will reboot. When the DAP is up-and-running again, it should have the RPN

of the replaced DAP.

15. MAINTENANCE TOOLING - DAP VIEWER

15.1. General

The DAP Viewer is a tool that displays operational data of the DAPs. This operational data covers IP networking data as well as detailed DAP data.

Note that the DAP Viewer is licensed! The license string is valid for one day only, based on the date of the day! It cannot be used on another date! When you issue a request for a license string, make sure to mention the date on which you want to use it!

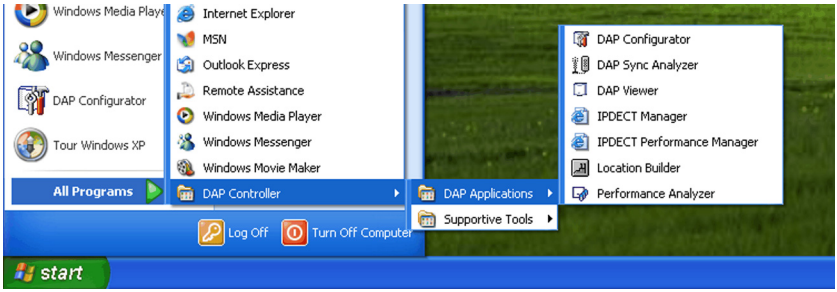
Note: *This chapter tells you how to start using the DAP Viewer but does not explain all the menu options and windows. Using the DAP Viewer requires that you have detailed knowledge of the architecture and operation of your IP DECT system. By means of this knowledge you should be able to interpret the menus and the windows in the DAP Viewer.*

15.2. Getting Started with the DAP Viewer

PROCEDURE: Getting started with the DAP Viewer

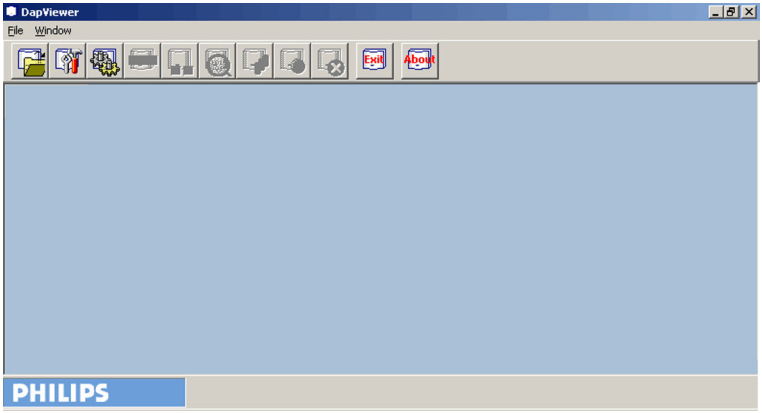
Actions

1. Start the DAP Viewer tool, via **Start**, **All programs**, **DAP Controller**, **DAP Applications**, **DAP Viewer**.



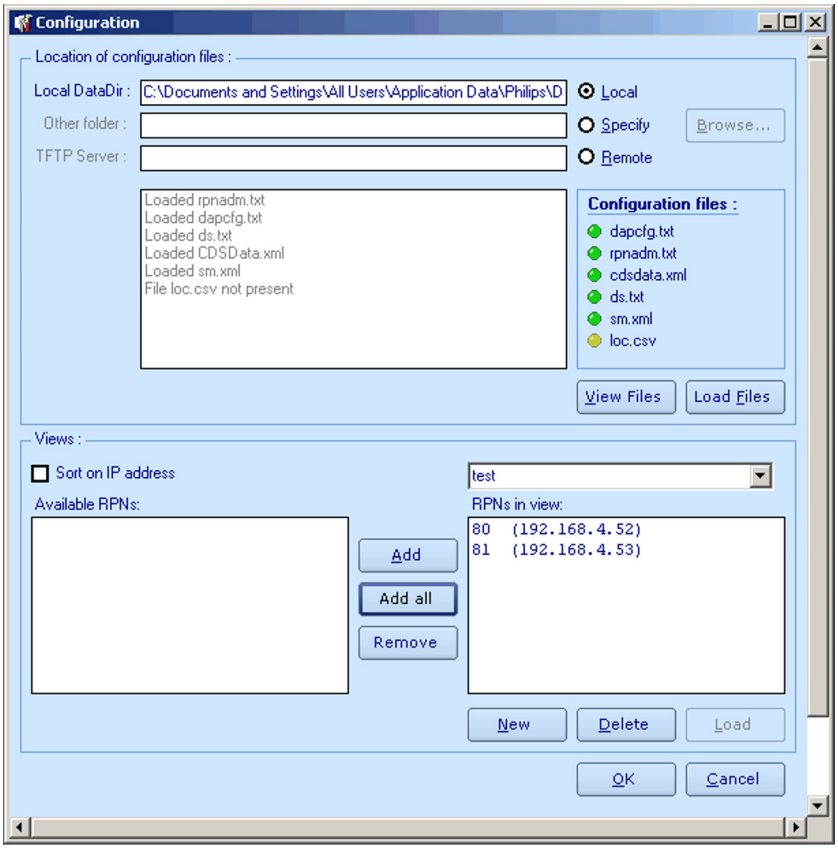
2. A window is displayed, where you must enter the license string. Enter the license string that is valid for this day.

3. The following window is displayed:



Click the top left icon.

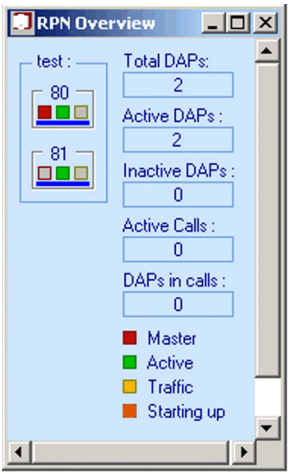
4. The following window is displayed:



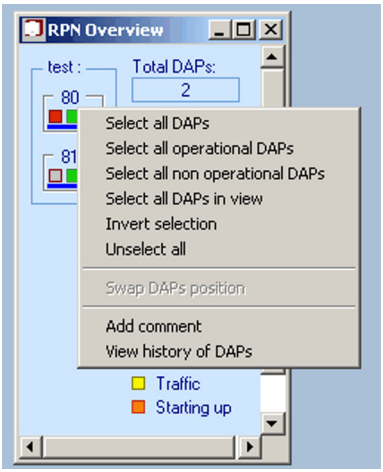
Select the "location of the configuration files". If you select "Local" the default directory for the configuration files is used: `C:\Documents and Settings\All Users\Application Data\Philips\DAP Controller\3.0`.
Click the button "Load Files".

5. In the bottom left pane, the available RPNs are displayed. Select the RPNs that you want to monitor, and click "Add" to move them to the pane "RPNs in View".

6. The following window is displayed.



In this RPN overview, you see overall data of the DAPs. To view detailed data, you must select a DAP or select all DAPs. When a DAP is selected, there is a blue line displayed under the RPN icon (see screen capture above.).
When you right mouse click an RPN, you will see a menu displayed:



Select the DAPs (RPNs) for which you want to display detailed information.

7. Now you can use the buttons in the tool bar in the top, to display detailed data. Click the button that shows you the information that you need. The following overview gives information about the functions of the buttons.

- **Open configuration files**
  This allows you to import the configuration files (and data files) into the DAP Viewer. Note that if a change is made (automatically) in one of the files (e.g. a new subscription), this is detected and the DAP Viewer asks you if you want to use the new file contents.

- **Change settings**
  Here you can change the RPN Monitoring interval. This is the interval between polling a DAP to retrieve data from it. There is also a possibility to set alarm levels. If an alarm occurs, the bottom bar in the DAP Viewer gets red and shows the message “alarm”. Note that the E-mail function is not enabled in this configuration!

- **Change services status**
  This allows you to stop/start the DAP Controller services.

- **Show RPN data**
  This window shows you detailed data of the selected RPN/RPNs. Note that you see an overview of the occupied timeslots on the selected DAP/DAPs. You can change the view from IPUI to DNR by means of a check box.

- **Start or stop the monitoring**
  Monitoring is done based on a polling mechanism. Based on this polling, DAPs sends their data to the DAP Viewer. You can stop this polling via the “Start or stop the monitoring”.

- **Start or stop tracing**
  This is used for third line tracing. For first line and second line maintenance, this tracing is not useful because it is hard to interpret. (Use Diag@Net instead.) Note that this option does not generate trace files. It only sends tracing data to a (dummy) destination, which is an IP socket. The actual tracing must be done by means of monitoring this (dummy) IP socket using a sniffer (like Ethereal).

- **Show registrations**
  This button offers you the possibility to show the registrations (subscriptions) on a DAP in Distributed mode. A nice overview of the subscribed numbers per DAP is available. Also you can search a subscribed number on the DAPs.

- **Location detection**
  This allows you to trace the subscription number-DAP relation for an active call. You can enter the subscription number, and then a coloured block on the DAP icon is shown, when a call is active.

- **Show alarms**
  This shows you a history log.

16. MAINTENANCE TOOLING - SYNC. ANALYZER

16.1. Introduction

The Synchronization Analyser offers you the possibility to generate a graphical overview of the synchronization structure in the system. Besides this it provides a feature to calculate the best candidate for being the synchronization master and is capable of pinpointing possible problems in the synchronisation structure. The Synchronization Analyser is free to use.

The input for the Synchronization Analyser is the `visadm.txt` file. This file is generated when clicking the "Save visibility" button in the Performance Manager interface, see Section "Performance Manager Items" in the IP DECT Advanced Data Manual.

The visibility data can also be combined with location data, making it possible to offer a three dimensional view of the synchronization of DAPs within a building or a site. The location data files are created in a tool called the Location Builder, on which more information can be found in Chapter 17. "LOCATION BUILDER TOOL".

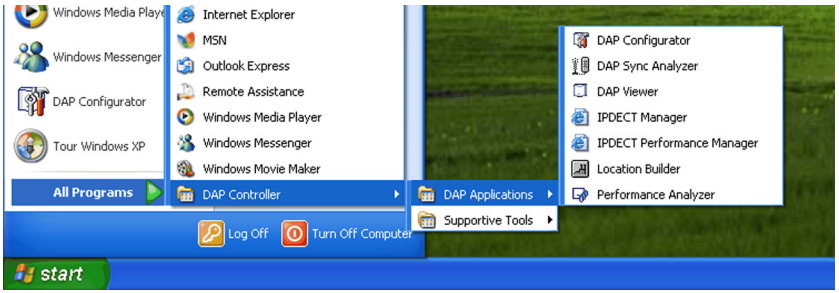
The program offers the following functionality:

- Hierarchic view of the DAP Synchronization using visibility files.
- Three dimensional localization of DAPs using location files (see also the chapter on the Location Builder)
- Traffic Bearer Control file analysis, to follow the path of a handset through the IP DECT system, when having a call.

The main window will be displayed. See the following sections.

16.2. Starting the Tool

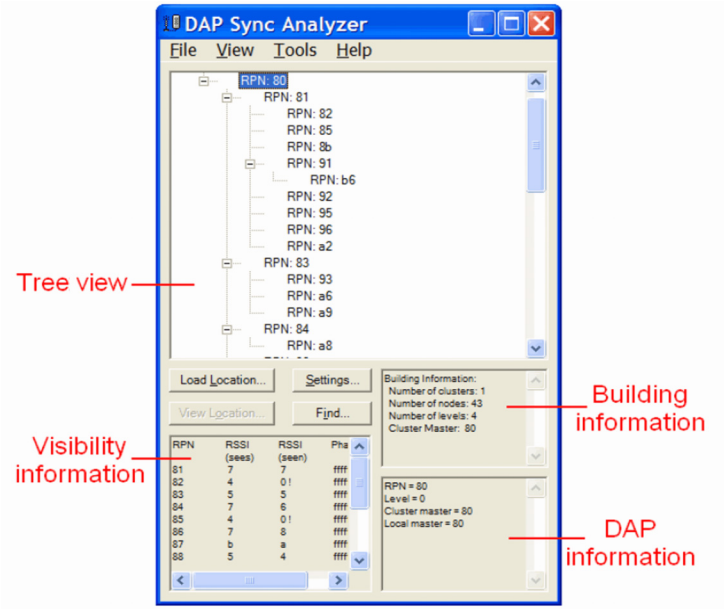
Start the DAP configurator tool, via **Start**, **All programs**, **DAP Controller**, **DAP Applications**, **DAP Sync Analyser**.



After the tool is started, the Main window is displayed.

16.3. Main Window

The following screen capture shows the main window, which is displayed when the Sync Analyser is started.



The main window displays the following information:

- **Tree view**
  Shows a hierarchical view of the synchronization tree. In the tree view, you can select a specific DAP. The visibility information of the selected DAP is displayed in the Visibility Information window.

- **Visibility Information**
  Shows an overview the RSSI values. “Sees” means that the selected DAP sees the other DAPs with a certain signal strength. “Seen” means that the other DAPs can see the signal strength of the selected DAP. Note that although the radio signal connection is reciprocal there can be differences in the “seen” and “sees” RSSI value. This difference is caused by the fact that this visibility information is based on a snapshot.
  The RSSI values are hexadecimal in the range: 0 ... e., , where “0” is no signal.The -80 dBm boundary is found at the boundary between value 3 and 4 (approximately).
  Generally, the Phase difference must be ffffffff with a maximum deviation of 7 (higher or lower).

- **Building Information**
  Shows overall data of the DECT cluster.

- **DAP Information**
  DAP Information shows data of the selected DAP.

In this main Window, you will find the following buttons:

- **Load Location**
  This asks for opening a Location file (file that contains a "map" of the building). See Chapter 17. "LOCATION BUILDER TOOL" for more information on the tool to create the Location file.
  After loading the file, it opens the Location window, see Section 16.4. "Location Window".

- **View Location**
  This opens the Location window without asking for a Location file, see Subsection 16.4. "Location Window"

- **Settings**
  This opens the Settings window, in which you can enter the RSSI threshold and the Phase Difference threshold.

- **Find**
  Allows you to search for an RPN based on entering the RPN number, the MAC address or Info Field.

The menu bar offers a number of menu options which are explained in the following lists:

- **File**
  - **Open**
    Opens a Visibility File
  - **Compare**
    Opens a Visibility file and compares it with the current tree.
    In the results you might see a: "+", "-", "=" or "X".
    "+" sign Red = The current level of an RPN is higher that the one in the compared file.
    "-" sign Red = The current level of an RPN is lower that the one in file that you have loaded for comparison.
    "=" sign Green = means current level is the same as the compared level.
    "X" sign Red = This DAP does not exist in the file that you have loaded for comparison.
  - **Print**
    Sends the Tree view to a printer.

- **Exit**
  Exits the program.

- **View**
  - **Problems**
    This selects the problem view, which is the default. A number of potential problems, like DAPs that can only synchronize with one other DAP, are defined within the program, and indicated in the tree view by an exclamation mark.
  - **Synchronization**
    This selects the synchronization view which shows the synchronization path of the selected DAP. Icons in the tree view indicate the following conditions:
    "+" sign Blue = Selected DAP sees this DAP.
    "+" sign Red = Selected DAP is synchronized on this DAP
    "+" sign Purple = Selected DAP sees and synchronizes on this DAP.
  - **New Master**
    Sets the currently selected DAP as cluster master in the tree view.
  - **Best Master**
    Calculates the best master.
  - **Expand All**
    Expands the entire tree view.
  - **Collapse All**
    Collapses the entire tree view.
  - **Location**
    This asks for opening a Location file (file that contains a "map" of the building). See Chapter 17. "LOCATION BUILDER TOOL" for more information on the tool to create the Location file.
  - **Settings**
    This opens the Settings window, in which you can enter the RSSI threshold and the Phase Difference threshold.
    The RSSI values are hexadecimal in the range: 0 ... e, where "0" is no signal. The -80 dBm boundary is found at the boundary between value 3 and 4 (approximately).
    Generally, the Phase difference must be ffffffff with a maximum deviation of 7 (higher or lower).

- **Tools**
  - **Track Portable**
    Asks for opening the traffic bearer file. After that it opens the Portable Tracking window.

- **Help**
  Self explaining.

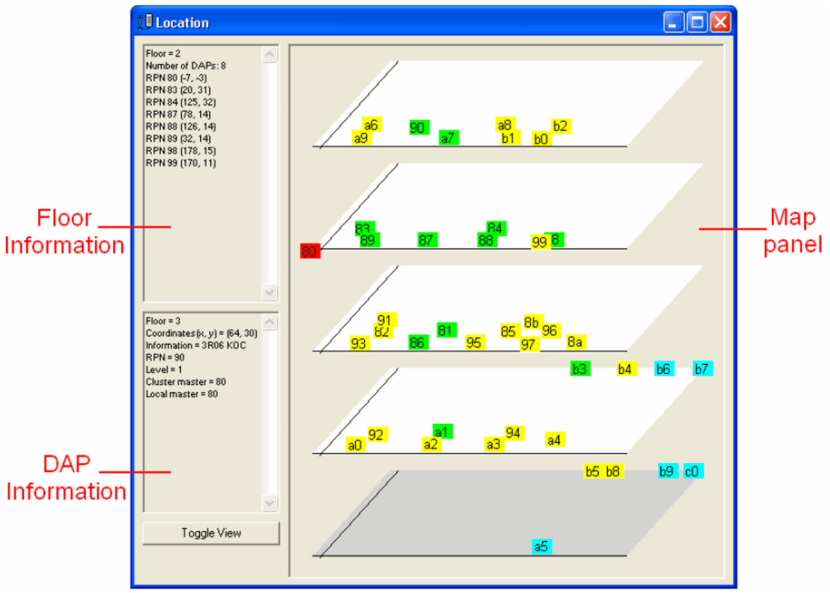
16.4. Location Window

The Location Window shows you a three dimensional view of the location of the DAPs. Each DAP has a colour that is related to its level, e.g. the following colours are used for the first three synchronisation levels:

- Red = Root level
- Green = First level
- Yellow = Second level

The location information must have been inported into the tool from a file. Consult Chapter 17. "LOCATION BUILDER TOOL" to see a Location file must be created. The presentation shows the floors in an area and the DAPs on each floor. When selecting a floor or a DAP, information is shown in the text boxes on the left side. When a DAP is selected, only the other DAPs it can “see” are coloured, and the corresponding node in the tree view is also selected. It is possible to zoom in on a single floor by double clicking the view or by using the Toggle View button. By right clicking on the map pane a context menu is shown that can be used to zoom in or out.

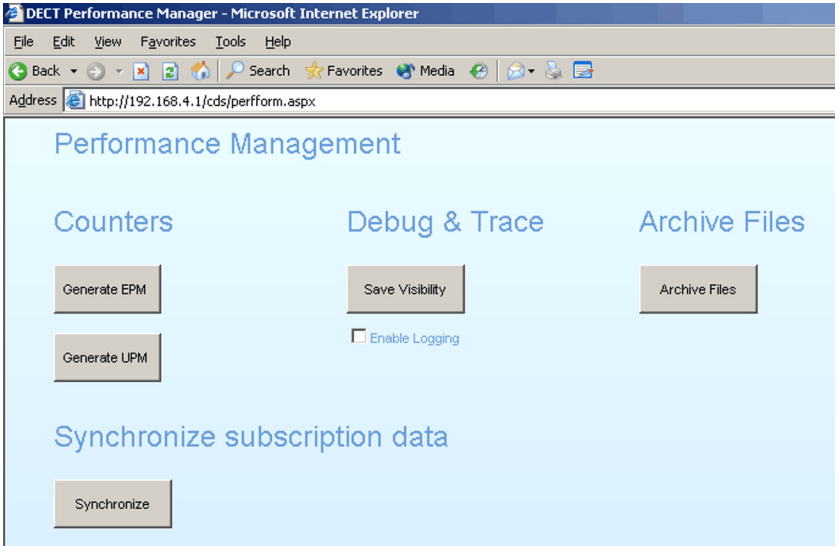
The following screen capture shows an example of a Location Windows.



16.5. Portable Tracking Window

The portable tracking window allows you to follow the movement of a portable from DAP to DAP. Be aware of the fact that the portable can only be tracked when it is having an active call!

Tracking a portable requires the file `pmtbc.dat`, which is the traffic Bearer Control file. This file contains a log of the used Traffic Bearers. It must be generated with the help of the DAP Performance Management interface. See the following screen capture.



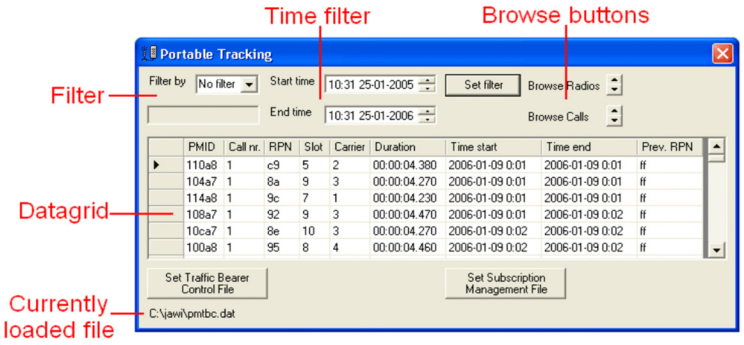
In this window, you must check the check box "Enable Logging" to start logging the use of the Traffic Bearers, and subsequently storing this information in the file `pmtbc.dat`.

When you have the required files, use the following procedure to execute portable tracking:

PROCEDURE: Portable Tracking Procedure

Actions

1. Make sure you are in the Main Window of the DAP Sync Analyser.
2. Select the "Tools" menu from the menu bar.
3. Select "Track Portable".
4. The window as shown in the following screen capture is displayed.



5. Now load the file: `pmtbc.dat` from the directory `C:\..\PM\` on the DAP Controller/ Manager PC. The information in this file is based on an internal portable Identifier, the PMID. However, you want to see the extension number in the window. The requires a conversion file, see next step.

6. Load the file `sm.xml` from the DAP Controller/Manager PC, using the "Set Subscription Management File" button. This file contains the relations between the PMIDs to the Extension numbers. Once this file is loaded, an extra column will appear in the data pane, providing the extension number.

7. Now you can use the Time Filter and the Browse buttons as qualifiers for the data that is displayed in the window. The following items give information on these qualifiers.

The qualifier controls:

- **"Filter by" , "Start time", "End time", "Set filter"**
  You can filter the data that is displayed, using the Filter controls. The data pane can be filtered on a specific PMID or DNR and on time and date. To apply a filter, the Set Filter button has to be pressed.
- **"Browse Radios", "Browse Calls"**
  These buttons can be used to quickly browse between different calls, or radios.

16.6. Typical Workflow

The following step-action procedure is an example of a typical workflow.

PROCEDURE: Example of a Typical Workflow

Actions

1. Double click the file: `DAPSyncAnalyzer.exe` to start the DAP Sync. Analyser.

2. Load the visibility file `visadm.txt` to import the synchronization data using the menu "File" --> "Open".

3. Use the options in the menu "View" to analyse the synchronization structure, and if necessary use the menu options under the menu "View" to trouble shoot the structure.

4. Optionally!
   After loading the visibility file you can load a location file. The location file contains a site "plan" (site "map") with buildings and floors in which the DAPS are positioned. This allows you to determine quickly the position and range of a specific DAP. You can create a Location file using the Location Builder tool. (See Chapter 17. "LOCATION BUILDER TOOL" for more information on the tool.)

5. Optionally!
   After loading the visibility file you can load a "Traffic Bearer Control" (`pmtbc.dat`) data file. This file contains statistics/logging on traffic bearers. To open this file, select "Track Portable" from the "Tools" menu. The program will ask for the location of the file.
   The data from the TBC file is presented in a table. At the start, only the PMID of a portable is known. To associate PMID values with a specific extension number, a Subscription Management (`sm.xml`) file is needed. Once this is loaded, an extra column will appear in the data pane, providing the extension number.

17. LOCATION BUILDER TOOL

17.1. Introduction

The Location Builder tool is used to create a site map with buildings and inside the buildings floors and if necessary, lines to indicate contours or anything else that you want to draw. In this map you can put the DAPs according to their position in the real site. By doing this, you will have an overview of the DAP structure in a building. You can store this information in a file. When you import this file into the DAP Sync Analyser tool, you will get a overview of the synchronization structure in a building which is based on measurements.

17.2. How to Use

17.2.1. General

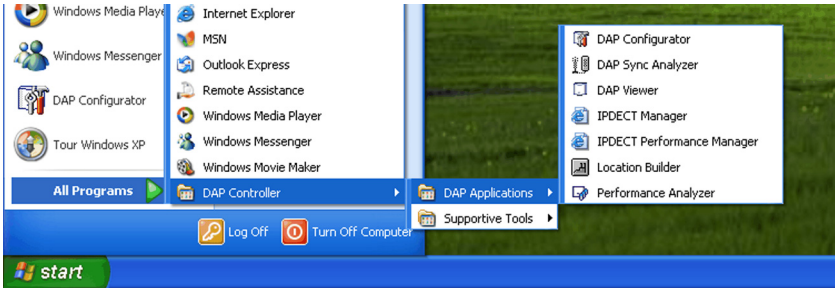
Using the Location Builder tool starts with starting up the tool and getting familiar with the main window. After that you can start creating a Location File. These two processes are described in the next sub-sections.

17.2.2. Starting the Location Builder.

PROCEDURE: Starting the Location Builder

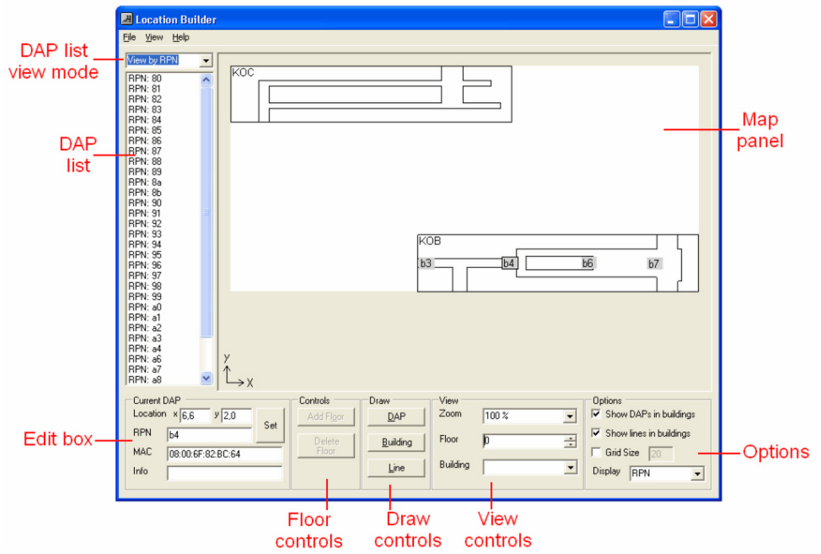
Actions

1. **Starting the Location Builder**
   Start the DAP configurator tool, via **Start**, **All programs**, **DAP Controller**, **DAP Applications**, **Location Builder**.



2. **Getting familiar with the Main screen**

The following screen capture shows you the main screen. Note that after starting the Location Builder, the main screen does not show data yet. However, in the screen capture below, there is already data *as an example* in order to explain the fields (panes) in the main window.



The main window contains the following panes:

- **Map panel**

  The map panel shows a map of the area. There are two view modes. The first is the Location View, which will show one whole floor with multiple buildings visible. The second is the building view, which will only show a floor inside a building. Double clicking on a building switches between views.

  It is possible to select either a DAP, a building or a line.

  When right clicking on the map, a context menu will be shown, that can perform a number of actions on the selected item.

  The Location Builder depends heavily on the usage of coordinates for the localization of DAPs, buildings and lines. When hovering over a map, the coordinates of the mouse cursor will be indicated. The origin of the coordinate system is located at the left bottom corner of the map.

- **DAP List view mode**
  This allows you to select the view mode for the DAP list. There are three view options: “RPN numbers”, “MAC addresses” or “Info” field
- **DAP List**
  Shows a list of DAPs that are not put on the map yet. They can be dragged from the list onto a position on the map. Normally the DAP list is populated from the `RPNadm.txt` file via the “File”, “Import” menu.
- **Edit box**
  When an item (Location, Building or DAP) is selected on the map, this box shows a number of properties that can be edited. The Set button must be used, otherwise the values will not be updated.
- **Floor controls**
  Allows you to add or delete a “Floor”, or set the location for a “Floor”
- **Draw Controls**
  Allows you to add a DAP a “Building” or a Line
- **View controls**
  Allows you to change the view of the Map pane.
- **Options**
  Useful self-explaining options.

3. **Continue with ....**
   Continue with creating a Location File. Use the following task procedure.

17.2.3. Creating a Location File

PROCEDURE: Creating a Location File

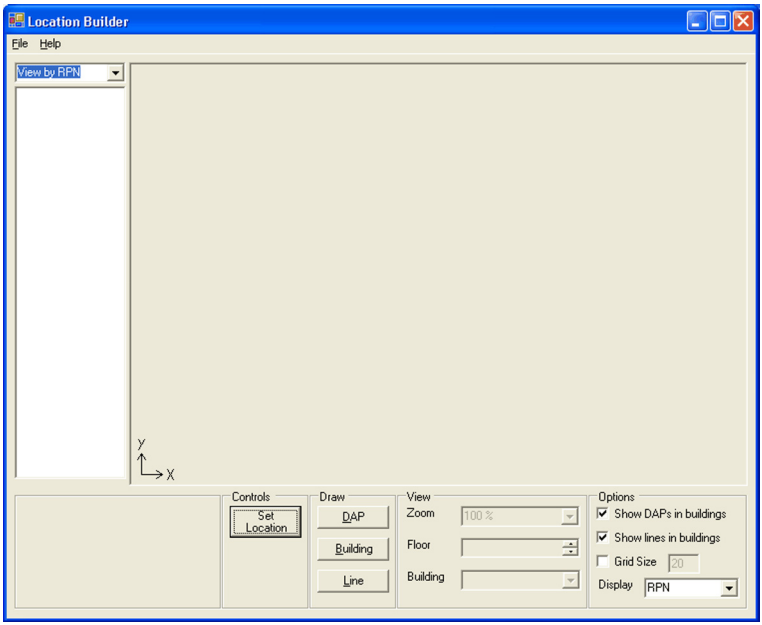
Actions

1. **Pre-requirements**
   Make sure that you have up-to-date maps of the building(s).

2. Make sure that you have a proper understanding of the sizes of the area and the buildings. Be aware that the scales of the maps may differ.

3. **Starting the Location Builder**
   Search for the **`LocationBuilder.exe`** file and **double click** it. This will start the Location Builder. The Location Builder window should be open now, according to the following screen capture.
   (Note that in the window that is displayed on your PC does not contain any data yet, and

should therefore look like the following screen capture.)



4. **Initializing Location**.
   Click the **Set Location** button to initialize the Location. Set the size of the Location to a value that allows all buildings to fill in.

Note: *You cannot define the dimensions (e.g. in meters) of the values that you enter. However, it is advised to enter values that equals meters, simply because it is easier to interpret.*

5. **Adding Building(s)**
   Click the button "**Building**" to add a building to the Location. Note that it is also possible to add a building using the left mouse button to indicate the left-bottom corner of the building and then clicking the right mouse to popup the menu containing "Add Building". Note that you will see the "Add Building" window. In this window you must enter the location and the Size:
   - x: "X" co-ordinate of the bottom left corner of the rectangle that represents the building.
   - y: "Y" co-ordinate of the bottom left corner of the rectangle that represents the

building.
- w: "W" is the width of the rectangle that represents the building. This should equal the actual size (length) of the building.
- h: "H" is the depth of the rectangle that represents the building. This should equal the actual size (width) of the building.

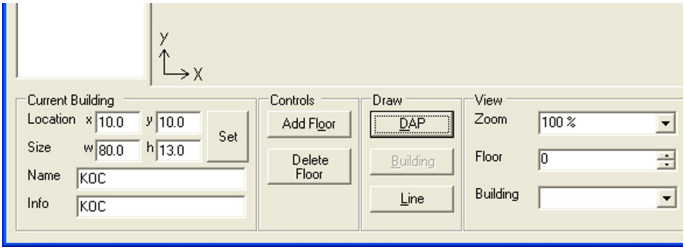
When a buildings does not have the correct size or location, this can be corrected by selecting the building, and then editing the building properties in the Edit pane (left bottom corner of the Location Builder).

6. **Adding Line(s)**
   Lines are used to add contours and shapes to buildings. The lines can provide a reference to items on the maps like stairwells, elevator shafts or oddly shaped (non rectangular) buildings.
   To add lines to a building, the building view must be used. Activate it by double clicking the building where lines should be added. Adding lines can be accomplished by using the **Add lines** option from the menu that is displayed when Right Mouse Button clicking in the Location area. It is also possible to add lines using free hand. To make it easier to add lines in freehand modes, it is advised to activate the grid (right bottom corner of the Location Builder window. This gives a better reference as to where the lines should be placed.
   To place lines in freehand modes, do the following:
   - Activate the "**Line**" button in the draw controls box.
   - Point the cursor to the location of the first point of the line.
   - Click and hold the left mouse button.
   - Point the cursor to the location of the second point of the line.
   - Release the mouse button.
   - Continue this procedure until all lines are drawn.

   The freehand modes has a helper function that helps drawing vertical and horizontal lines. This straightens a line that is almost horizontal or almost vertical.

Note: *There are two view modes. The first is the Location View, which will show one whole floor with multiple buildings visible. The second is the building view, which will only show a floor inside a building. Double clicking on a building switches between views.*

7. **Adding Floor(s)** Only necessary when buildings are multi-floor buildings.
   A building usually consists of multiple floors. In this step these floors will be added. To add a floor, first double click the border line of the Building to which you want to add a Floor. The "Map panel" changes, and you will only see the Building instead of the entire Location. The "Control" pane in the bottom part of the Location Builder shows the Floor controls. See following detailed screen capture:



Click the "Add Floor" button. The "Add Floor" window opens. Enter the relevant data in the "Add Floor" box and click "OK". As you might have noticed, it is possible to add multiple floors at once and to copy the lines of the current floor to the newly created floors. After the floors are added, it might be necessary to also add lines to the new floors, or to change the lines that are copied to the new floors.

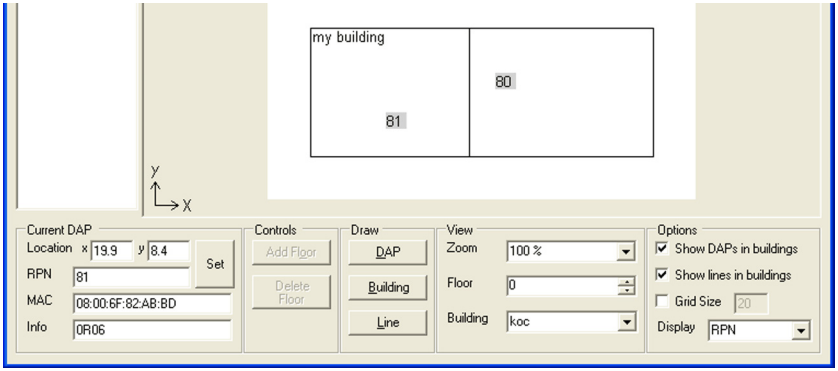
8. **`RPNadm.txt` file available?**
   At this point the location should be filled with buildings, the buildings with floors and the floors with lines. This is all the information needed to provide a reference framework for the position of the DAPs. The next step depends on the current status of the system. When the system is up and running, there is an `RPNadm.txt` file available. If so, proceed to the next step, step 9. If there is no `RPNadm.txt` file available, proceed to step 11.

9. **Import `RPNadm.txt`**
   The `RPNadm.txt` file is generated by the DAP Manager. It contains the relation between the RPN number, the MAC address, etc. Select the "Import" menu from the "File" menu. Open the `RPNadm.txt` file. The program will ask for the location of the `RPNadm.txt` file. Navigate to the relevant directory. After that a dialogue box will popup asking what the preferences are for the importing of the file. If "Update DAPs already located" is checked, uncheck it, and click Ok. The DAPs will now appear in the DAP list at the left of the program window.

10. **Dragging the DAPs to the map**
    The DAP list shows the DAPs that need to be located on the Map. On top of the list you see the view mode select box where you can select the display mode. To move a DAP to the Map, simply drag it onto the Map. When accidentally a DAP is released on the wrong position, you can drag it to correct place or it can be put back in the DAP list by the option "Move To" in the context menu (right mouse button click on DAP).
    When a DAP is placed on the Map, an autonumber function for the Info field will be activated. This function only works when the following two items are true:

- The previous DAP added must have an Info field in the form `{current floor number}{string}{number}`. e.g. `0R05`. Note that these are the notations as used in the Site Survey, consult therefore the Site Survey manual for more info on these notations.
- The current DAP must have an empty Info field.

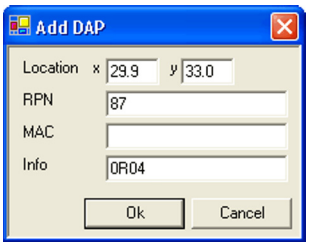
If both these requirements are met, the current DAP will get an Info field assigned in the form `{current floor number}{string}{number + 1}` e.g. `0R06`. The following screen capture shows the RPN data and the Info field data in the Edit box pane, titled Current DAP.



Continue with placing the DAPs until the DAP list is empty, then skip the next step and proceed to step 8.

11. **Adding DAPs**

To add a DAP manually, right mouse click a point on the Map. Select Add DAP from the popup menu and you will see the following window displayed.



There are two autonumber functions active for this purpose. The RPN will be automatically increased, and the Info field will be filled in, according to the description in the previous step (10). A DAP will be created at that position.

12. **Finishing actions**
    When the building the Location is complete, you can use the following options: use the Save option in menu File to save the location file as `.xml` file. You can also export the file as `.csv` file, which can be used in the DAP Sync Analyser.
    - Save
      To save the Location file as `.xml` file. This file can be imported into the DAP Sync Analyser tool.
    - Export
      Export can be used to export the following files:
      Location file , file type `.csv`. This file does not contain building information, only DAPs information
      Dummy visibility file, file type `.txt`. This creates a flat synchronisation hierarchy. This can be used when no realistic visibility file can be obtained.
      RPNadm file, file type `.txt`. This file contains the RPN data as you have setup in the Location Builder tool. Normally this contains the RPN data as given in the imported `RPNadm.txt` file.

17.2.4. Maintenance

Changes in the Location configuration might be made after the Location file is created. The following changes might be necessary in an existing configuration:

- **Minor configuration changes (excluding RPNadm data)**
  When minor or small changes must be made in the configuration, import the Location file. After that select the item that has to be updated. The properties of the selected item are displayed in the Edit box, where they can be changed.
- **Changing RPNadm.txt data**
  The `RPNadm.txt` import function contains an update utility. For this, an up to date `RPNadm.txt` file is needed. When this is imported, check the "Update DAPs already located" option, and when necessary, choose for MAC address or RPN to take preference. This is useful when for instance a number of RPNs have changed in the DAP Manager, but the radios are still identical, thus having identical MAC addresses.

A . CONNECTING DIRECTIONAL ANTENNAs

WARNING: THE ERP (EFFECTIVE RADIATED POWER) OF A DIRECTIONAL ANTENNA IS HIGHER THAN AN THE ERP OF AN OMNI-DIRECTIONAL. THEREFORE, ONLY USE THE DIRECTIONAL ANTENNA (GAIN 8 DBI) THAT IS SUPPLIED BY NEC PHILIPS UNIFIED SOLUTIONS. THE MINIMUM DISTANCE BETWEEN PEOPLE AND THIS (ACTIVE) ANTENNA MUST BE AT LEAST 6,5 CM. (NECESSARY TO COMPLY WITH THE EU COUNCIL RECOMMENDATION 1999/519/EC.)

The DAP AP200**E** allows you to connect directional antennas. It is equipped with connectors instead of internal antennas. However, these connectors are inside the DAP. Therefore follow the following procedure to connect the antennas:

PROCEDURE: Connecting Directional Antennas to AP200E

Actions

1. Remove the two screws in the holes at the rear side of the AP200E.

2. Open the AP200E cabinet. This might be a bit difficult, because it is closed by means of four "click" mechanisms, two at each long side of the cabinet. If necessary, use a small screw driver to open the click mechanisms one by one carefully.

Note: *Be careful with the cover, the printed circuit board is a part of the cover. Keep the cover on a save place, to avoid damaging the printed circuit board. Take precautions of static charges.*

3. When you have opened the AP200E box, you see two antenna connectors on the printed circuit board. The directional antenna has two connectors as well; you must install coax cables in between. Determine if the cables should leave the AP200E cabinet via the rear side or via the bottom side. In case the cables should leave the cabinet at the rear side, push out the two holes at the back of the AP200E cabinet. In case the cables should leave the cabinet at the bottom side, drill two holes in the bottom side of the cabinet.

4. Connect the cables to the AP200E and to the antenna. Secure the nuts of the coax cables with a SMA Torque Wrench.

5. Snap the cover side of the AP200E to the rear side of the cabinet, to close the cabinet. Screw the two screws back into the two holes in the rear side, to secure the two sides (rear side and cover side) of the AP200E cabinet.

B . UPGRADE TO LATEST RELEASE

To upgrade to the latest release of the DAP Controller software, consult the IP DECT Advanced Data Manual.

C . PROBLEMS WITH .Net Framework 2.0

Problems with the WEB interface may occur when .NET Framework version 2.0 is installed as default. This is the case if:

- you use Windows 2003 R2 .
- Other Windows versions with an updated .NET Framework (to version 2.0)

Follow the following procedure to solve the problem:

PROCEDURE: Adapt settings for IP DECT with .NET Framework 2.0

Actions

1. Go to “Start”, “Settings” “Control Panel”, “Administrative tools”, “IIS Manager”.
2. In the IIS window, go to “local computer”, “Websites” and open the “Default Website”.
3. In the right hand pane, you will see “CDS”. Select CDS and right mouse click on it.
4. Select “properties”.
5. In the window that opens, click the ASP.NET tab.

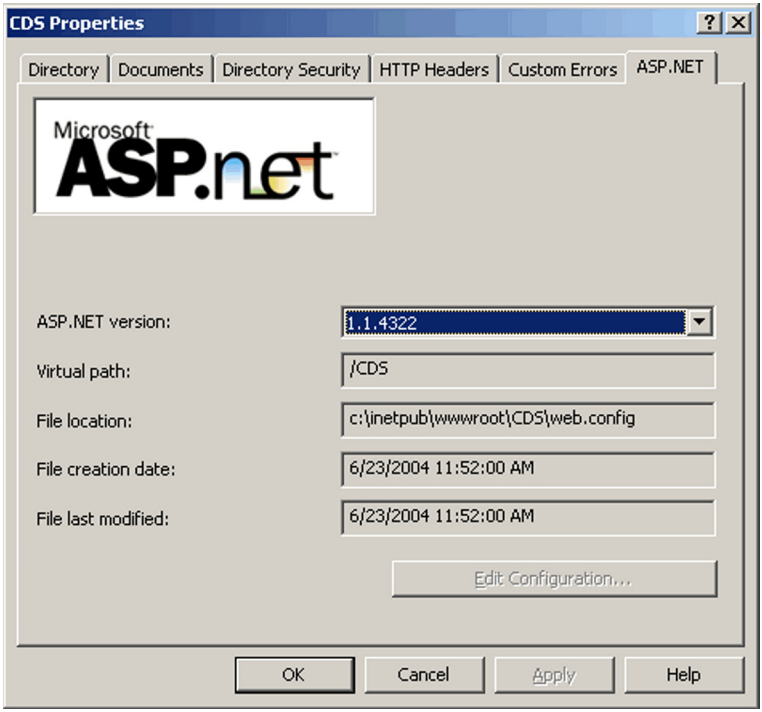


Figure C-1 ASP.NET Settings.

6. In ASP.NET version, select version 1.1.xxxx.

7. Click OK and close all windows involved.

D . OVERVIEW OF DEFAULT USED IP PORTS

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

Protocol	Interface/Device	Default Destination port
DHCP	DHCP Server	67
	DAP	68
Call Control	DAP	28000-28006
RTP (Real Time Protocol)	DAP	3000-22179
TFTP	TFTP Server	69 (only for initial communication) . then:1024-65535

Table D-1 Default ports used in Business Mobility IP DECT.