UNIVERGE® SV8300

IP-DECT Installation Guide

NDA-31472
Issue 1.0

NEC Corporation of America reserves the right to change the specifications, functions, or features at any time without notice.

NEC Corporation of America has prepared this document for use by its employees and customers. The information contained herein is the property of NEC Corporation of America and shall not be reproduced without prior written approval of NEC Corporation of America.

D^{term}, NEAX and UNIVERGE are registered trademarks of NEC Corporation and Electra Elite is a registered trademark of NEC America, Inc.

NEC Corporation of America
6535 N. State Highway 161
Irving, TX 75039-2402

Communications Technology Group

Preface

This manual is valid for Business Mobility IP DECT Software Release 6.0.

IMPORTANT:

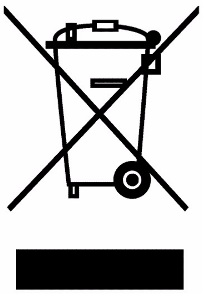
This manual gives information for setting up a Business Mobility IP DECT system. However, the Business Mobility IP DECT is normally part of an IP network. The success of the installation depends on the structure and components in the IP network. Make sure that you have sufficient knowledge of the customers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

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 are 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-unified.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.

TABLE OF CONTENTS

Chapter 1 DECT System Characteristics

Chapter 2 DECT In An IP Network

Chapter 3 Licenses

Chapter 4 Network Configurations

Chapter 5 DAP Installation Items

Chapter 6 Preparing Your DAP Manager PC

Chapter 7 Installing - The DAP Controller/Manager

Chapter 8 Configuration - DAP Configurator Tool

Chapter 9 DAP Configurator Settings

Chapter 14 IP DECT Mobility In SV8300

Chapter 15 DAP Controller Redundancy

Appendix A Upgrade To Latest Release

Appendix B AP300 Versus AP200

Appendix C AP400 Versus AP300

Appendix D LRMS Messaging

Appendix E Overview Of Default IP Ports

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES AND TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

DECT System Characteristics

SECTION 1 GENERAL DESCRIPTION

The **DECT** System allows mobile users to use the switched telecommunication facilities provided by an SV8300 system. Such a mobile user can make or receive calls by using a cordless handset. Many call handling facilities of the SV8300 are available on the cordless handset. As the cordless connection is an IP 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 SV8300 via an IP Ethernet connection. The radio transceivers are placed within the working area so that a portable handset/telephone is always within radio coverage area of at least one such transceiver.

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

A radio transceiver in the DECT System is called the Radio Fixed Part (**RFP**) according to the DECT Standard. The RFP is also referred to as a base station. However, in the 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. Figure 1-2 DECT System Parts in an IP Solution as Add-On to a PBX shows a general IP DECT Solution. It shows the basic system setup for the Business Mobility IP DECT system.

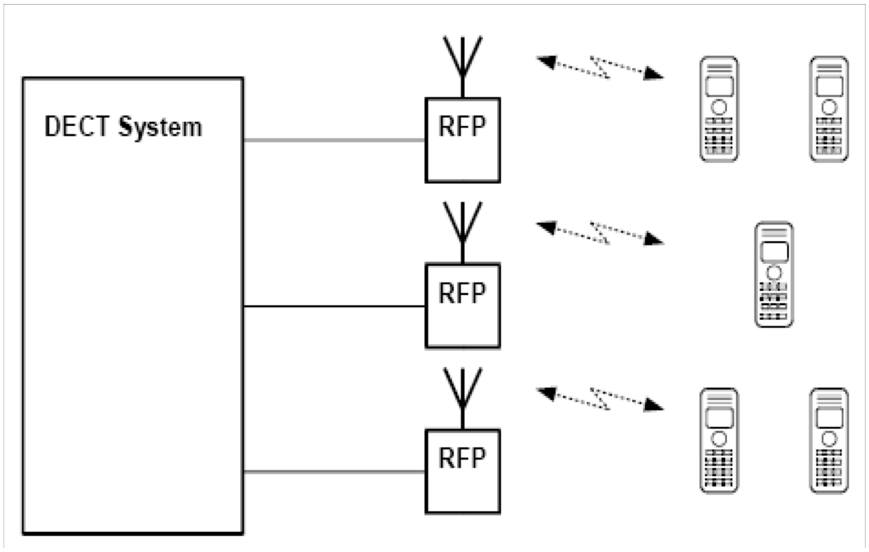
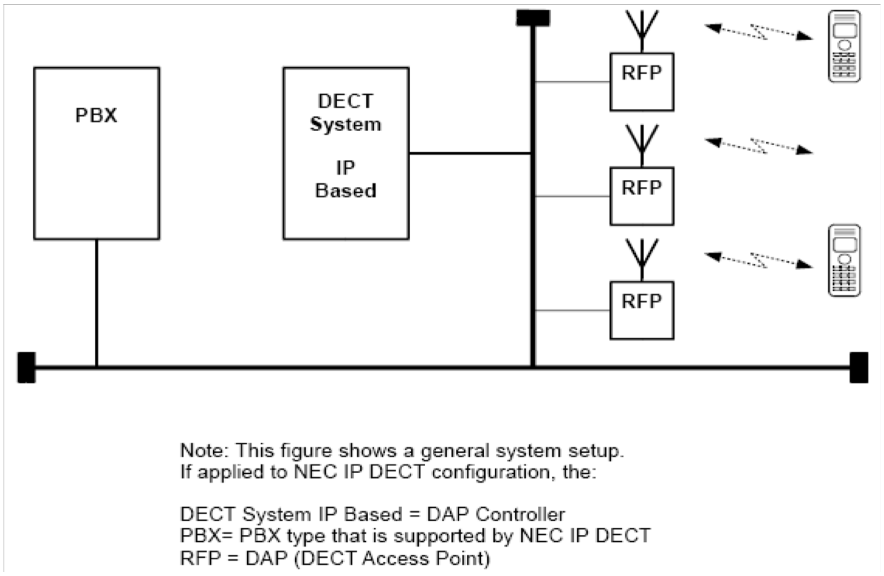


Figure 1-1 DECT System Parts (General)



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

DECT System IP Based = DAP Controller
PBX= PBX type that is supported by NEC IP DECT
RFP = DAP (DECT Access Point)

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

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 licenses.)

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

❍ The size of the area.

❍ The nature of the area:

❍ The number and the size of buildings in the area.

❍ The radio propagation characteristics of the building(s).

❍ Materials used for walls, floors, elevator shafts, reinforced glass, doors etc.

❍ Strong magnetic fields in the area (e.g. as result of welding equipment, radar, etc.).

❍ The amount of telephone users in an area, and how often they make or receive calls.

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

1.1 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. Refer to Figure 1-3 Carriers and Time Slots in the DECT Air Interface.

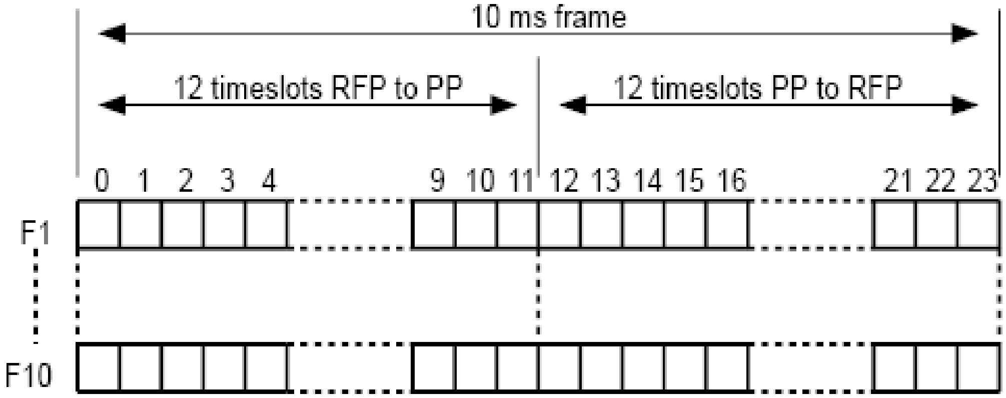
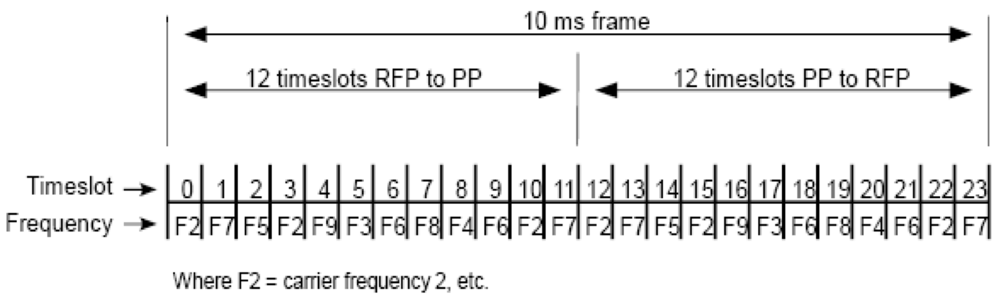


Figure 1-3 Carriers and Time Slots in the DECT Air Interface

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



Timeslot →	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Frequency →	F2	F7	F5	F2	F9	F3	F6	F8	F4	F6	F2	F7	F2	F7	F5	F2	F9	F3	F6	F8	F4	F6	F2	F7

Where F2 = carrier frequency 2, etc.

Figure 1-4 Each Time Slot Can Use Any of the 10 Carrier Frequencies

A PP can use any of the 12 time slots (in each direction) on any of the 10 frequencies for a full duplex connection. So a maximum of 120 full duplex channels are available for connections to the PPs, within a cluster of a microcellular 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.

1.2 Beacon Signal

1.2.1 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.

1.2.2 Beacon Signal and PP

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

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

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

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

1.3 Call Handling Procedures between PP and RFP

1.3.1 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 SV8300. (The voice connection is setup between the RFP/DAP and the other party.)

1.3.2 Paging and Answering a Call

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

1.3.3 Encryption

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

1.4 Cluster Arrangement

1.4.1 General

A cluster is defined as a logical group of radio cells belonging to one DECT system. Within this arrangement bearer handover is possible. 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 overlaps 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.

1.4.2 RFP Behavior 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.)

1.4.3 PP Behavior in a Cluster

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

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

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

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

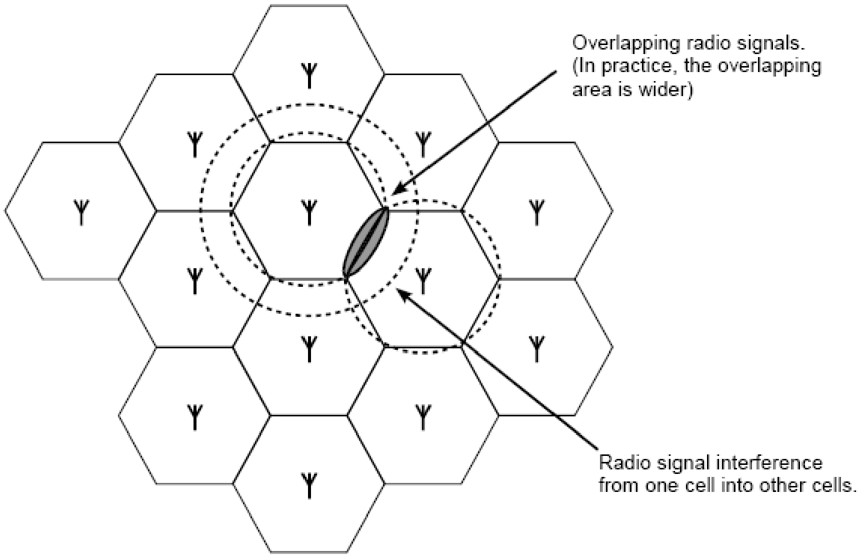

Overlapping radio signals. (In practice, the overlapping area is wider)
Radio signal interference from one cell into other cells.

Figure 1-5 Cluster Arrangement

1.5 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 to allow a "seamless handover" (no breaks and delays 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.

✎ A handover is always initiated by the PP!

1.6 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).
3. 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.
4. **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 opposite party. (Note that muting is done on both ends of the connection independently.)

1.7 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 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)

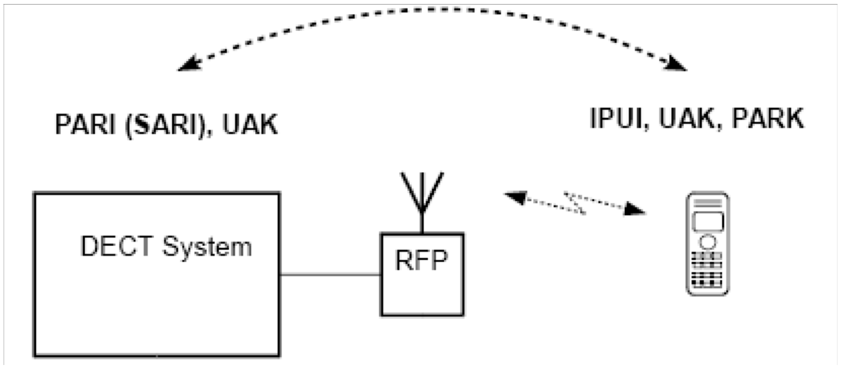


Figure 1-6 UAK Relation Between the IPUI and the PARI

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, refer to Figure 1-6 UAK Relation Between the IPUI and the PARI. The PARI is stored in the PP as PARK, the PP gets a unique identifier (IPUI) and a secret key (UAK) is assigned to the relation between the PP and the DECT System. From now on the PP knows to which system (PARI) it is subscribed. (In this section only the PARI is mentioned. Refer to 1.8 Secondary Access Right Identifier (SARI) on page 1-12).

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.

1.8 Secondary Access Right 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 1-7 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.

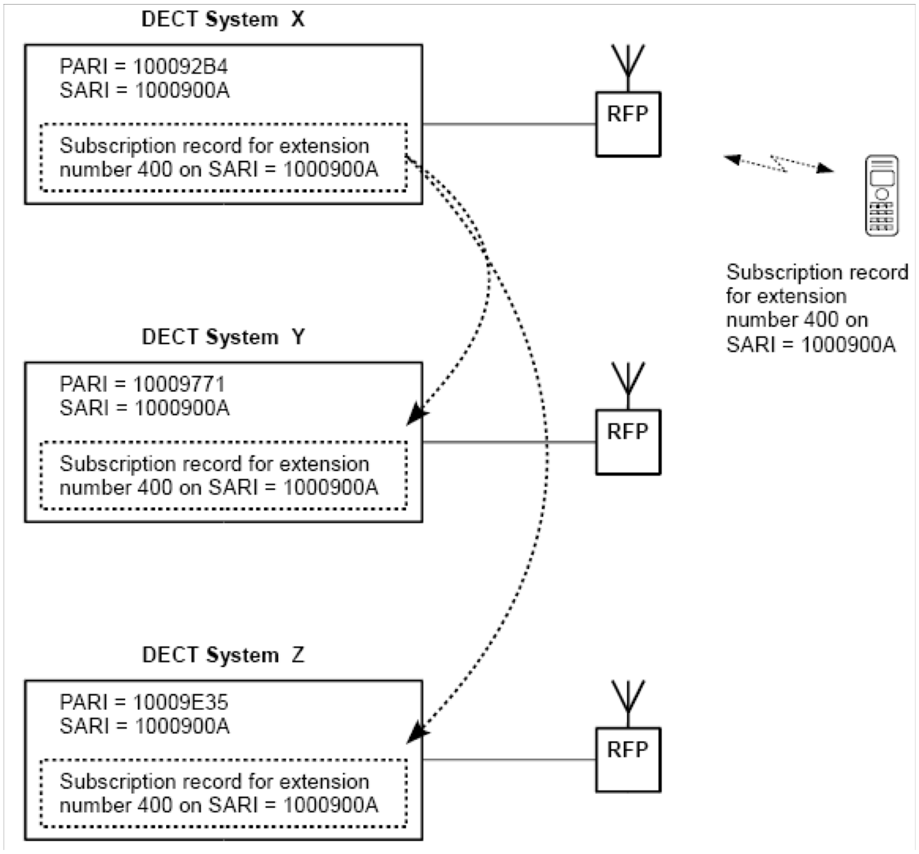

DECT System X
PARI = 100092B4
SARI = 1000900A
Subscription record for extension number 400 on SARI = 1000900A
RFP
Subscription record for extension number 400 on SARI = 1000900A
DECT System Y
PARI = 10009771
SARI = 1000900A
Subscription record for extension number 400 on SARI = 1000900A
RFP
DECT System Z
PARI = 10009E35
SARI = 1000900A
Subscription record for extension number 400 on SARI = 1000900A
RFP

Figure 1-7 Using SARI in Three DECT Systems

THIS PAGE INTENTIONALLY LEFT BLANK

DECT In An IP Network

2

SECTION 1 SYSTEM ARCHITECTURE

Figure 2-1 IP DECT with SV8300 - System Configuration refers to the general configuration of the IP DECT system in an SV8300 configuration.

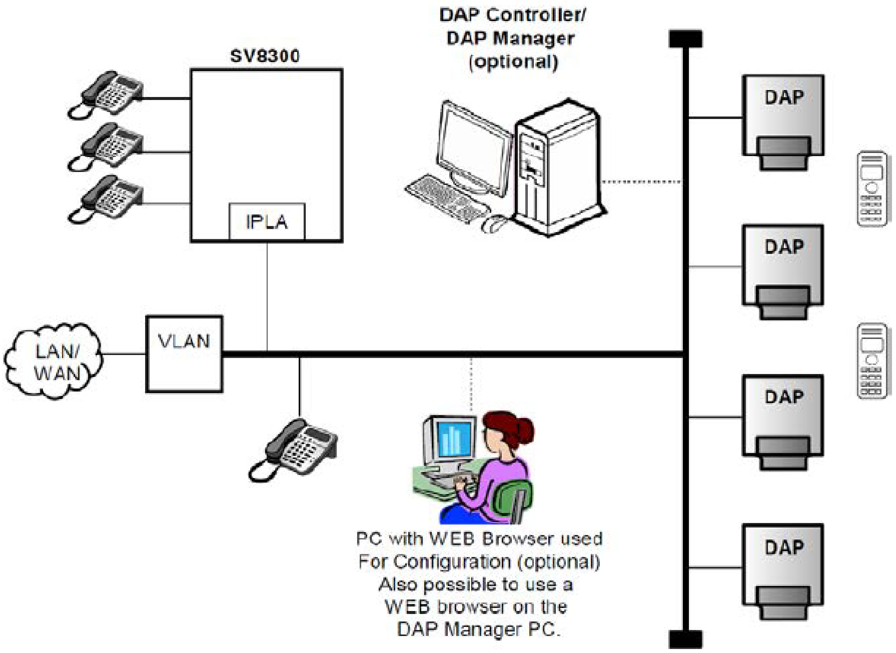


Figure 2-1 IP DECT with SV8300 - System Configuration

❍ DAP

The DAP (DECT Access Point) is the actual DECT transmitter/ receiver. There are three generations of DAP types: AP300 and the AP400. The AP400 is the latest model.
All DAP Types supports up to 12 simultaneous calls. For the AP400, functionality licenses are applicable.
The power provision is done via the Ethernet interface (PoE).

Besides radio traffic, the DAPs take care of subscription control and call control data handling to/from the SV8300.
The AP300 and AP400 are equipped with internal antennas.

- DAP Controller/Manager

  The DAP Controller/Manager performs the following main functions:

  - WEB Server for management (based on IIS = Internet Information Services)
  - Distribution of subscription data over the DAPs.
  - Firmware Uploading to handsets
  - Collecting Subscription data
  - Low rate messaging Services
  - Controlling the IP DECT system in case there are Branch Office location.

Besides the items mentioned above, the DAP Controller software comes with a Configurator, to setup the IP DECT Configuration. 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, except for the following functions.

  - Business Mobility IP DECT configuration with branch offices.
  - Low Rate Messaging Services (LRMS).
  - Maintenance
  - Collecting diagnostic data

- IPLA in SV8300

  The IPLA blade in the SV8300 is the IP interface between the IP DECT system and the CPU in the SV8300. It also provides conversion from Time Division Multiple Access (TDM) to Voice Over IP and vise versa.

- 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 limited number of configuration settings. Note that the WEB browser must be Internet Explorer 6.0 or higher!

✎ *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, the or IPLA/CPU in the SV8300 sends a call setup message 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 and the other party (either an IP telephone or the IP-PADIPLA).

However, before you can establish a call, the handset must have been subscribed and registered in the SV8300.

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

SECTION 2 HANDSET SUBSCRIPTION/REGISTRATION

Before you can use a handset, the handset must be subscribed to the DECT system. Besides that the handset must be registered in the SV8300. Subscription requires manual intervention, registration is done automatically. Figure 2-2 Phases in the Subscription Process in the SV8300 Environment shows the phases in the subscription process in an SV8300 environment.

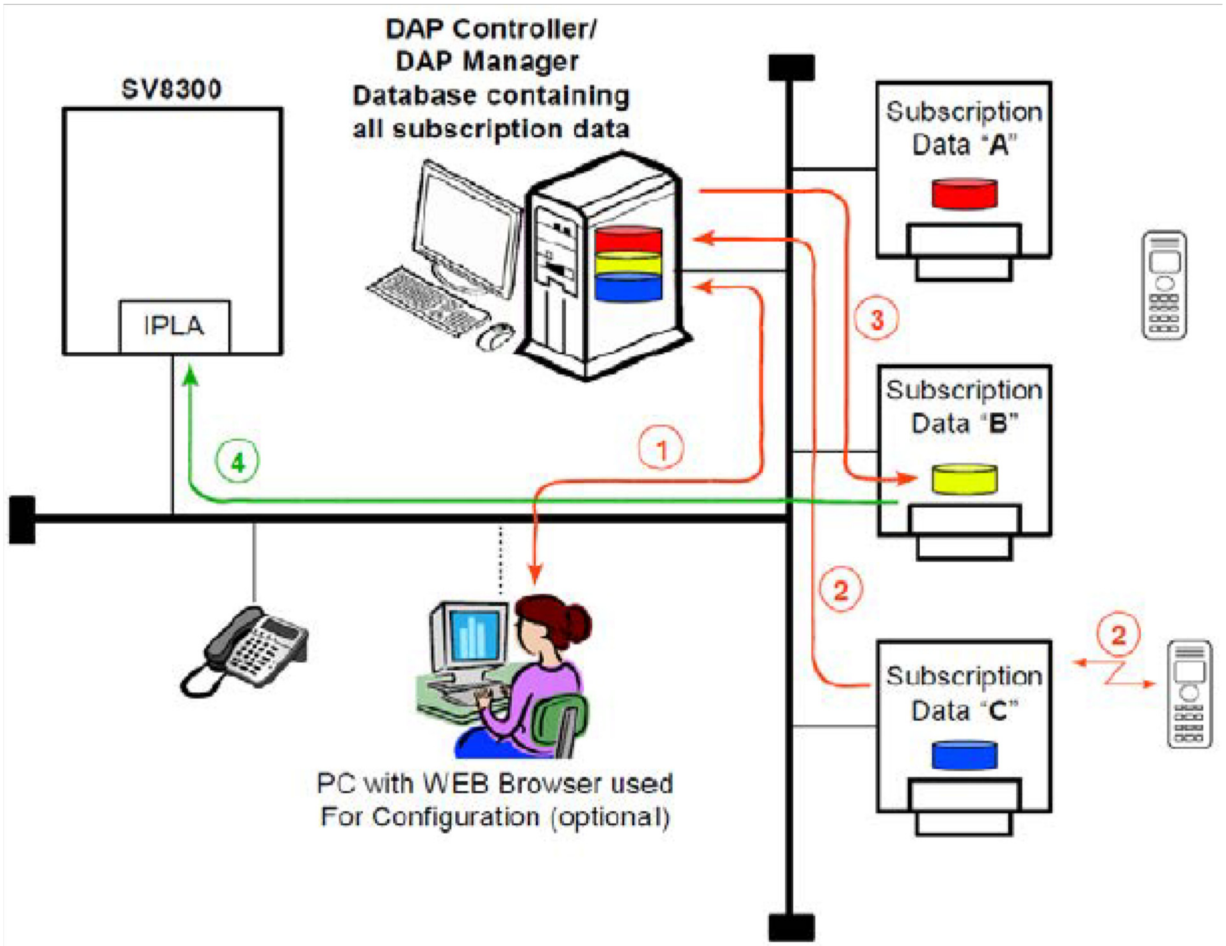


Figure 2-2 Phases in the Subscription Process in the SV8300 Environment

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.
2. The administrator "enables" a subscription, which means that the subscription process is started. The IP DECT System is now waiting for action from a handset.

3. 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.
4. The DAP Manager will distribute the subscription data to one of the DAPs. 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 DAP is 25.
   - Once a subscription record is stored into a DAP, it will normally not be moved to another DAP anymore. There are two exceptions on this: If you “Delete” a DAP manually from the DAPs list in the DECT Manager, the subscription records of that DAP will be distributed over the remaining DAPs. 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.
5. The DAP sends a Registration to the SV8300 using the Protims protocol.

After the subscriptions are executed, each DAP 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.

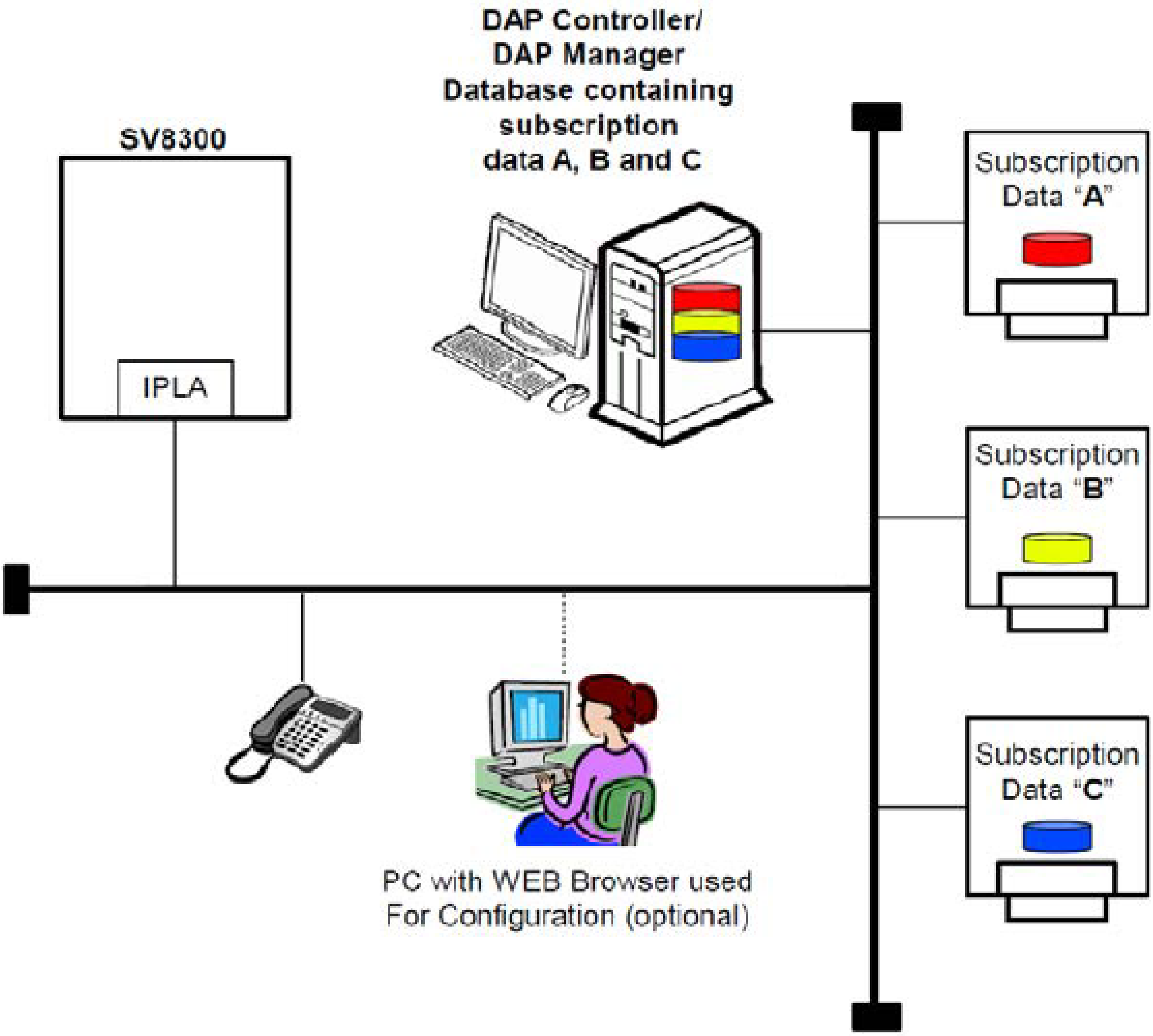


Figure 2-3 Subscription Locations (in SV8300 Environment)

SECTION 3 AUTOMATIC DISTRIBUTION WHEN A DAP IS DOWN

When a DAP goes down, the subscription records in that DAP are not accessible anymore, and therefore, the associated handsets cannot be used anymore. However, the subscription records of a broken DAP are automatically distributed over other DAPs after 10 minutes down time. This time is adjustable; the shortest time is 5 minutes.

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 that you can replace the faulty DAP with a new one, with moving the original subscriptions to the new DAP within those 10 minutes. This time is configurable.

SECTION 4 HANDSET REGISTRATION IN THE SV8300

DECT Handset registration means that a DECT Handset makes itself know to the SV8300. It establishes a relationship between a Station number in the SV8300 and a DECT handset number in the Business Mobility IP DECT system.

Note, that you cannot make a call with a DECT Handset if it is not properly registered!

A DECT extension is regarded as IP Dterm from the SV8300 point of view. A Dterm must register/report itself to the SV8300 to make itself known. The same is true for a DECT handset, however, this process is automated.

Immediately after a handset is subscribed to the Business Mobility IP DECT system, the DAP containing the subscription record sends login information to the SV8300 or in other words it reports/registers itself to the SV8300. The SV8300 receives the DECT handset extension number from the DAP and checks if there is a matching Station number. If there is a matching Station Number, the SV8300 establishes the relation between the DECT Handset and the Station number as if it is an IP Dterm. Now the SV8300 knows that the extension exists. (Note that the Station number must have been assigned before in the SV8300, via the same procedure as for an IP Dterm.)

SECTION 5 HANDOVER MECHANISM

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

In Figure 2-4 Call Connection Before Handover (in SV8300 Environment) the speech path is a peer-to-peer VoIP connection between the IP extension and a DAP.

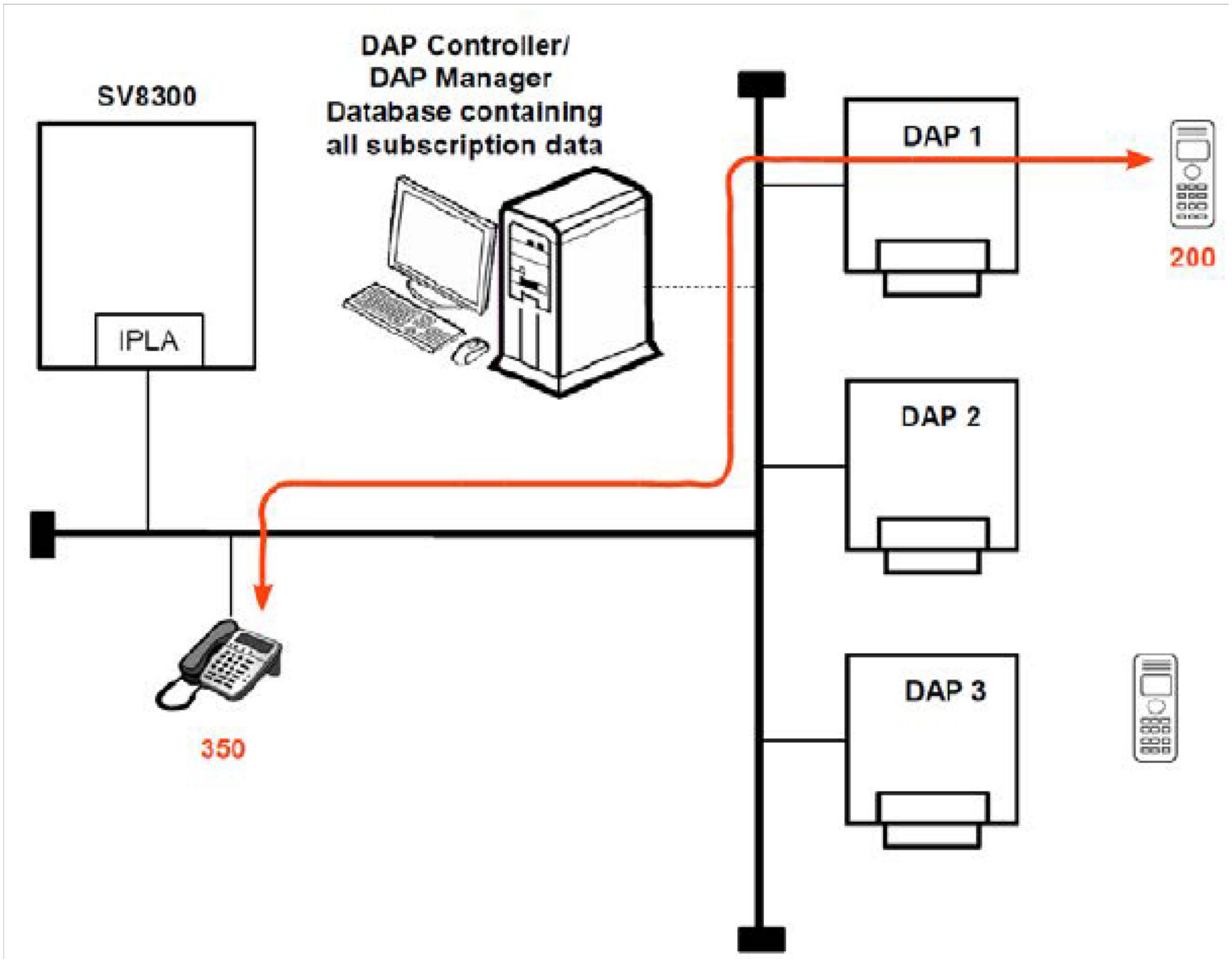


Figure 2-4 Call Connection Before Handover (in SV8300 Environment)

However, handset 200 moves from DAP 1 to DAP 2. Refer to Figure 2-5 Handover Action Started (in SV8300 Environment) on page 2-9. The handset searches for a better radio signal, and detects that the second DAP has a better signal. The handset issues a request for handover to the new DAP (DAP 2). However, the DAP 2 does not know where the existing voice connection to handset 200 resides so it issues a multicast request for searching previous connection to handset 200 over the network with DAPs. DAP 1 responds to this request because the call was initially be set up via this DAP.

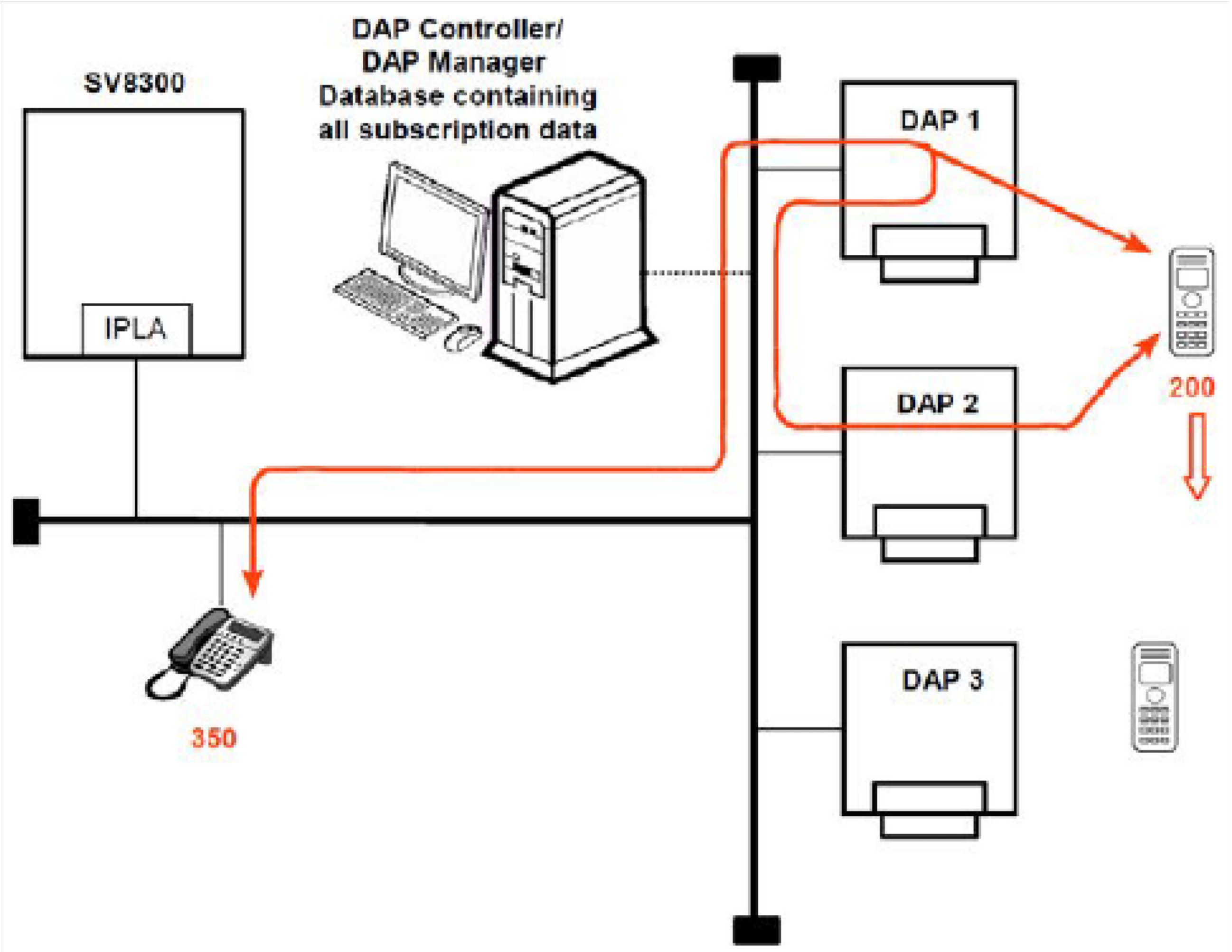


Figure 2-5 Handover Action Started (in SV8300 Environment)

Now the connection is *copied* from DAP 1 to DAP 2. The original/first DAP will release the *radio connection* to the handset and the new connection remains in place. Refer to Figure 2-6 Handover Taken Place, New Connection Active (in SV8300 Environment) on page 2-10. Note that the original connection is not removed from the DAP 1, but this DAP "relays" the connection to the second DAP. DAP 1 cannot release the IP voice connection, because the IP voice connection between the IP extension (350) and DAP 1 is established, based on a combination of sockets. This combination is fixed during the connection.

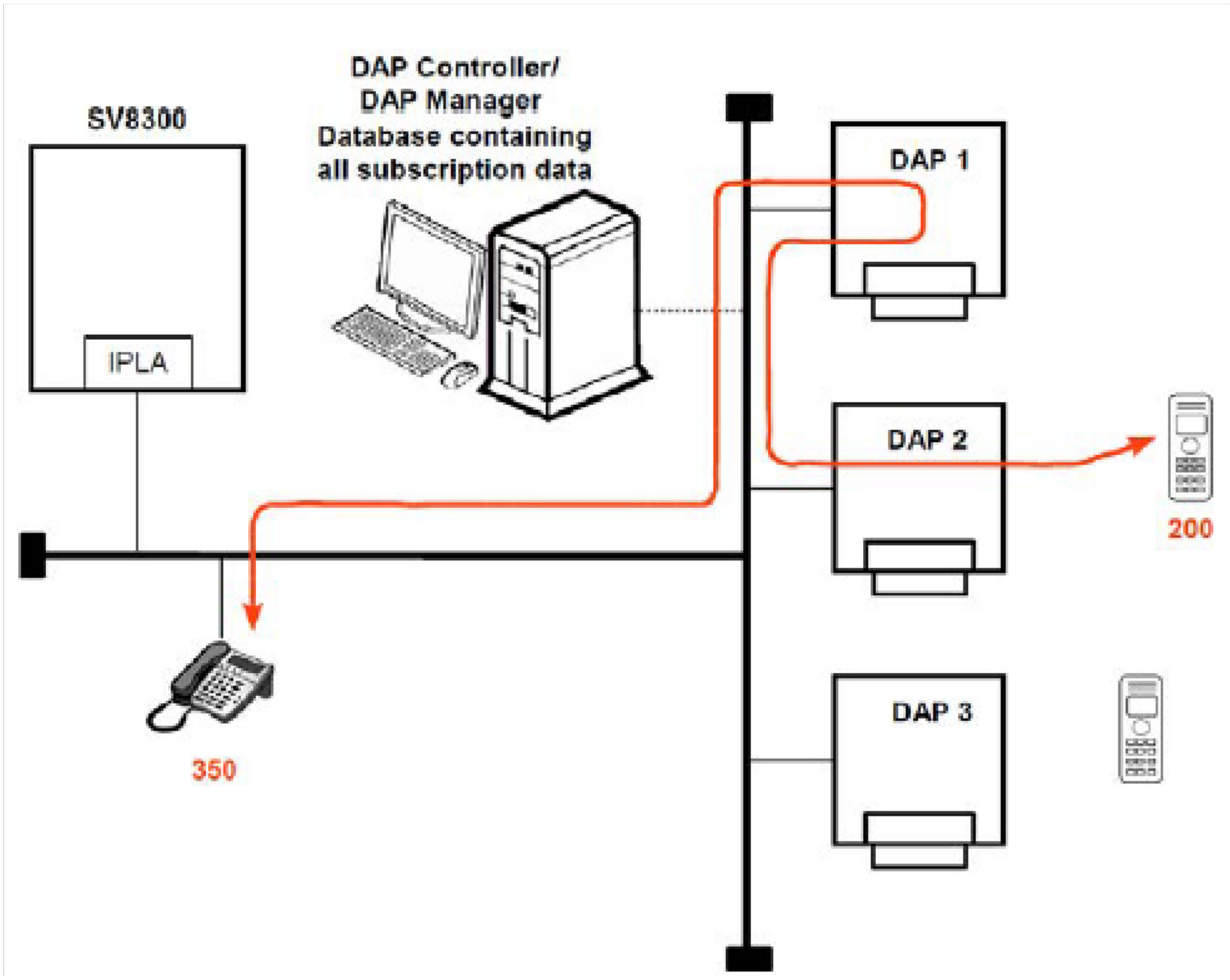


Figure 2-6 Handover Taken Place, New Connection Active (in SV8300 Environment)

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

SECTION 6 IS DAP MANAGER REQUIRED?

The DAP Manager is not required for call handling. A simple Business Mobility IP DECT system will therefore look like the picture shown in Figure 2-7 Simple Business Mobility IP DECT Configuration without DAP Manager (in 8300 Environment).

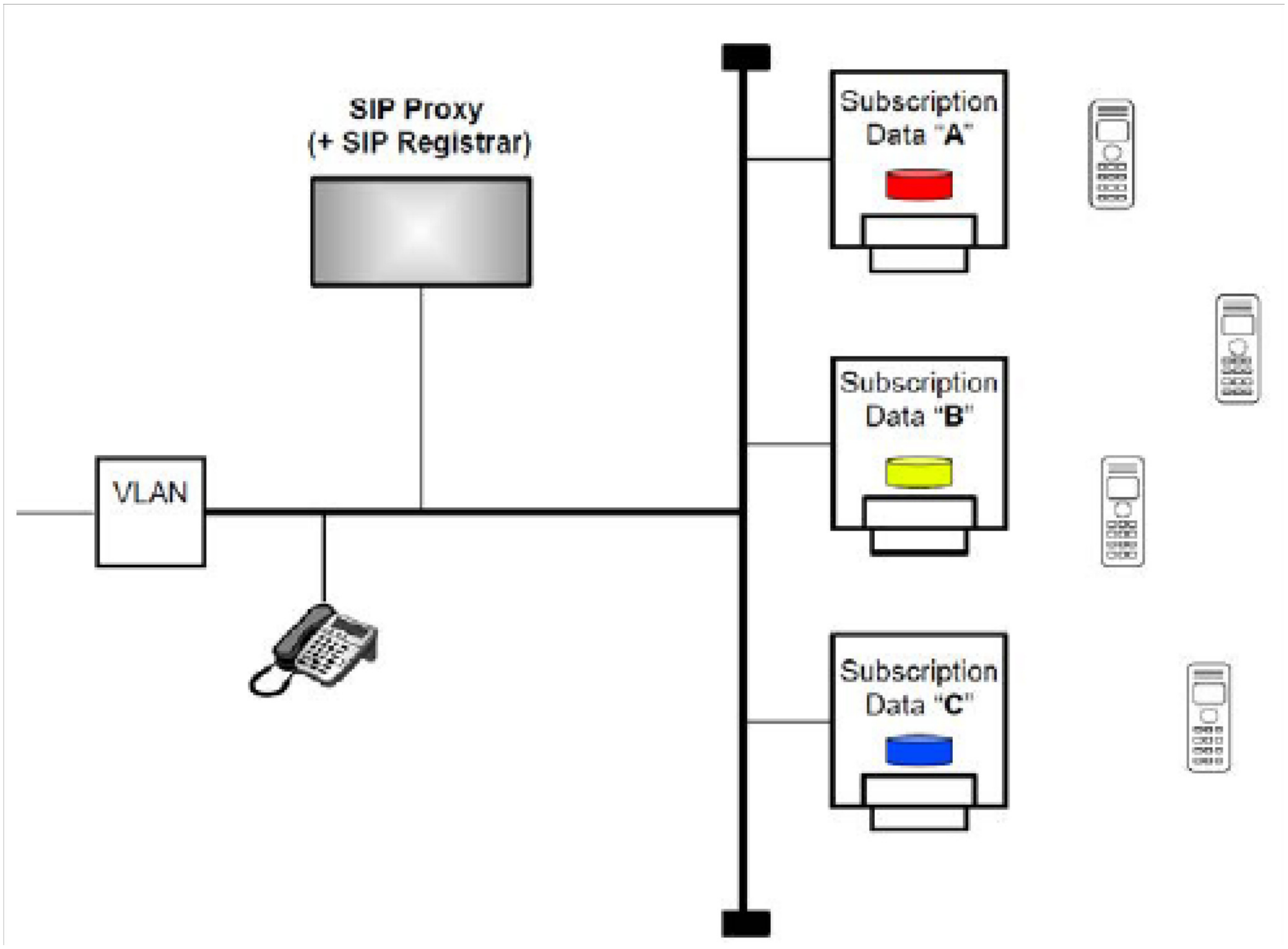


Figure 2-7 Simple Business Mobility IP DECT Configuration without DAP Manager (in 8300 Environment)

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

When you replace a DAP 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.

✎ *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.

❍ Sending alarm e-mails or sending SNMP traps

The DAP Controller is capable of sending an e-mail when a DAP goes down, or a predefined threshold of channel occupation is exceeded or when the DDS service in the DAP Controller goes down. Also it can send an SNMP trap in case of one of these events (for more info, consult the Advanced Data manual).

❍ Collecting diagnostic data)

The DAP Controller can collect detailed diagnostic and performance data. This automatically enabled when the DAP Controller is up and running.

SECTION 7 RADIO SYNCHRONIZATION

7.1 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.

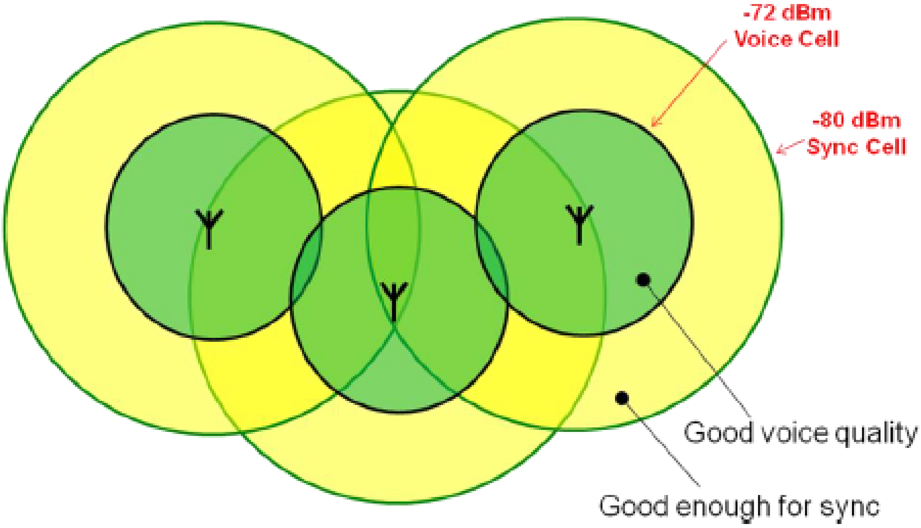


Figure 2-8 Radio Synchronization

A DAP (Radio) cell can be seen theoretically as a circle around the DAP. Referring to Figure 2-8 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).

7.2 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.

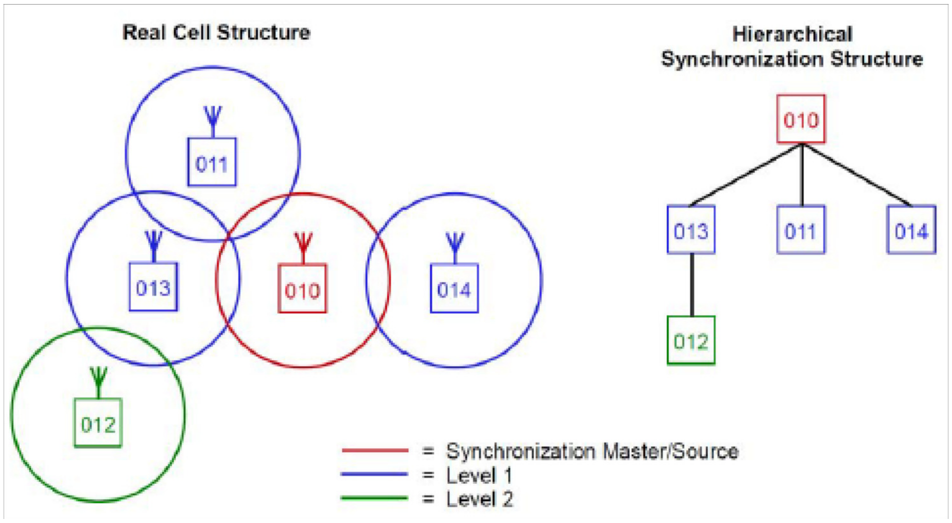

Real Cell Structure
011
013
010
014
012
Hierarchical Synchronization Structure
010
013
011
014
012
= Synchronization Master/Source
= Level 1
= Level 2

Figure 2-9 Synchronization Structure

Referring to Figure 2-9 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:

❍ 010

  The automatic assignment of RPNs starts at 010 when the IP DECT system is setup as Distributed DAP Controller. Manually assigned numbers can be in the range 000 . . . 00F.

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

7.3 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. Refer to Figure 2-10 Signal Strength Considerations.

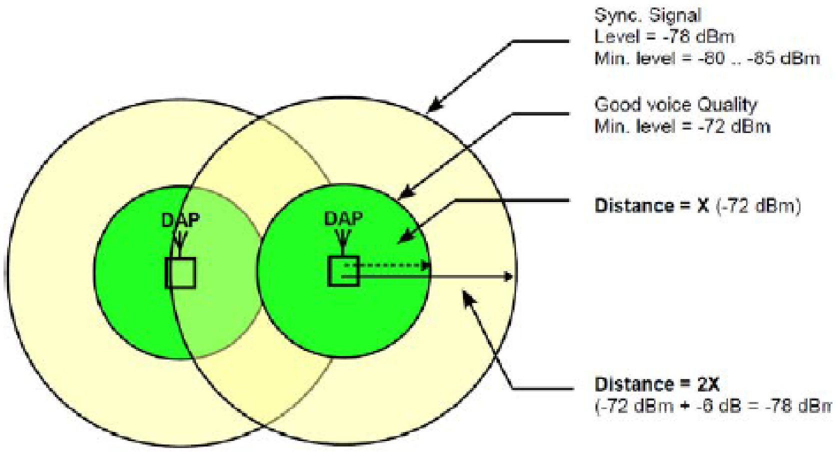


Figure 2-10 Signal Strength Considerations

- 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 acceptable).

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

SECTION 8 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 and adapt the port number range to your wishes.

8.1 DAP Characteristics

8.1.1 General

The following DAP types exist:

❒ AP300 Series, from November 2010 till June 2012

❒ AP400 Series, current AP400 version (from June 2012 onwards)

All of these DAPs share common characteristics. These characteristics are described next.

Type dependant characteristics are given in the following subsections.

8.1.2 Common Characteristics

Features

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

❒ 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.

❒ DAP Software downloadable.

Capacity

❒ Max. number of simultaneous calls: 12
Please note that this maximum number of calls is only applicable when the DAP is synchronization source/master. If the DAP is not the synchronization master, the maximum number of simultaneous calls is 11. Also note that the maximum number of simultaneous calls per DAP is also limited by licenses in a licensed version of IP DECT.

❒ Max. number of simultaneous relay calls: 12

❒ Max. number of DAPs per network: 256

❒ Max. number of DAPs with DAPs in Branch Offices: 750

❒ Max. number of simultaneous calls per network with 256 DAPs: 11 x 255 +12 =2817. This depends on the network configuration and available DAP channels.

IP Interface Characteristics

❒ 100 Base-T Full duplex, full support of 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: -25º to +55º Celsius

❒ Operational temperature: 0º to +40º Celsius

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

8.1.3 AP300 (not available anymore)

The AP300 is described in the AP300 Customer Engineer Manual. Please consult the AP300 Installation Manual for more information:

8.1.4 AP300E (not available anymore)

The AP300E is the same as the AP300 but allows you to connect external antenna’s. When used in an AP200S configuration it does not support G.729.

8.1.5 AP400 (Currently available)

This is the generic AP400, NEC branded.

SECTION 9 AP300/AP400 POWER PROVISION

The AP300/AP400 is powered via PoE. It supports Class detection. The AP300/AP400 is a Class 2 device when used on PoE Switches. For more information consult the ***AP300/AP400 Installation Manual***.

SECTION 10 MORE THAN 256 DAPS

IP DECT allows you to setup an IP DECT System with more than 256 DAPs. There are two possibilities.

❍ System with Branch offices

Maximum number of DAPs per *IP DECT system* with Branch Offices is 750. Per Main site or Branch Office, the maximum number of DAPs is 256.
This configuration can be setup with the standard IP DECT installation.

❍ One IP DECT Cluster with seamless handover

Maximum number of DAPs per IP DECT System is 750, all on one location (Main Site). Please note that this type of system is possible on “project” base and is not part of the standard installation. For more information, please contact your IP DECT supplier.

SECTION 11 RPN NUMBER RANGES PER BRANCH OFFICE

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 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`.

Licenses

3

SECTION 1 GENERAL

From IP DECT Release 6.0 onwards, licenses are introduced. All licenses has to be entered into the DAP Controller.

SECTION 2 FUNCTIONAL LICENSES

The following functional Licenses are available:

- Maximum number of DAPs

  You must have a license for the number of DAPs. Please note that the total number of DAPs that you specify in this license, is the sum of license unities of 10 and 50 licences. E.g. when you have 70 DAPs, you need one license for 50 DAPs and 2 licenses for 10 DAPs. (1x50) + (2x10).

  The maximum number of DAPs in a certain configuration is determined by the DAP types. This can be:

  - 256 (type: AP400)
  - 750 (type: AP400) in case you also have the “Big Projects License”.

- For Future use: CAT-iq Data Licenses

  Please note that this license is not yet available and is planned for future use.

- Redundancy Central Site

  This license is required to have a redundant DAP Controller configuration in the Central site.

- Branch Office Survivability

  You need this license to allow Local DAP Controllers in one or more Branch Office locations.

- Software Upgrade Allowance

  To upgrade a Release 6.0 to a higher version, you need an Upgrade License. When the license is activated, *it provides a window of one month to install a higher version*.

  Please note that this license is made dependant on the system size. The steps are:

  - 10 DAPs
  - 50 DAPs
  - 100 DAPs
  - 256 DAPs

  Please note that the total number of DAPs is the sum of the licences. E.g. when you have 70 DAPs, you need one license for 50 DAPs and 2 licenses for 10 DAPs. (1x50) + (2x10).

- Messaging License.

  Messaging is licensed in the DMLS and in the DAP Controller. Licenses are exchangeable between the DMLS and the DAP Controller, so if you have a licence for DMLS, you can import that license into the DAP Controller and vice versa. In the DAP Controller, the license is related to the number of DAPs in the system and should be the same number as specified in the first item in this list of licenses. For more info on the Messaging License refer to Section 6 DMLS Licenses.

- Location Detection License, on top of the Messaging License.

  This license is available on the DMLS and also in the DAP Controller. Licenses are exchangeable between the DMLS and the DAP Controller, so if you have a licence for DMLS Location Detection, you can import that license into the DAP Controller and vice versa. The Location detection license is applicable for single point and multipoint on the DMLS. When you order the license, you must order it on top of the Messaging License. In the DAP Controller, the license is related to the number of DAPs in the system and should be the same number as specified in the first item in this list of licenses.

SECTION 3 PROJECT BASED LICENSES

There are a number of licenses that are only available on project base. Special support is required.

- Large configuration License – Big Projects License

  This license is required when your IP DECT system consists of more than 256 DAPs in one cluster with seamless handover. This license requires a RAP (Risk Assessment Procedure) and includes on-site support.

- Dual Band Mode – Cruise line license.

  This is a special license for IP DECT installations on cruise ships. This license requires a RAP (Risk Assessment Procedure) and includes on-site support.

- Reflection Cancelling.

  This is a special license for IP DECT in environments with a lot of reflections. This license requires a RAP (Risk Assessment Procedure) and includes on-site support.

SECTION 4 SYSTEM ASSURANCE LICENSE

The system assurance license is a license to allow software upgrading from Release 6.0 to higher versions. The license is based on the number of DAPs. The license is already mentioned in Section 2 Functional Licenses .

Note that there are two ways to get the Software Upgrade License:

- By means of the NEC ordering tool.
- By means of becoming a member of the System Assurance Program.

When the license is activated, *it provides a window of one month to install a higher version*.

SECTION 5 FROM RELEASE 5 TO RELEASE 6

IP DECT Release 5 was license free, in IP DECT Release 6.0 and higher you need license for the various functions and features.

When you upgrade from Release 5 to Release 6, the system will automatically generate a license file with all the features that your system had in Release 5. So, you do not need to have a license prior to upgrading.

This license has the following characteristics:

- It will cover all existing system configuration.
- It is Free of Charge.

You must send the license file that is generated to NEC for registration.

For new features, you must order a new license.

SECTION 6 DMLS LICENSES

From Release 6 onwards, the DMLS is licensed in the DAP Controller License mechanism. You don’t need a dedicated license for the DMLS anymore. The license is based on the number of DAPs.

In the DAP Controller, there is a license for “DECT Messaging” and for “DECT Location detection”. The Location Detection license is on top of the Messaging License.

There are two options to enable the DMLS Messaging/Location feature:

❍ DMLS License String

When you already have a DMLS license string, you can use that license in the DMLS and you can import that license string into the DAP Controller License mechanism by means of the button “Add DMLS”. (Refer to 13.3 License Information Window on page 9-44.). Please note that this is applicable for the Messaging license as well as for the Location license.

❍ DAP Controller License for Messaging and perhaps also Location detection.

When you have a license for Messaging or Location detection on the DAP Controller, you can synchronize the DMLS application with it. The DMLS can retrieve the license data from the DAP Controller license mechanism by means of one button.

When you have a “CTI license” for Messaging on the DAP Controller, you do not need to have the Messaging license in the DAP Controller.

SECTION 7 WHERE TO ENTER AND TO FIND THE LICENSE DATA?

After ordering DECT licenses, you will receive a text file with the license data. You should import that file into the DAP Configurator. In the DAP Configurator, you can also read out the license information.

For more information, consult the applicable sections in the chapter that describes the DAP Configurator Settings:

❍ 13.1 Install a new License File on page 9-42

❍ 13.2 Reading out the Licenses on page 9-43

❍ 13.3 License Information Window on page 9-44

Network Configurations 4

SECTION 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 information about the system behavior over a router, in chapter “System Behavior over Router”.

✎ *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”.

SECTION 2 SIMPLE CONFIGURATION

2.1 Network Configuration

Figure 4-1 Example of a Simple IP DECT Network Configuration on page 4-2 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).

The general characteristics of a simple configuration are as follows:

- Seamless handover is supported between all DAPs.

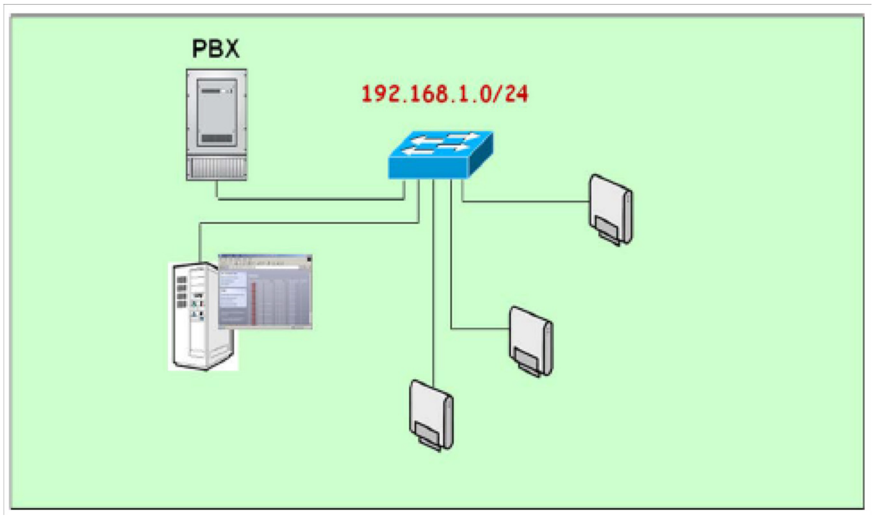
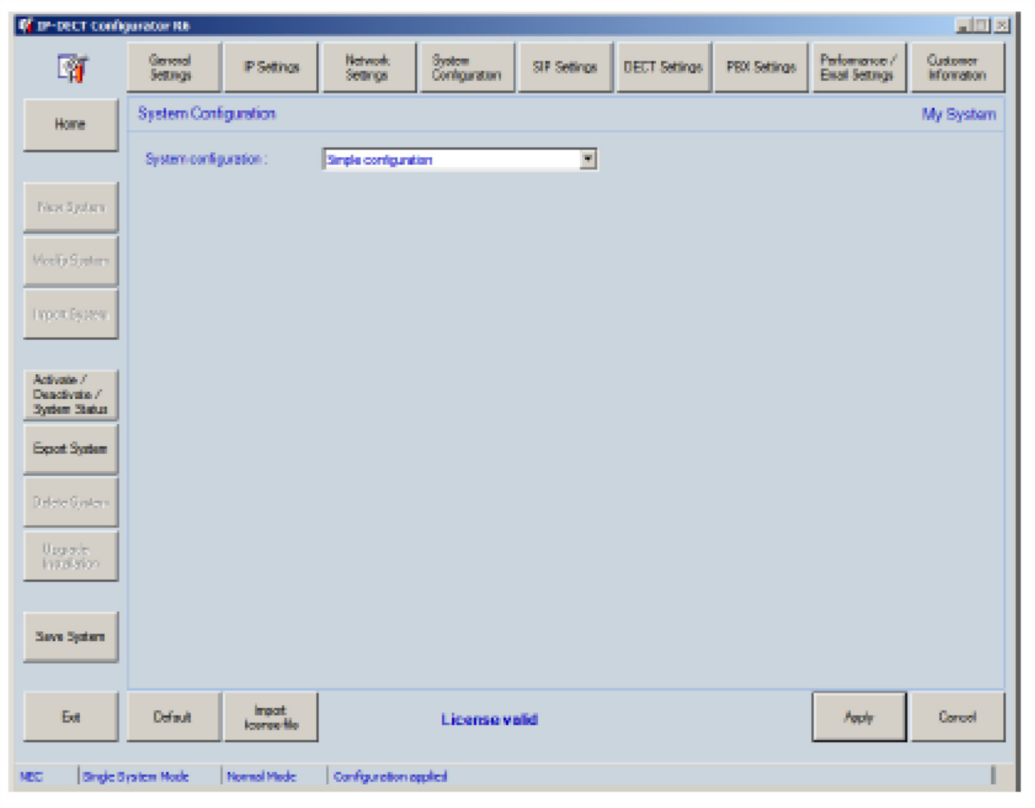


Figure 4-1 Example of a Simple IP DECT Network Configuration

SECTION 3 SETTINGS IN DAP CONFIGURATOR

The DAP Configurator is described in Configuration - DAP Configurator Tool. However, in this section you will find an example of a setup for a simple configuration.



System Configuration

My System

System configuration : Simple configuration

License valid

NEC | Single System Mode | Normal Mode | Configuration applied

Figure 4-2 IP DECT System Simple Configuration Screen

SECTION 4 BRANCH OFFICE SOLUTION

4.1 Network Configuration

Figure 4-3 Example of an IP DECT Configuration With a Branch Office 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.

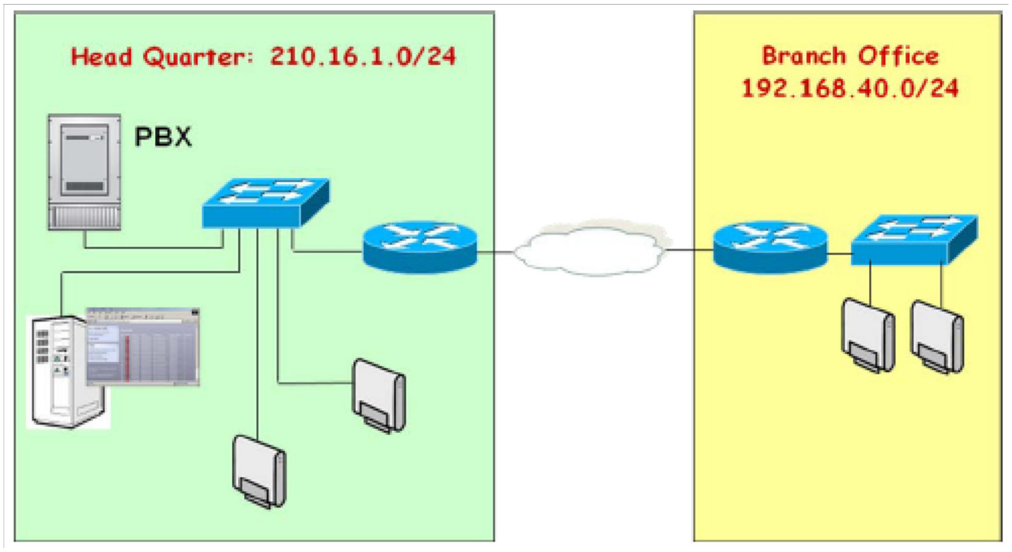


Figure 4-3 Example of an IP DECT Configuration With a Branch Office

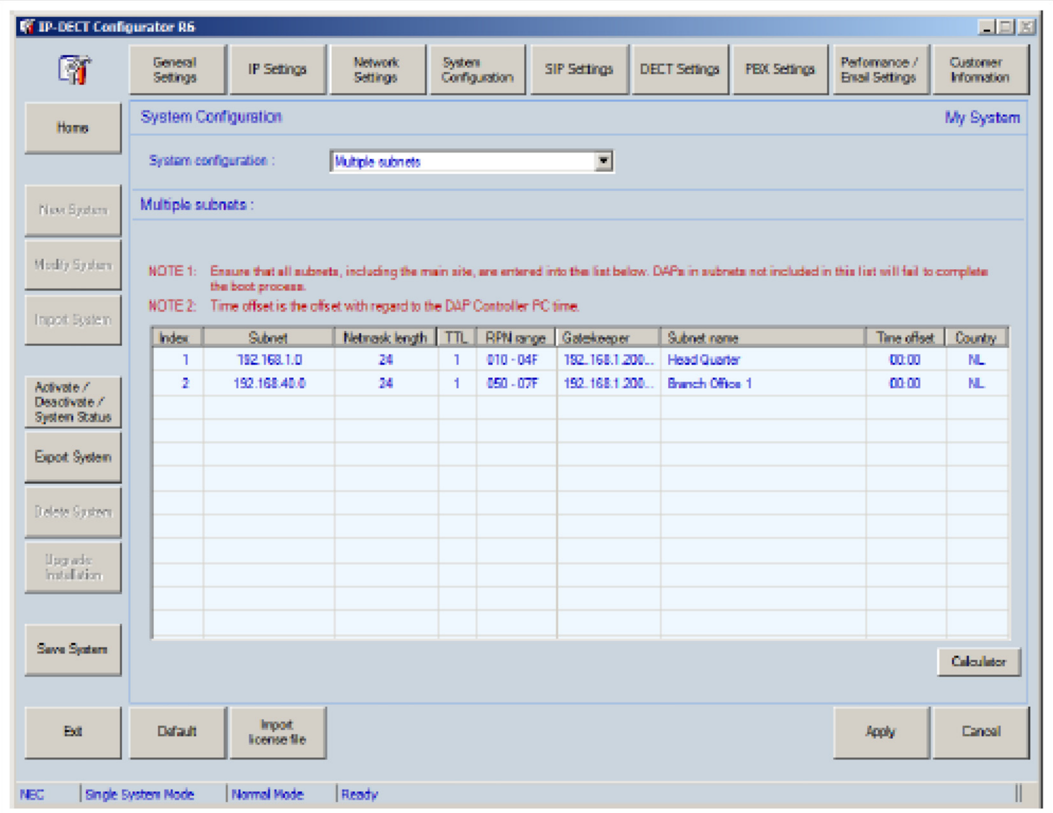
The general characteristics of an IP DECT configuration with Branch Offices are as follows:

- 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.

4.2 Settings in DAP Configurator

Refer to Figure 4-4 Branch Office Settings for configuring the Branch Office settings.



System Configuration My System

System configuration : Multiple subnets

Multiple subnets :

NOTE 1: Ensure that all subnets, including the main site, are entered into the list below. DAPs in subnets not included in this list will fail to complete the boot process.

NOTE 2: Time offset is the offset with regard to the DAP Controller PC time.

Index	Subnet	Netmask length	TTL	RPN range	Gatekeeper	Subnet name	Time offset	Country
1	192.168.1.0	24	1	010 - 04F	192.168.1.200...	Head Quarter	00:00	NL
2	192.168.40.0	24	1	050 - 07F	192.168.1.200...	Branch Office 1	00:00	NL

Figure 4-4 Branch Office Settings

SECTION 5 ROUTED HEAD QUARTER

5.1 Network Configuration

Figure 4-5 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.

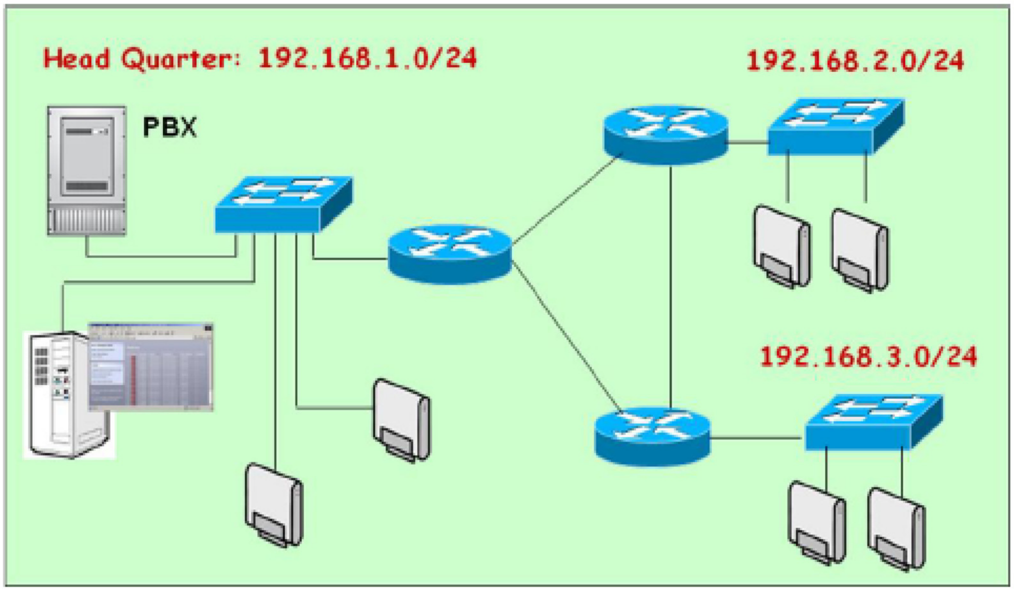


Figure 4-5 Example of an IP DECT Routed Head Quarter Configuration

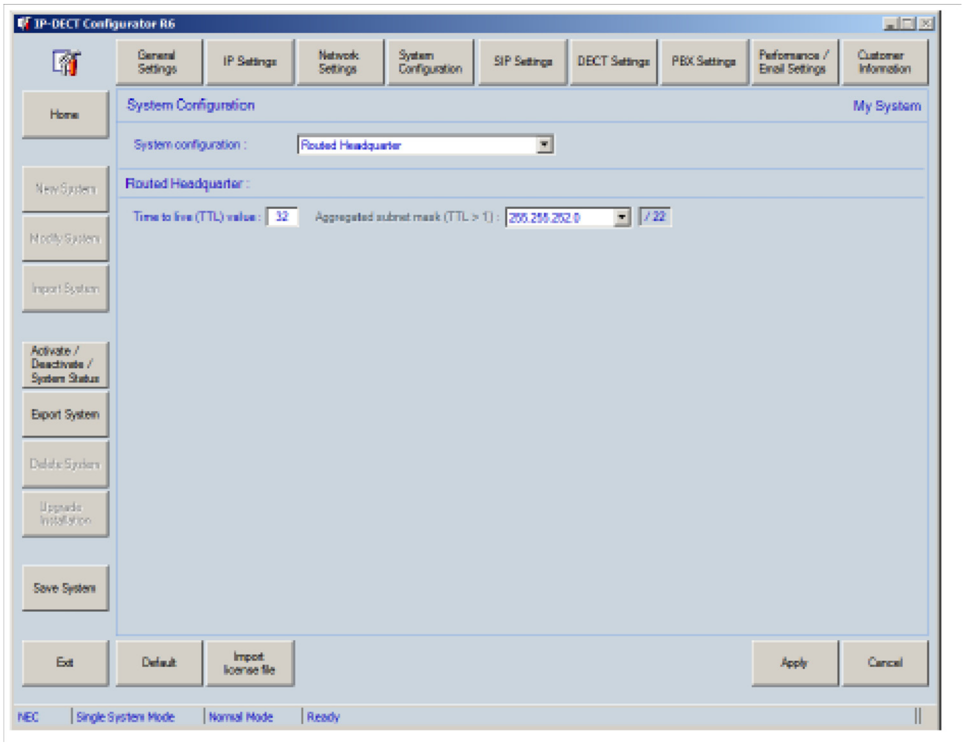
The general characteristics of an IP DECT Routed Head Quarter configuration are as follows:

- ❍ 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. 255.255.252.0) for up to four subnets as in the previous example.

5.2 Settings in DAP Configurator

The DAP Configurator is described in Configuration - DAP Configurator Tool However, in this section you will find an example of a setup for a Branch Office configuration.



IP-DECT Configurator R6

System Configuration

My System

System configuration : Routed Headquarter

Routed Headquarter :

Time to live (TTL) value : 32 Aggregated subnet mask (TTL > 1) : 255.255.252.0 / 22

Figure 4-6 Routed Headquarter System Configuration Screen

Please note that the TTL is the TTL value for IP Multicast, which must allow Multicast traffic over the Routers in the Routed Head Quarter. That should be higher than 1, but based on the TTL settings in the Router, it is advised to use a TTL value of 32.

Please note that the *Aggregated* subnet mask is the subnet mask that includes all three networks in the Head Quarter. So, this is NOT the IP subnet mask on the Network adaptors on the IP Network segments. Please do not mix up the *Aggregated* Subnet Mask and the normal IP Subnet mask.

SECTION 6 ROUTED HEAD QUARTER WITH BRANCH OFFICES

6.1 Network Configuration

Figure 4-7 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 throughput LAN).

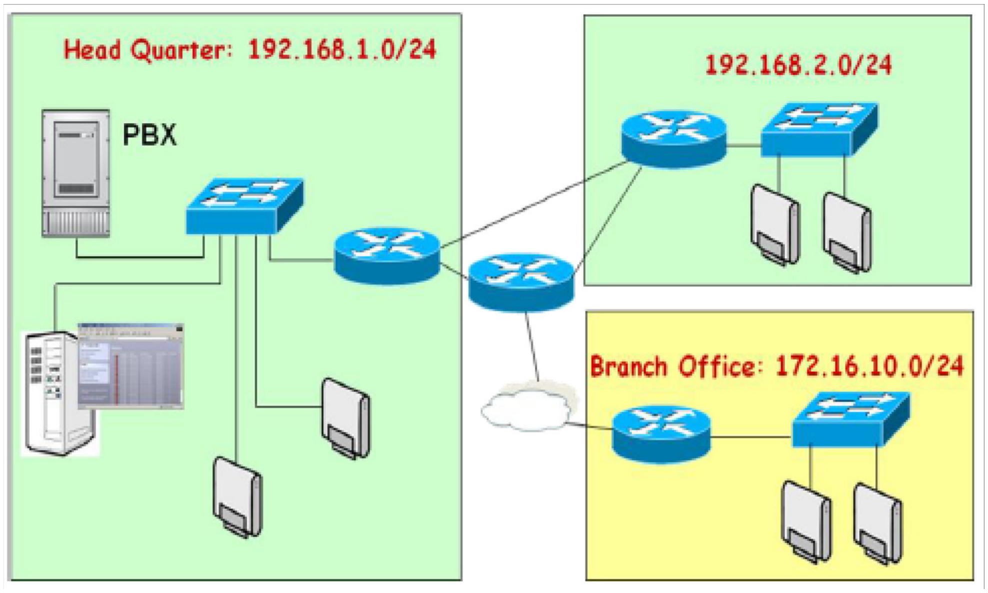


Figure 4-7 Example of an IP DECT Routed Head Quarter Configuration with Branch Office

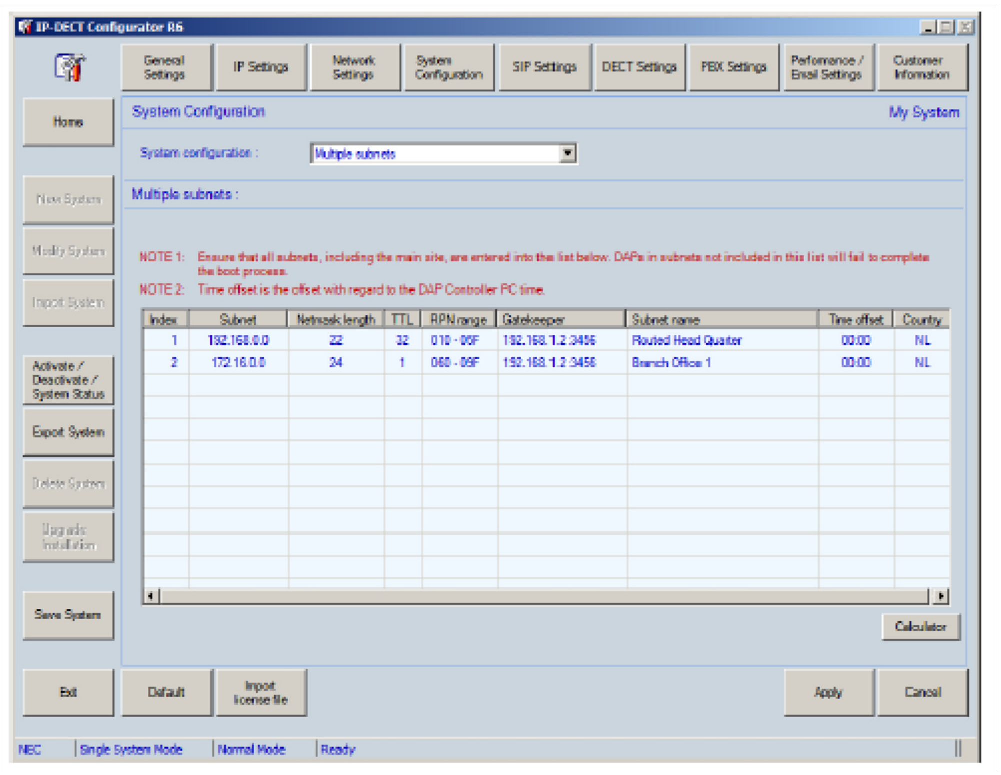
The general characteristics of an IP DECT Routed Head Quarter configuration with Branch Office(s) are as follows:

- 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. 255.255.252.0 for in this example).

6.2 Settings in the DAP Configurator

Figure 4-8 Example of Setup for a Routed Head Quarter with Branch Office Configuration shows an example of a setup for a Routed Head Quarter with Branch Office configuration.



System Configuration — My System

System configuration : Multiple subnets

Multiple subnets :

NOTE 1: Ensure that all subnets, including the main site, are entered into the list below. DAPs in subnets not included in this list will fail to complete the boot process.

NOTE 2: Time offset is the offset with regard to the DAP Controller PC time.

Index	Subnet	Netmask length	TTL	RPN range	Gatekeeper	Subnet name	Time offset	Country
1	192.168.0.0	22	32	010 - 05F	192.168.1.2:3456	Routed Head Quater	00:00	NL
2	172.16.0.0	24	1	060 - 09F	192.168.1.2:3456	Branch Office 1	00:00	NL

Figure 4-8 Example of Setup for a Routed Head Quarter with Branch Office Configuration

SECTION 7 ROUTED HEAD QUARTER WITH ROUTED BRANCH OFFICES

7.1 Network Configuration

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 throughput LAN).

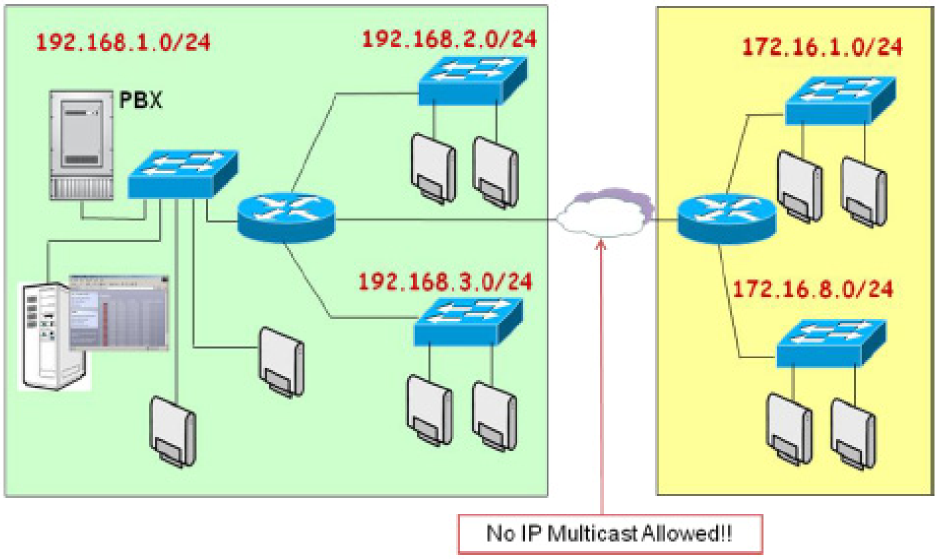


Figure 4-9 Example of an IP DECT Routed Head Quarter Configuration With a Routed Branch Office

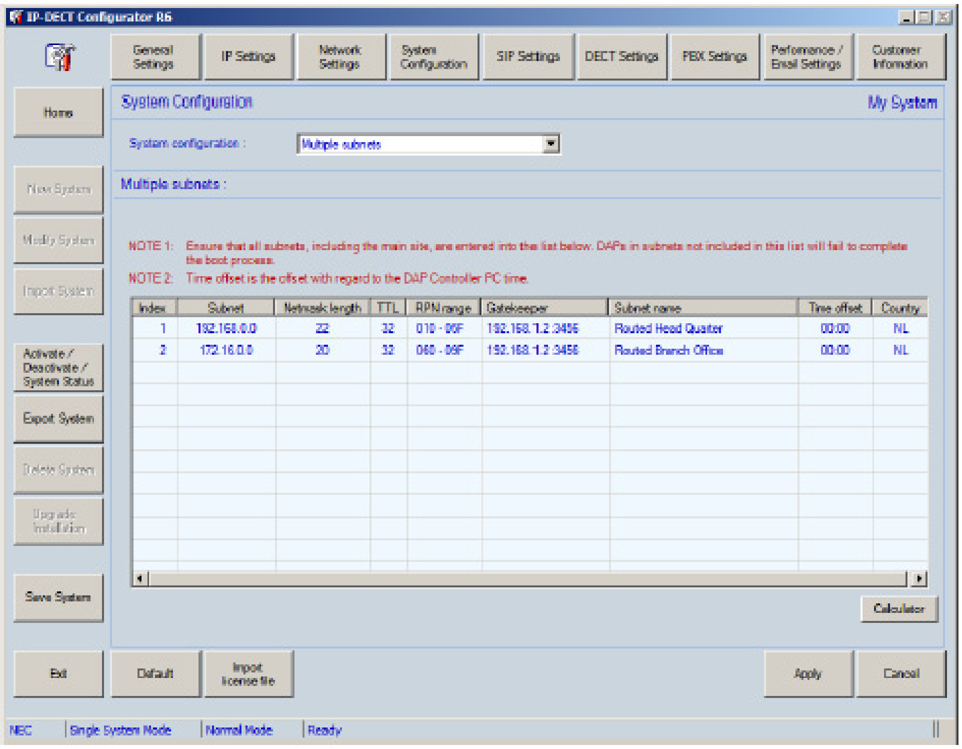
The general characteristics of an IP DECT Routed Head Quarter configuration with Routed Branch office are as follows:

- 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 Routed Branch Offices.
- In the Routed Head Quarter part, all characteristics which are mentioned previously for the Routed Head Quarter are applicable.
- In the Routed Branch Office part, all characteristics which are mentioned previously for the Routed Head Quarter are applicable, except for that the Routed Branch Office must be in different subnets than the Routed Head Quarter.

- In the Head Quarter the Multicast TTL >1, and in the branch Office the Multicast TTL >1(!).
- Edge Router, connected to the WAN, should not forward Multicast packages to the WAN.
- The Routers between the Routed Head Quarter and the Routed Branch Office should block Multicast!
- Full support of seamless handover between all DAPs in the Head Quarters configuration with the subnet. Full support of hand over in the Routed Branch Office. No handover between the Routed Head Quarter and the Routed Branch Office.
- Routers in the Head Quarter must support IP Multicast routing.
- Routers in the Routed Branch Office should 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 Aggregated subnet mask that is needed to cover all Head Quarters subnetworks (e.g. 255.255.252.0 for in this example.). Also in the Routed Branch Office, you must calculate the Aggregated subnet mask that covers all subnets in the Routed Branch Office.

7.2 Settings in the DAP Configurator

Figure 4-10 Routed Head Quarter with Routed Branch Office Configuration show an example of a setup for a Routed Head Quarter with Routed Branch Office configuration.



System Configuration

My System

System configuration : Multiple subnets

Multiple subnets :

NOTE 1: Ensure that all subnets, including the main site, are entered into the list below. DAPs in subnets not included in this list will fail to complete the boot process.

NOTE 2: Time offset is the offset with regard to the DAP Controller PC time.

Index	Subnet	Netmask length	TTL	RPN range	Gatekeeper	Subnet name	Time offset	Country
1	192.168.0.0	22	32	010 - 05F	192.168.1.2:3456	Routed Head Quater	00:00	NL
2	172.16.0.0	20	32	060 - 09F	192.168.1.2:3456	Routed Branch Office	00:00	NL

Figure 4-10 Routed Head Quarter with Routed Branch Office Configuration

✎ The Netmask Length in both items in the screenshot above is the Aggregated Subnet Mask, not the real subnet mask.

DAP Installation Items

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

SECTION 2 DAP POWER PROVISION

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

The following overview gives the specifications of the PoE.

- Voltage at the DAP: minimum 36 Volts, maximum 57 Volts.
- Connector: Standard RJ45 connector, using the spare wires pins (wires). Refer to Figure 5-1 RJ45 Pinout.
- Maximum cable length: **100 meters**.

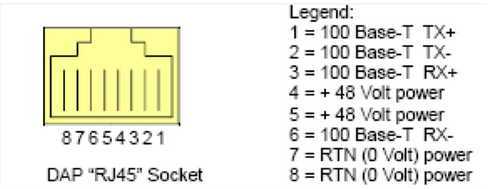


Figure 5-1 RJ45 Pinout

SECTION 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.

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).

   ✎ ***You must enable option 67 in the DHCP server whether you fill in a file name or not. If you do not fill in a file name, the DAP will try to upload the default configuration file name dapcfg.txt. If you fill in a file name in option 67, the DAP will upload the configuration file name that you have entered here. It is strongly recommended to leave the file name field blank.***

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.

✎ 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.

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.

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.

✎ 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. Refer to Section 2 Installing the DAP Controller Release 6 on page 7-1.

✎ Do not use the TFTP Server that comes with the DAP Controller for permanent use. The TFTP Server is included in the DAP Controller software, in order to allow you to setup a system easily, without DAP Controller permanently connected. In a customer network with the DAP Manager permanently connected, please use the TFTP server that the IT Manager recommends you to use.

3.3 Operation without DHCP or TFTP Server

If your DHCP server and or TFTP server is not permanently connected, you can store the IP address and the configuration file in the DAPS in Flash memory. Note that the firmware is always 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 Configuration in the boot options in the DAP Configurator screen. Refer to Section 3 IP Settings on page 9-3.

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 Configuration in the boot options in the DAP Configurator screen. Refer to Section 3 IP Settings on page 9-3.

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.

✎ 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 “Replace” 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.

3.4 Using other DHCP and/or TFTP 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 3.1 DHCP Server on page 5-2. 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 start 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.

✎ *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.*

Preparing Your DAP Manager PC

6

SECTION 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

❍ 1 GB RAM or more

❍ DVD-ROM drive

❍ 2GB hard disk space free

SECTION 2 SOFTWARE REQUIREMENTS

2.1 Operating System

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

❍ Windows 2003 SP2 or Windows 2003 Rel.2.

❍ Windows XP Professional, SP2/SP3.

❍ Windows 7 (not the Home version!)

❍ Windows 2008 SP2

❍ Windows 2008 R2

✎ 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 your IP DECT Supplier, and clearly indicate which MS Windows version is used and the nature of the problem.

2.2 IIS and Internet Explorer

Besides the operating system, the Windows WEB server, called IIS (Internet Information Services) is required. *However, during installation, IIS is automatically installed*.

When you install the DAP Controller software under Windows XP or Windows 2003, the system may ask for the Operating System CD-ROM/DVD-ROM.

✎ On the client computer, you must use Internet Explorer 6.0 or higher to view the DECT Manager WEB pages.

2.3 .NET Framework

The DAP Controller software requires .NET Framework 4.0. *However, this is automatically installed when installing the DAP Controller software.*

If there is already another version of .NET Framework on your PC, it does not do any harm. .NET Framework versions can co-exist.

2.4 DHCP Server and TFTP Server

❍ DHCP Server.

A DHCP Server is required in the network. However, the DAP Controller software Release 5 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.

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 a default gateway/router address in the DHCP server, which is within the subnet address range of the DAPs.

✎ *You should use the built-in DHCP server that comes with the DAP Controller only in very small installations (< 10 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. It is recommended to use the built-in TFTP server only in small installations (< 20 DAPs). For larger installations you should use a professional TFTP server.

2.5 Virtualization

The DAP Controller Release 6 supports virtualization on VMWare and Xen.

The Virtual Machine system should meet the requirements for a non virtualized server. If the network connection on the virtual machine is shared with another virtual machine or the Host, make sure that there is sufficient bandwidth available for the DAP Controller Virtual Machine.

2.6 Marathon Fault Tolerancy

Marathon software with the EverRun® software and Citrix XenServer can be used to provide fault tolerance on various software applications. IP DECT Release 6 supports working on a Marathon platform, to provide fault tolerance.

For more information on the Marathon software, please consult the NEC Unified web page.

Please note, that IP DECT supports Redundancy on the DAP Controller, without Marathon. Refer to Chapter 15 DAP Controller Redundancy.

THIS PAGE INTENTIONALLY LEFT BLANK

Installing - The DAP Controller/Manager 7

SECTION 1 PRECONDITIONS

Make sure that you have decided which DHCP Server you are going to use. Also make sure that you have decided which TFTP server you are going to use.

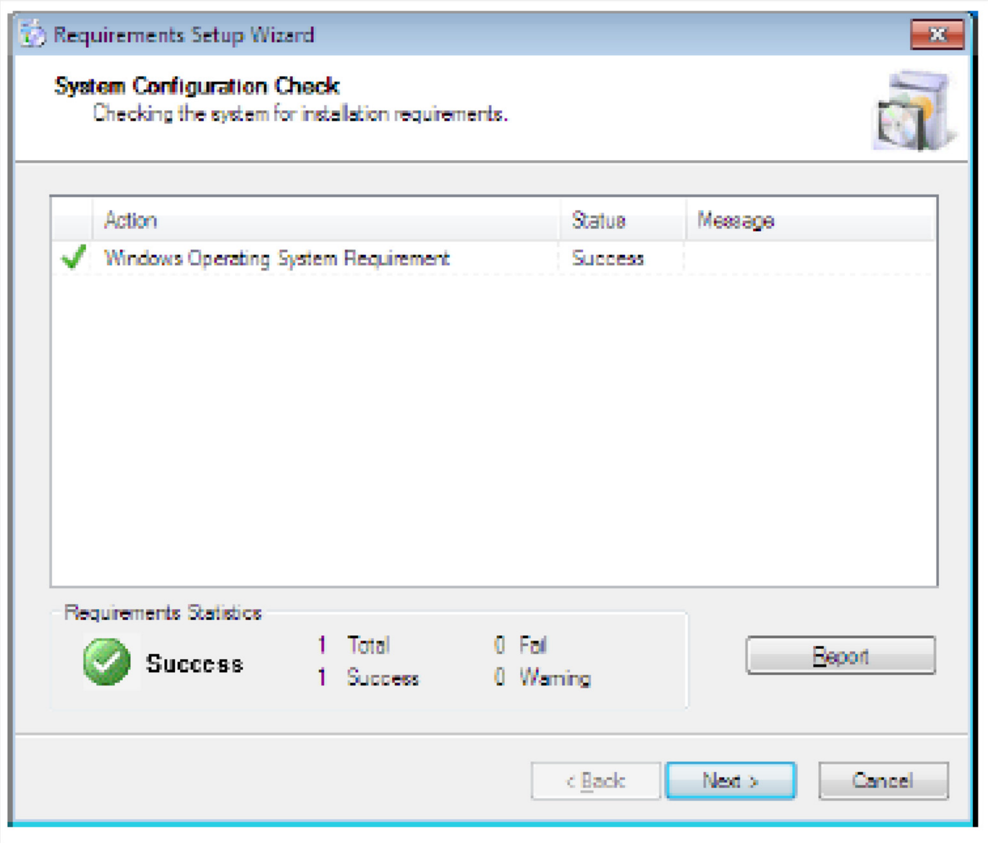
Also make sure that the network components (Switches, Routers) are correctly configured for VoIP and IP multicast. Be fully aware of the network topology! Make sure that the network supports IP Multicast between all network components that are used for Business Mobility IP DECT.

SECTION 2 INSTALLING THE DAP CONTROLLER RELEASE 6

PROCEDURE: “Installation”

1. Make sure that you are logged in with Administrator Rights!
2. Un-zip the DAP installer package.
3. Double click **`setup.exe`** or **`setup`**.
4. Depending on the version of your Windows operating system, you will now see a security screen from Windows saying "Do you want to allow the following program to make changes to your computer?" Click **Yes**.

5. You will see the following window.



Requirements Setup Wizard

System Configuration Check

Checking the system for installation requirements.

	Action	Status	Message
✓	Windows Operating System Requirement	Success	

Requirements Statistics

Success

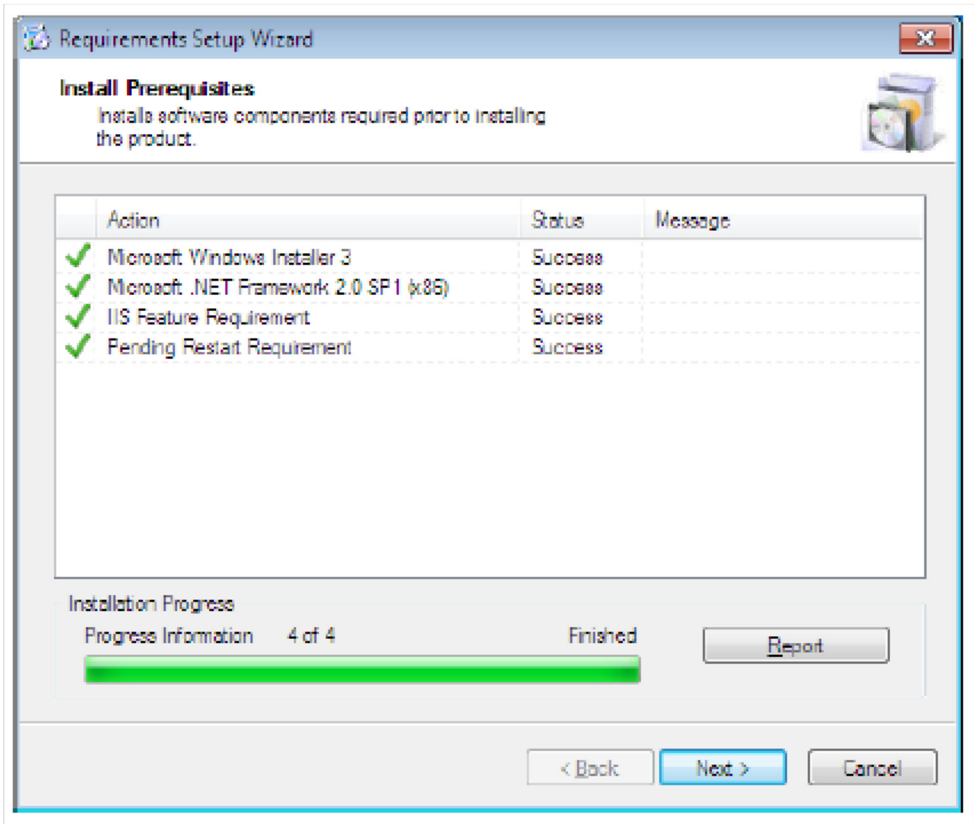
1	Total	0	Fail
1	Success	0	Warning

Figure 7-1 System Configuration Check Screen

It indicates that the DAP Controller software supports your version of Windows. Click **Next** to proceed.

6. Now the installation of "Prerequisites" takes place.
Note that this can take several minutes!

When all required prerequisites are installed, you will see the following window.



Requirements Setup Wizard

Install Prerequisites

Installs software components required prior to installing the product.

	Action	Status	Message
✓	Microsoft Windows Installer 3	Success	
✓	Microsoft .NET Framework 2.0 SP1 (x86)	Success	
✓	IIS Feature Requirement	Success	
✓	Pending Restart Requirement	Success	

Installation Progress

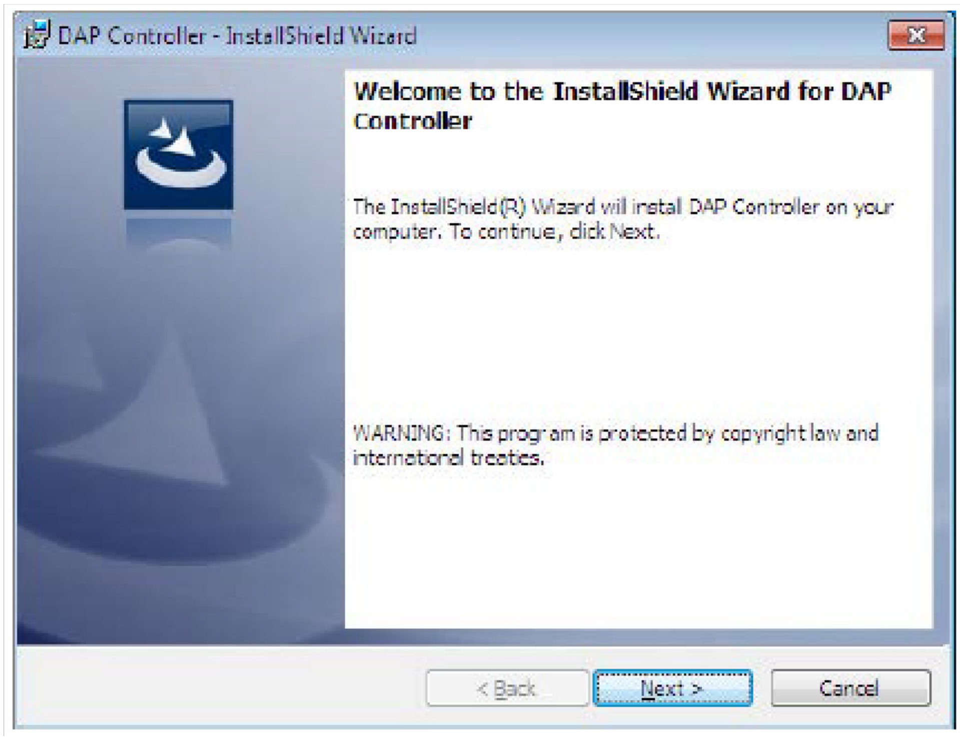
Progress Information 4 of 4 Finished

Figure 7-2 Install Prerequisites Screen

In case of Windows XP or Windows 2003, the system may ask for the Windows Operating System CD/DVD-ROM. If asked for, insert the CD/DVD-ROM.

Click **Next** to continue.

7. Now the following screen is displayed, indicating that the system is ready to start the installation of the DAP Controller.



Welcome to the InstallShield Wizard for DAP Controller

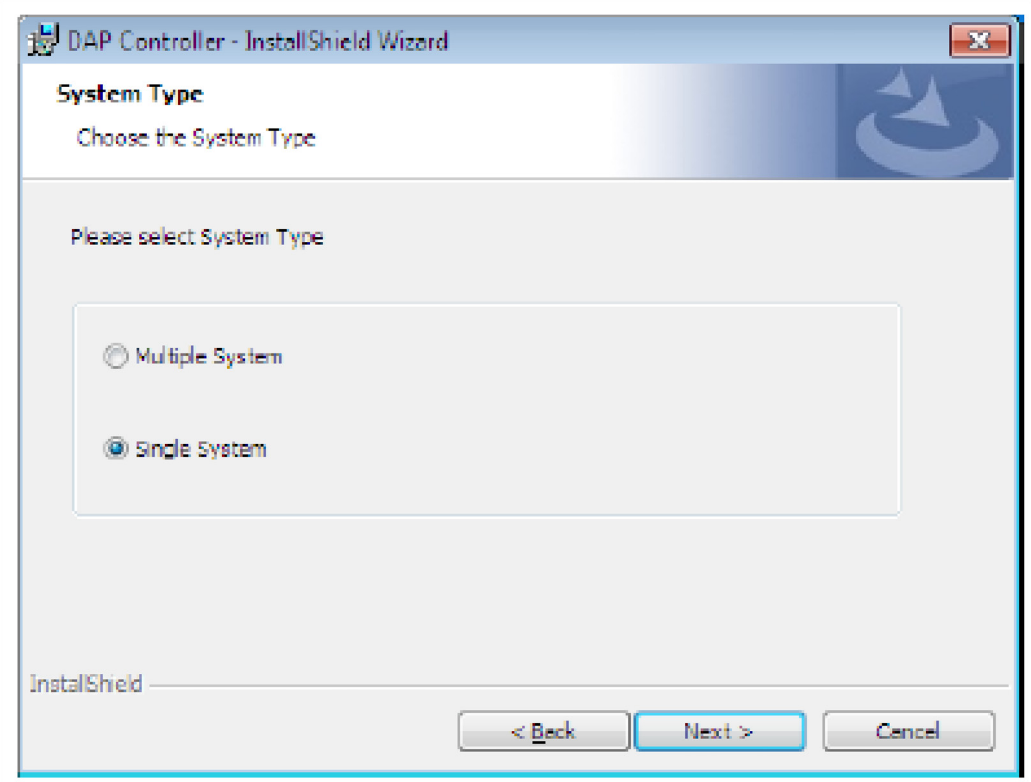
The InstallShield(R) Wizard will install DAP Controller on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Figure 7-3 DAP Controller Installation Wizard

Click **Next** to continue.

8. In the window that is displayed, please select the system type that you prefer, "Multiple System" or "Single System".



System Type

Choose the System Type

Please select System Type

○ Multiple System

● Single System

Figure 7-4 Choose System Type Screen

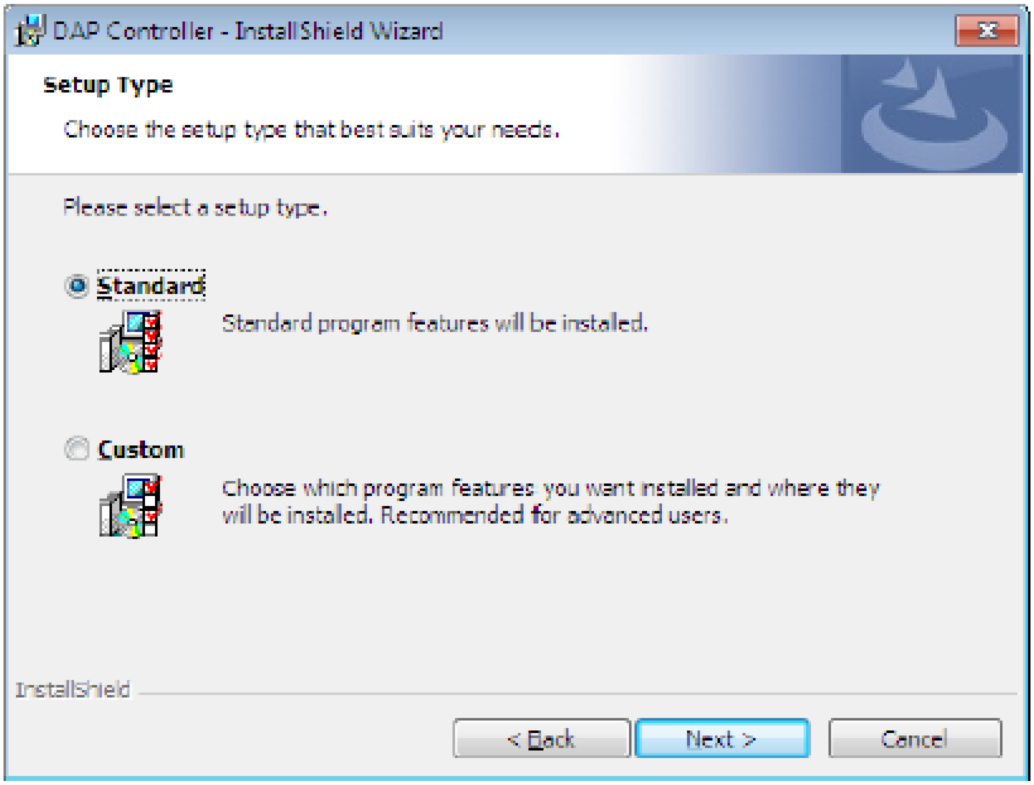
Select **Single System** if you want to manage only one IP DECT system, or **Multiple System** if you want to manage more than one IP DECT system with your PC. Click **Next**

✎ *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.*

✎ *If you select Multiple System, the Services that are installed for IP DECT are installed with startup parameters "Manual". This means that they will not start automatically when Windows boots up. If you select "Single System", the Services will be installed with startup parameters "Automatic".*

✎ *You can always change the settings from Multiple System to Single System and vice versa later on.*

9. The following window is displayed.



DAP Controller - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

● Standard

Standard program features will be installed.

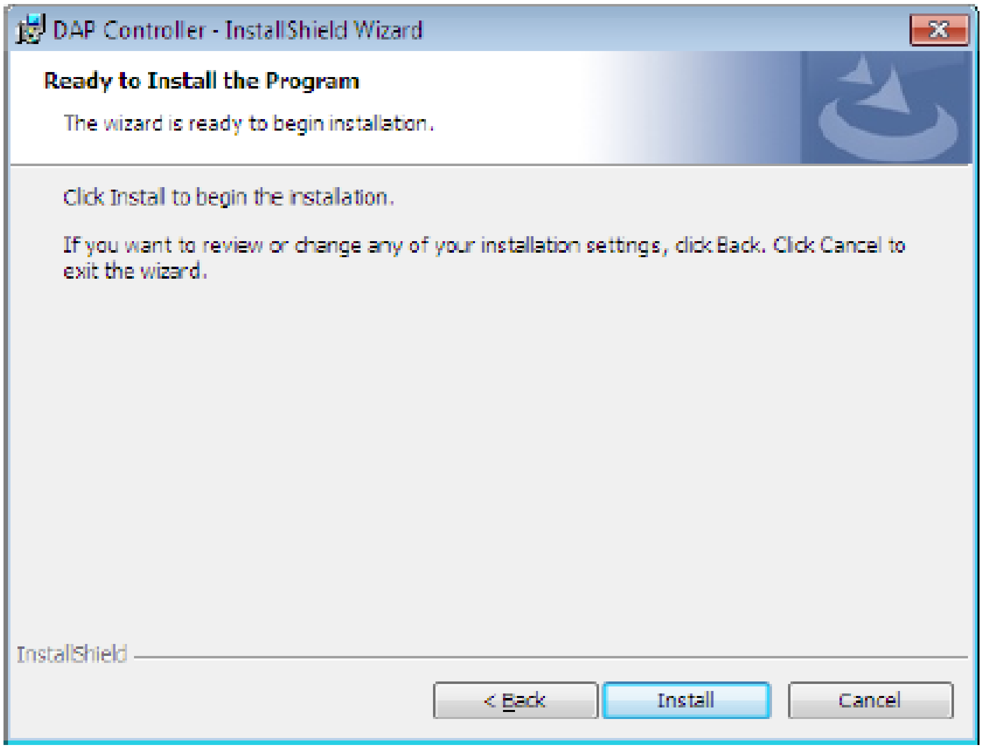
○ Custom

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

Figure 7-5 Setup Type Screen

In this window “InstallShield Wizard” you should specify the “Setup Type”. Select **Standard** and click **Next**. Note that if you want to fine tune the installation you should select “Custom”.and click "Next".

10. The system has collected sufficient info to start the actual installation.



DAP Controller - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.

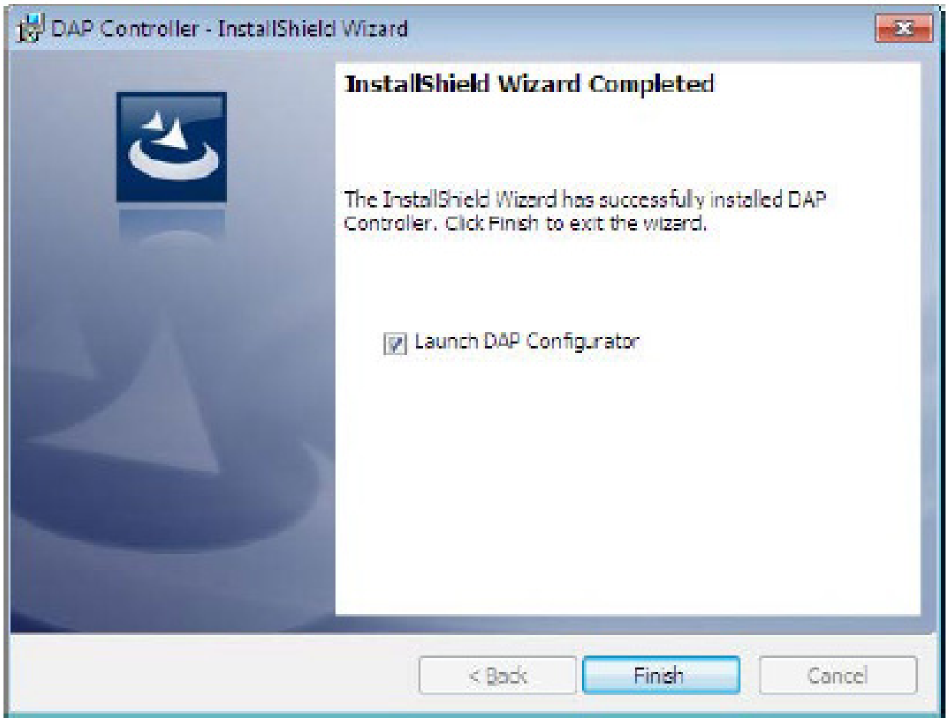
Click Instal to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Figure 7-6 Ready to Install Screen

Click **Install** to start the installation.

11. When the installation is finished, you will see the window "InstallShield Wizard Completed".



DAP Controller - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed DAP Controller. Click Finish to exit the wizard.

☑ Launch DAP Configurator

Figure 7-7 InstallShield Wizard Completed Screen

When the checkbox "Launch DAP Configurator is checked, the DAP Configurator will start after clicking Finish. If not, the installation will finish, but the DAP Configurator will not be started. However, you can start the DAP Configurator from the Programs menu later.

Click **Finish**.

Configuration - DAP Configurator Tool

SECTION 1 GENERAL

The DAP Configurator is a 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 “Start”, “All Programs”, “DAP Controller”, “DAP Application”, DAP Configurator” menu.

SECTION 2 USING THE DAP CONFIGURATOR

PROCEDURE: “Setting up the Configuration”

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**.

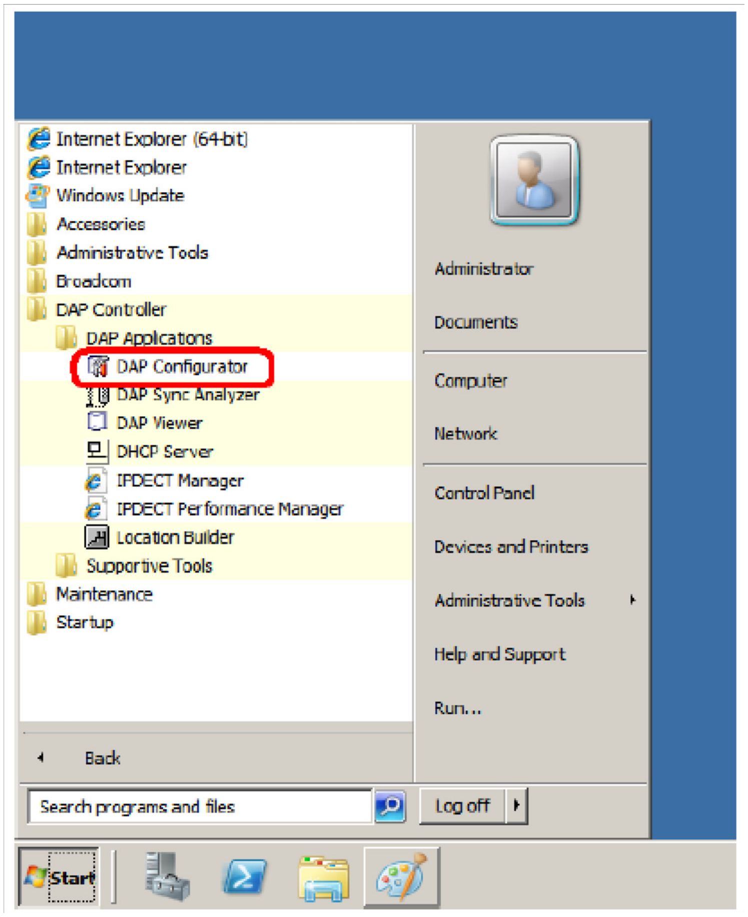
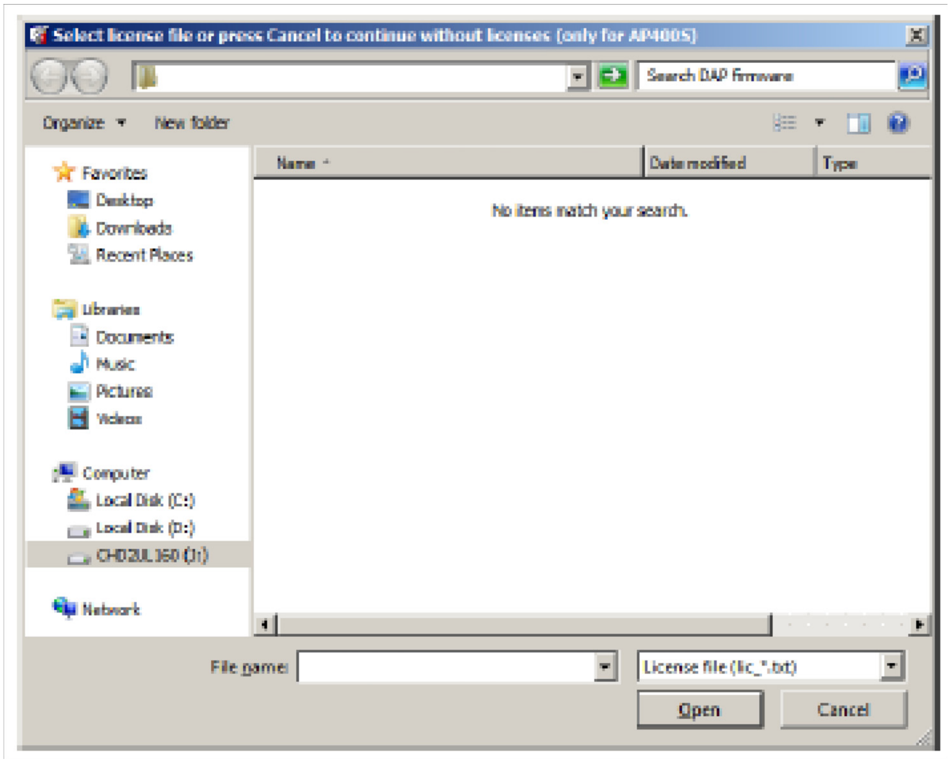


Figure 8-1 DAP Configurator Selection

3. If there is a problem with your network card (e.g. no cable connection), you will get a message. Please solve the problem. 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, the system asks you for the license file.



Select license file or press Cancel to continue without licenses (only for AP400S)

Search DAP Firmware

No items match your search.

File name:

License file (lic_*.txt)

Figure 8-2 Select Licence File Screen

5. Select the license file and click **open**.
For IP DECT on the SV8300, you must always have a License file.

6. You will see the following window displayed.

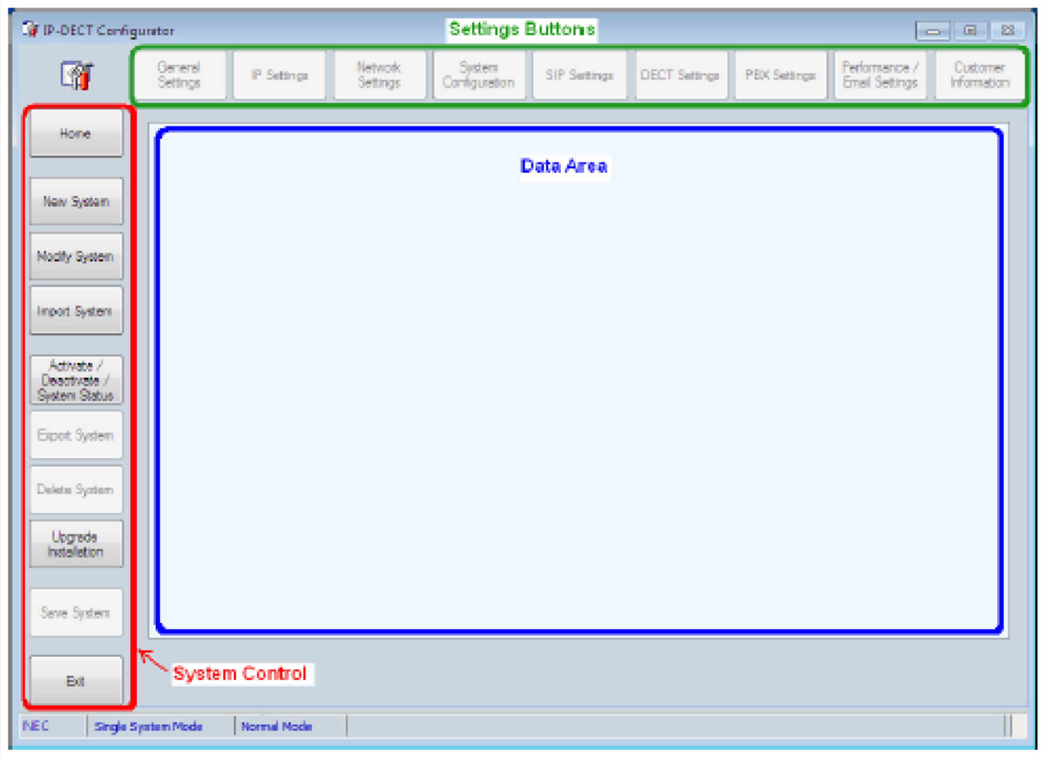


Figure 8-3 Setting Buttons

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.

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

7. 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**.

✎ *If you don't want to start a new system installation, refer to* Section 3 System Control Section on page 8-5 *for more information on the buttons.*

✎ *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 1 Settings Buttons on page 9-1.

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

SECTION 3 SYSTEM CONTROL SECTION

3.1 General

The System Control section is located at the left side of the IP DECT Configurator 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 your 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.

✎ 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.

- DAP Lite Download System (if displayed, it is greyed out)

  Not applicable for this configuration.

- Activate - Deactivate - System Status

  The system status button leads you to a window in which you can control the system status. Refer to 3.2 System Status Window on page 8-6. 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 be 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.

❍ Upgrade Installation

This allows you to upgrade the installation in a convenient way. You are guided through the Upgrade procedure.

❍ 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.

❍ Default

Return to default settings.

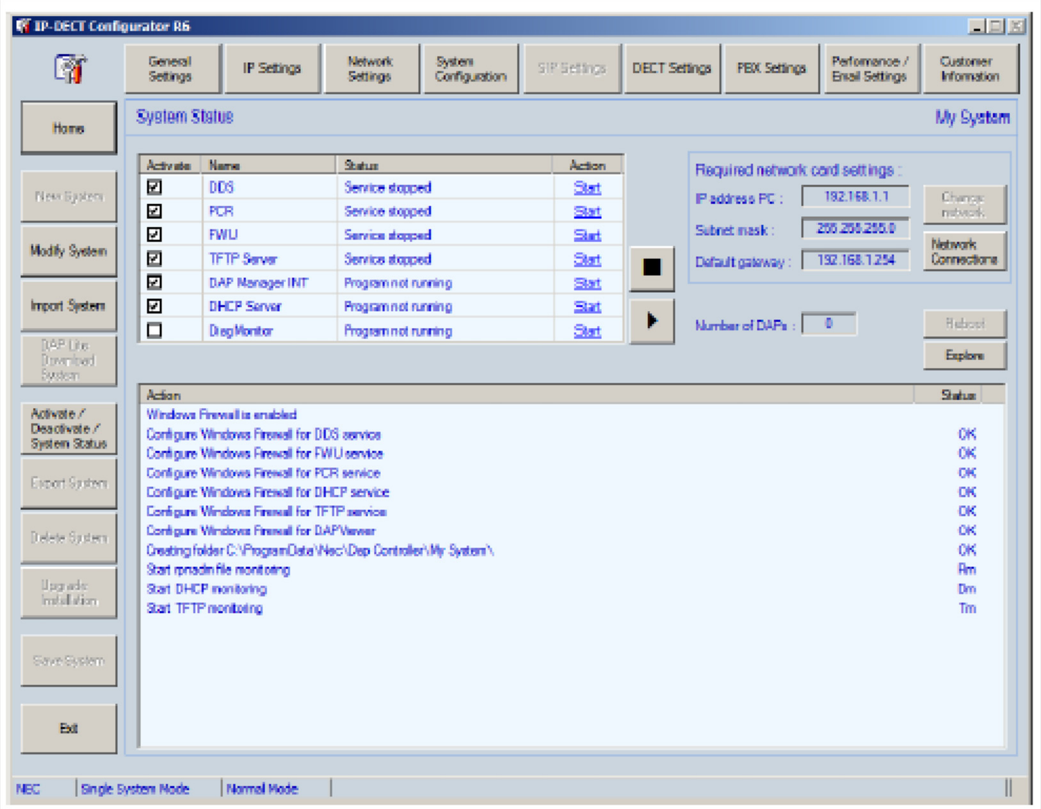
3.2 System Status Window

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.

✎ Make sure that you have stopped a previously running system.

✎ 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.

✎ Starting or stopping the system, only starts or 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.



Activate	Name	Status	Action
☑	DDS	Service stopped	Start
☑	PCR	Service stopped	Start
☑	FWU	Service stopped	Start
☑	TFTP Server	Service stopped	Start
☑	DAP Manager INT	Program not running	Start
☑	DHCP Server	Program not running	Start
☐	DiagMonitor	Program not running	Start

Required network card settings :

IP address PC : 192.168.1.1

Subnet mask : 255.255.255.0

Default gateway : 192.168.1.254

Number of DAPs : 0

Action	Status
Windows Firewall is enabled	
Configure Windows Firewall for DDS service	OK
Configure Windows Firewall for FWU service	OK
Configure Windows Firewall for PCR service	OK
Configure Windows Firewall for DHCP service	OK
Configure Windows Firewall for TFTP service	OK
Configure Windows Firewall for DAPViewer	OK
Creating folder C:\ProgramData\Nec\Dap Controller\My System\	OK
Start rpnadm file monitoring	Rm
Start DHCP monitoring	Dm
Start TFTP monitoring	Tm

NEC | Single System Mode | Normal Mode

Figure 8-4 IP DECT Configurator Screen

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 performance thresholds are exceeded or when a DAP goes down.

- FWU

  FirmWare Upload must be running if you want to use Firmware Upload.

- 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 start-up. 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

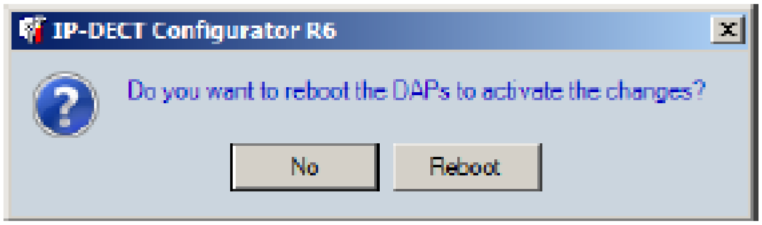
The DHCP server runs as an application. It can be started or stopped. Make sure that you are allowed to use a DHCP server on the Network.

❍ 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 may ask 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!



IP-DECT Configurator R6

Do you want to reboot the DAPs to activate the changes?

Figure 8-5 Reboot Screen

SECTION 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.

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

PROCEDURE: “Switching between Single Site and Multi Site”

1. Make sure that the IP DECT Configurator is open. If not open the IP DECT Configurator/DAP Configurator. Refer to Section 2 Using the DAP Configurator on page 8-1.

2. Using the DAP Configurator left mouse click the top left IP DECT Configurator icon. See icon below.

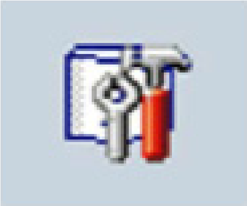
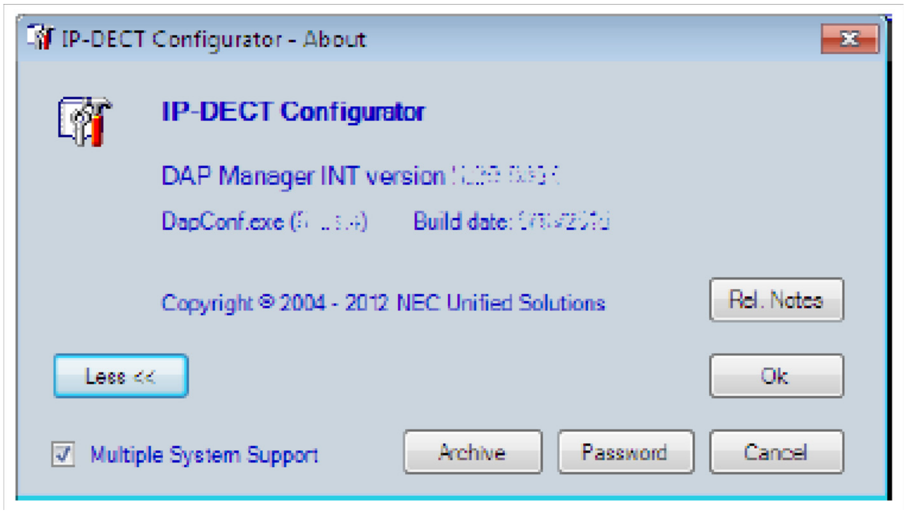


Figure 8-6 IP DECT Configurator Icon

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



IP-DECT Configurator - About

IP-DECT Configurator

DAP Manager INT version [illegible]

DapConf.exe ([illegible]) Build date: [illegible]

Copyright © 2004 - 2012 NEC Unified Solutions

☑ Multiple System Support

Figure 8-7 About Screen

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.

THIS PAGE INTENTIONALLY LEFT BLANK

DAP Configurator Settings

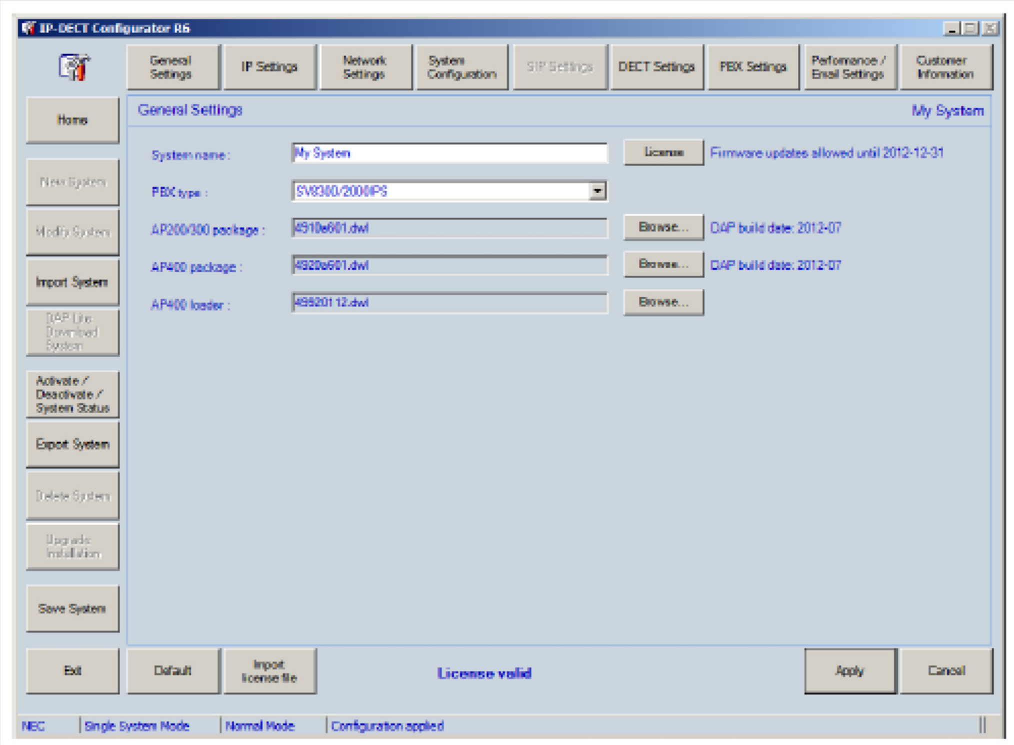
9

SECTION 1 SETTINGS BUTTONS

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

SECTION 2 GENERAL SETTINGS

When you click the “General Settings” the following window is displayed:



General Settings — My System

System name : My System — Firmware updates allowed until 2012-12-31

PBX type : SV8300/2000IPS

AP200/300 package : 4910e601.dwl — DAP build date: 2012-07

AP400 package : 4920e601.dwl — DAP build date: 2012-07

AP400 loader : 49920112.dwl

License valid

NEC | Single System Mode | Normal Mode | Configuration applied

Figure 9-1 General Settings Screen

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.

❍ PBX Type

Select the platform to which the IP DECT system is (going to be) connected. This must be SV8300.

❍ AP300 Package

Here you must enter the firmware file specification for the firmware package for the AP300. For SIP, the file name should look like this: `4910axyz.dwl` (e.g. `4910a610.dwl`).

❍ AP400 Package

Here you must enter the firmware file specification for the firmware package for the AP400. For SIP, the file name should look like this: `4920axyz.dwl` (e.g. `4920a610.dwl`).

❍ AP400 Loader (not needed in basic installations)

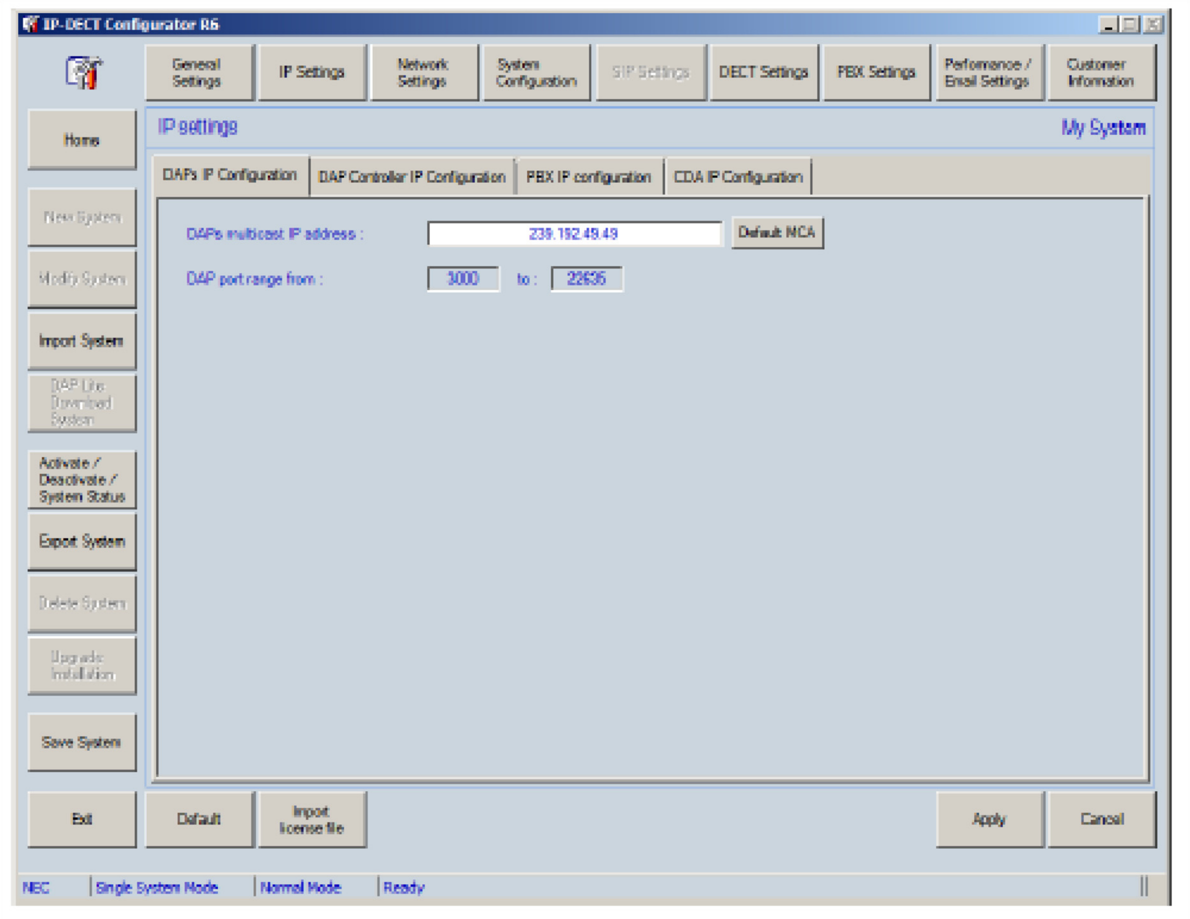
Here you must enter the Loader file specification for the firmware package for the AP400. For SIP, the file name should look like this: `49920112.dwl`.

When finished, click “Apply”. On the bottom of the window, you should see, “License valid”. Continue with clicking button “IP Settings”.

SECTION 3 IP SETTINGS

3.1 The Window

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



DAPs multicast IP address : 239.192.49.49

DAP port range from : 3000 to : 22636

Figure 9-2 IP Setting Screen

3.2 IP Settings, tab “DAPs IP Configuration”

Please click the tab: DAPs IP configuration. Now the following fields can be edited:

❍ DAPs 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

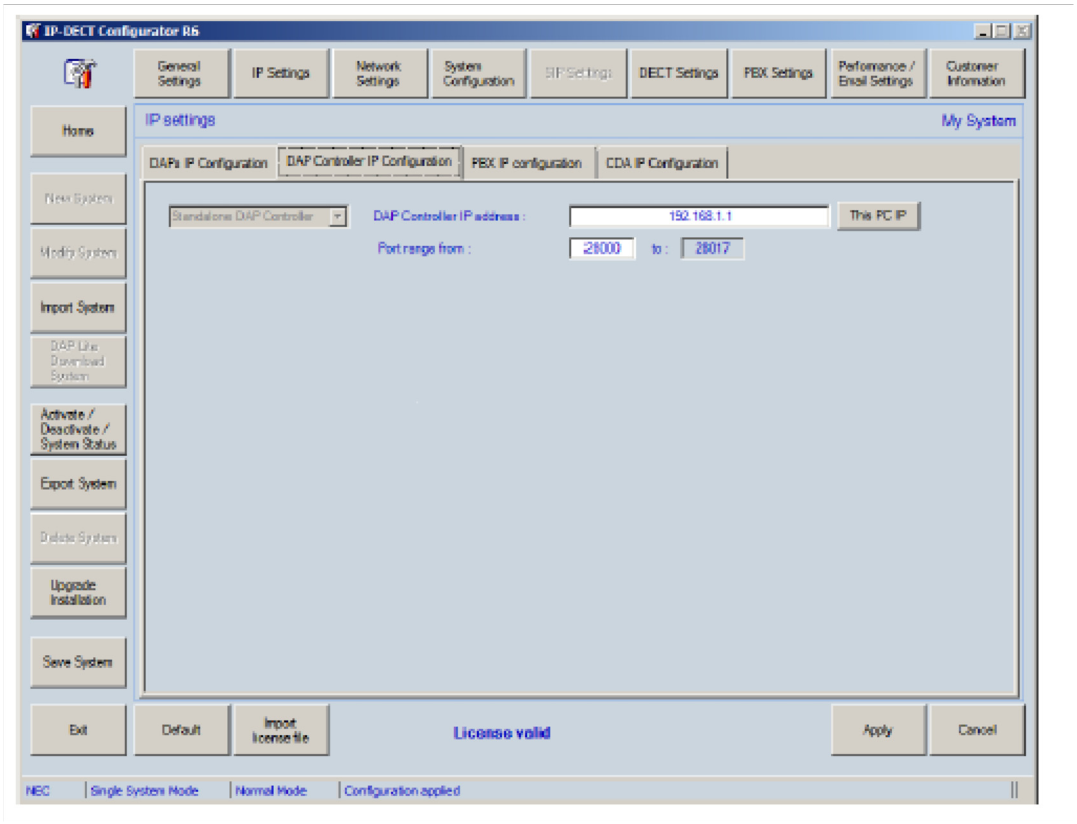
By default the port range on the DAPs will start at port 3000. *Please note that you cannot change port range.*

3.3 IP Settings, tab “DAP Controller IP Configuration”

Please click the tab: DAPs IP configuration.

✎ Depending on the Licenses that you have, one of the following screens is displayed.

If you have a multiple DAP Controller system, refer to Chapter 15 DAP Controller Redundancy, before you continue making the configuration.



Standalone DAP Controller

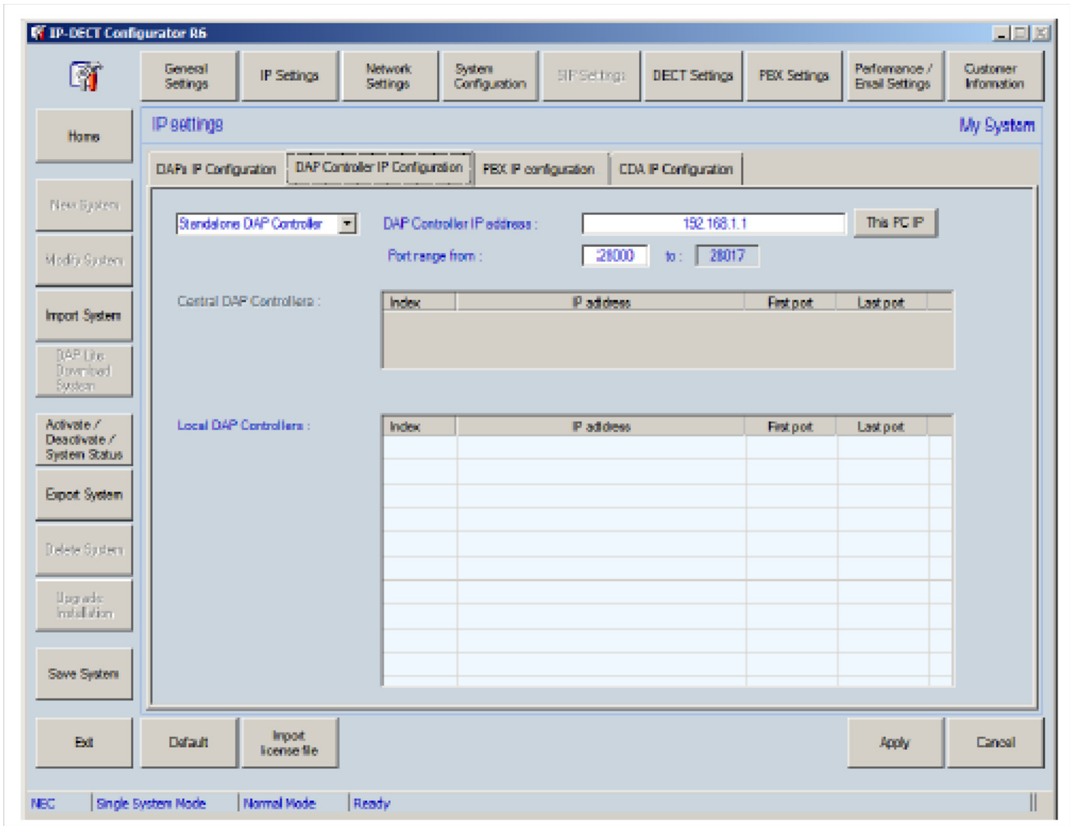
DAP Controller IP address : 192.168.1.1

Port range from : 28000 to : 28017

License valid

NEC | Single System Mode | Normal Mode | Configuration applied

Figure 9-3 DAP Controller IP Configuration



Standalone DAP Controller

DAP Controller IP address : 192.168.1.1

Port range from : 28000 to : 28017

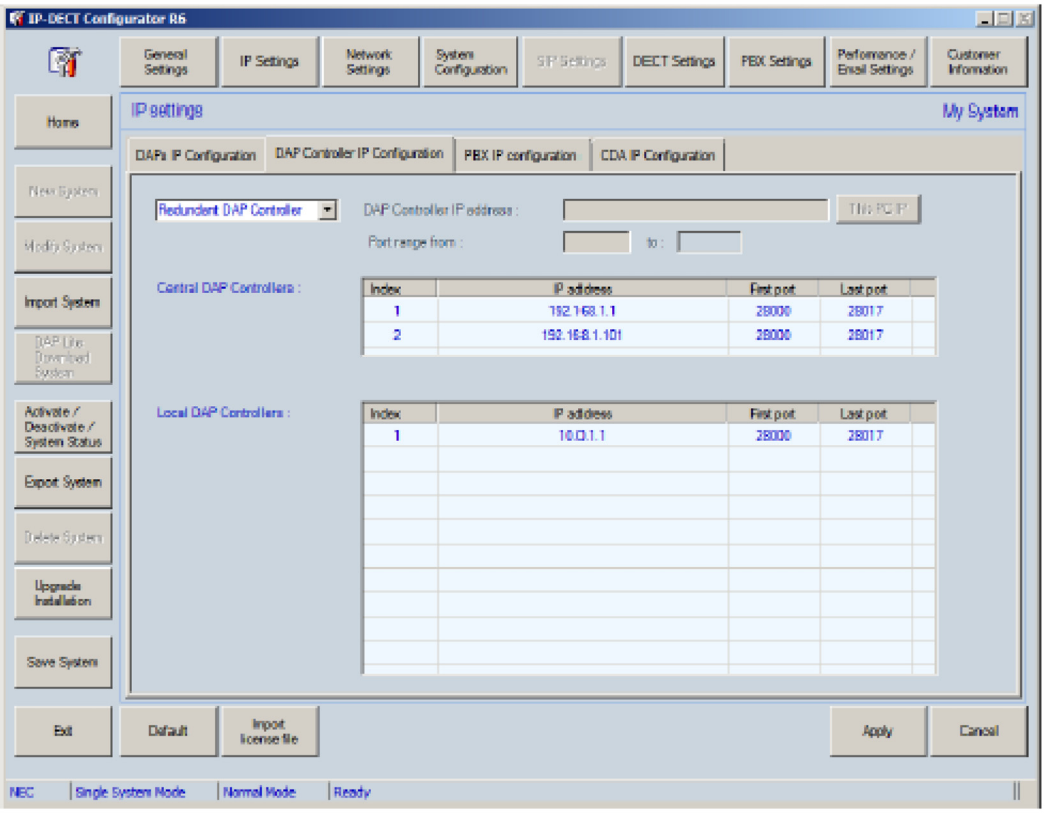
Central DAP Controllers :

Index	IP address	First port	Last port

Local DAP Controllers :

Index	IP address	First port	Last port

Figure 9-4 DAP Controller IP Configuration (Continued)



IP settings — My System

DAPs IP Configuration | DAP Controller IP Configuration | PBX IP configuration | CDA IP Configuration

Redundant DAP Controller

DAP Controller IP address :

Port range from : to :

Central DAP Controllers :

Index	IP address	First port	Last port
1	192.168.1.1	28000	28017
2	192.168.1.101	28000	28017

Local DAP Controllers :

Index	IP address	First port	Last port
1	10.0.1.1	28000	28017

NEC | Single System Mode | Normal Mode | Ready

Figure 9-5 DAP Controller IP Configuration (Continued)

✎ You fill in the data of all DAP Controllers in the DAP Configurator of the Primary DAP Controller.

❍ DAP Controller 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

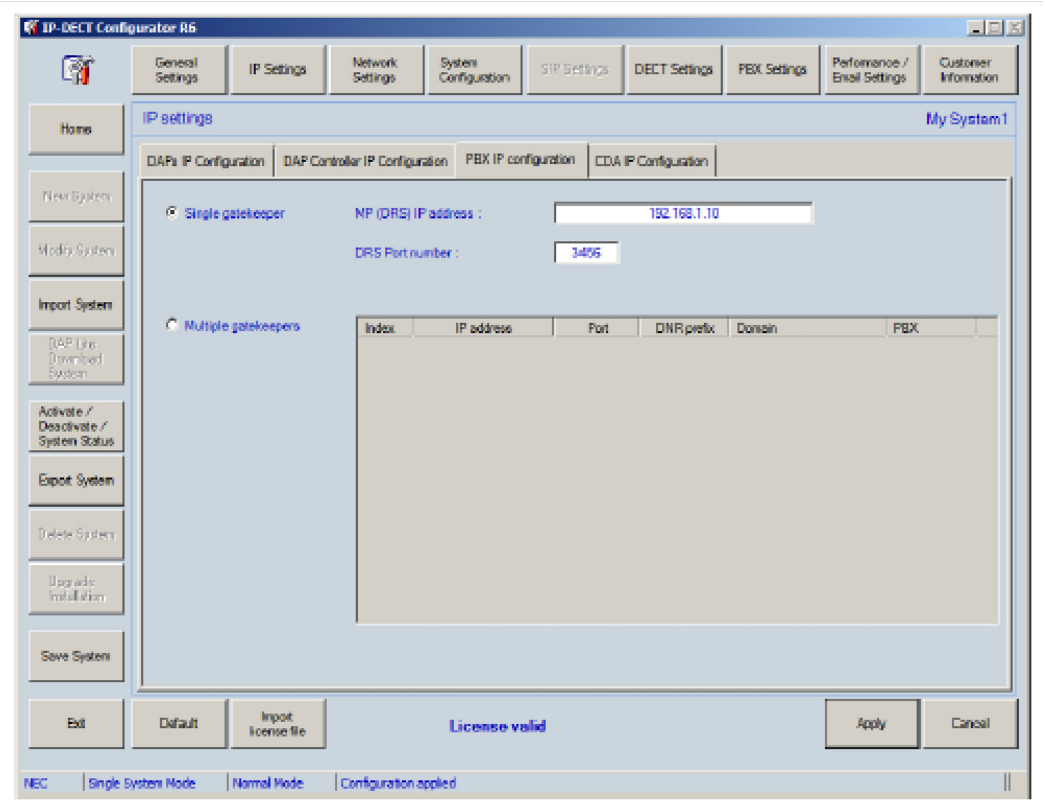
Start of port range in use for IP DECT on the DAP Controller/Manager PC. Note that this port range is automatically filled in. Please do not change manually.

Enter the IP Addresses of the DAP Controllers that are in your system.

✎ When you enter more DAP Controllers than your License allows, you will get the message “License Violation”.

3.4 IP Settings, tab “PBX IP Configuration”

Please click the tab: PBX IP Configuration. Now the following fields can be edited:



● Single gatekeeper

MP (DRS) IP address : 192.168.1.10

DRS Port number : 3456

○ Multiple gatekeepers

Figure 9-6 PBX IP Configuration

❍ Single Gate Keeper

Click this radio button to select a system type with only one gatekeeper.

❍ MP (DRS) IP Address

Enter the IP Address of the IPLA in the SV8300.

❍ DRS port number

Enter DRS (D-term Registration) port number on the SV8300. The default port is 3456.

❍ Multiple gatekeepers.

When you click this radio button, are able to enter more than one DRS address. This is can be useful for redundancy reasons.

Multiple Gatekeeper settings:

When you select “Multiple Gatekeepers, the table in which you can add gatekeepers is activated. Right mouse click inside the table and select “new” to add a gatekeeper. The following items needs to be entered.

❍ Index

This is a unique identifier per SV8300. This specifies the priorities.

❍ IP Address

Enter the IP address of the next SV8300. Note that the first proxy is already in the list.

❍ Port

Enter the port number for the SV8300.

❍ DNR Prefix

Not applicable for the SV8300.

❍ Domain

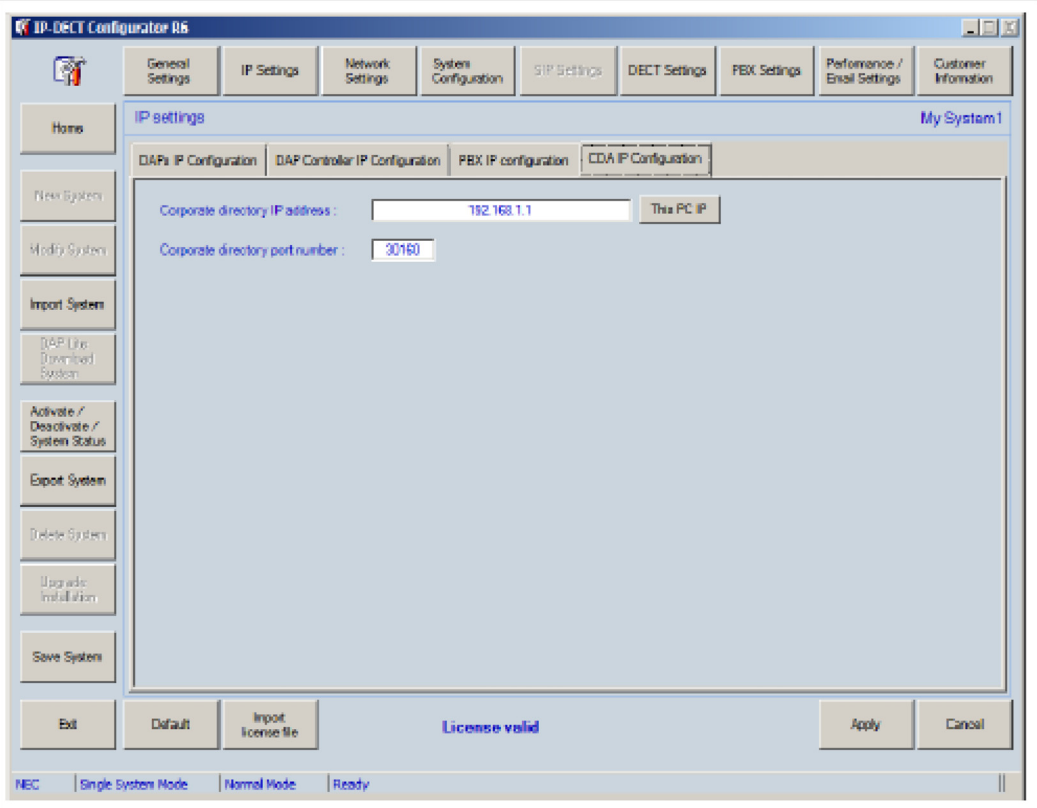
Not applicable for the SV8300.

❍ PBX

Here you must select the PBX type. Not applicable for the SV8300

3.5 IP Settings, tab “CDA IP Configuration”

Please click the tab: CDA IP Configuration. Now the following fields can be edited:



Corporate directory IP address : 192.168.1.1

Corporate directory port number : 30160

Figure 9-7 CDA IP Configuration

- Corporate directory IP Address

  The IP address of the Central Directory Server (if applicable)

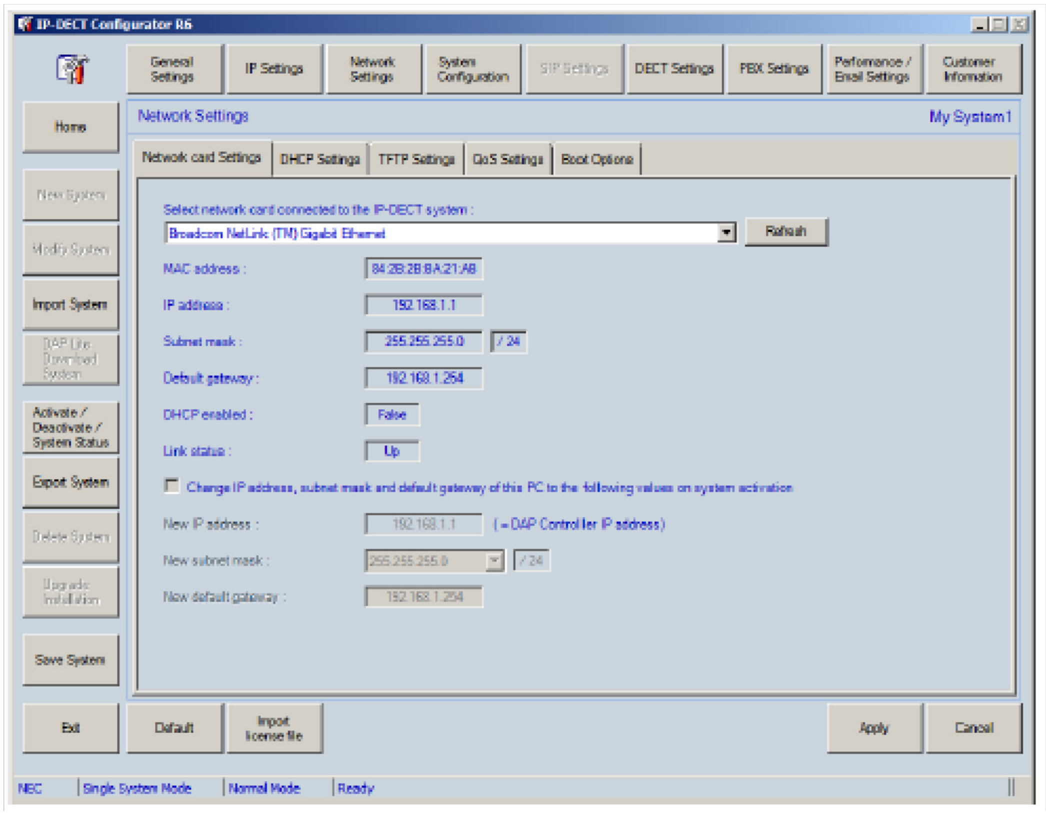
- Corporate Directory port number

  Port number on the Central Directory server. Default port number is 30160.

SECTION 4 NETWORK SETTINGS

4.1 Network Settings, tab “Network Card Settings”

Please click the tab: Network card settings. Now the following fields can be edited:



Network Settings My System1

Select network card connected to the IP-DECT system :
Broadcom NetLink (TM) Gigabit Ethernet

MAC address : 84:2B:2B:8A:21:A8
IP address : 192.168.1.1
Subnet mask : 255.255.255.0 / 24
Default gateway : 192.168.1.254
DHCP enabled : False
Link status : Up

□ Change IP address, subnet mask and default gateway of this PC to the following values on system activation

New IP address : 192.168.1.1 (= DAP Controller IP address)
New subnet mask : 255.255.255.0 / 24
New default gateway : 192.168.1.254

NEC | Single System Mode | Normal Mode | Ready

Figure 9-8 Network Card Settings

❍ Select network card connected to the IP DECT system.

If you have more than one network card in your system, select the network card that you want to use here.

The network card data is displayed. Please note that you cannot change the network card data here!

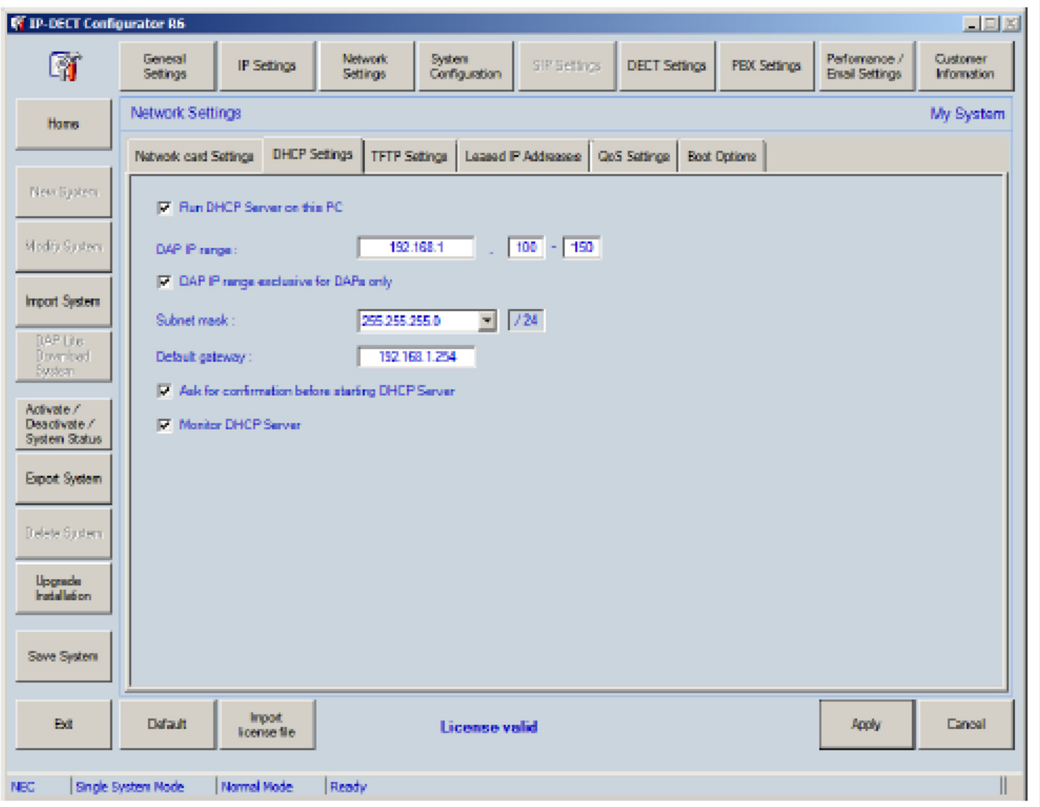
❍ Change IP address, subnet mask and default gateway of this PC in the following values on system activation.

If this box is checked, the IP address, subnet mask and default gatekeeper of your network card is automatically changed to the DAP Controller IP address that you have specified in . This can be useful when you manage

more than one IP DECT system with your computer. The moment that you start up one of your DECT system configurations, the IP settings of your network card are automatically changed to the right settings for that particular system.
Please not that the IP settings on the network card are automatically changed, but are not changed back to the previous settings.

4.2 Network Settings, tab “DHCP Settings”

Please click the tab: DHCP Settings. Now the following fields can be edited:



☑ Run DHCP Server on this PC

DAP IP range : 192.168.1 . 100 - 150

☑ DAP IP range exclusive for DAPs only

Subnet mask : 255.255.255.0 / 24

Default gateway : 192.168.1.254

☑ Ask for confirmation before starting DHCP Server

☑ Monitor DHCP Server

Figure 9-9 DHCP 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 if you check the checkbox “DAP IP range exclusive for DAPs only”. In that case 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` in the system directory.

❍ DAP IP Range

Specify IP address range that will be issued to the DAPs.

❍ DAP IP Address range exclusive for DAPs only.

If checked, the DHCP server will respond to DAP requests only. This is based on the “Vendor Class ID” that the DAPs issue when they do a DHCP request.

❍ Subnet Mask.

Self explaining.

❍ Default Gateway

Self explaining.

❍ Ask for confirmation before starting the DHCP server

Self explaining.

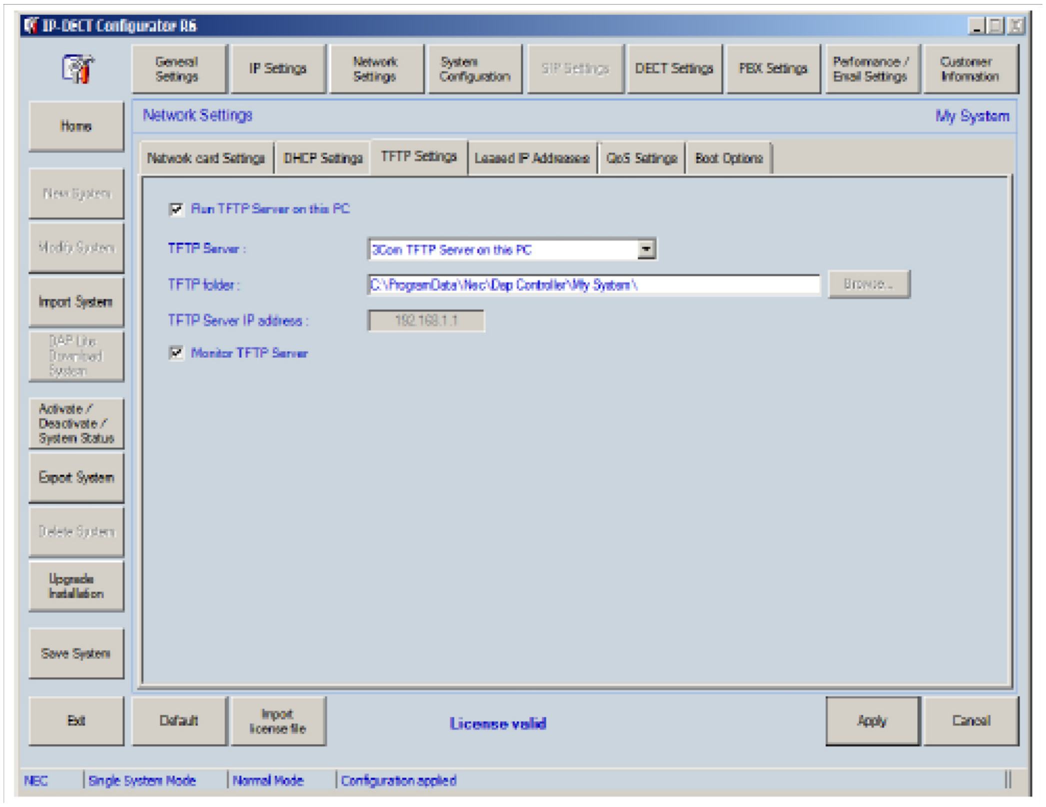
❍ Monitor DHCP Server

This allows you to monitor the DHCP activity of the built-in DHCP server. You see the results in the System Status Window, which is opened when you click the button “Activate / Deactivate / System Status”. Refer to .

✎ *The built-in DHCP issues an “unlimited” lease time.*

4.3 Network Settings, tab “TFTP Settings”

Please click the tab: TFTP Settings. Now the following fields can be edited:



☑ Run TFTP Server on this PC

TFTP Server : 3Com TFTP Server on this PC

TFTP folder : C:\ProgramData\Nec\Dap Controller\My System\

TFTP Server IP address : 192.168.1.1

☑ Monitor TFTP Server

License valid

NEC | Single System Mode | Normal Mode | Configuration applied

Figure 9-10 TFTP Settings

- ❍ Run TFTP Server on this PC

  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\Nec\DAP Controller\<system name>.` When you are using Windows 7 or Windows 2008, the directory is `C:\ProgramData\Nec\DAP Controller\<system name>`

- ❍ TFTP Server IP Address.

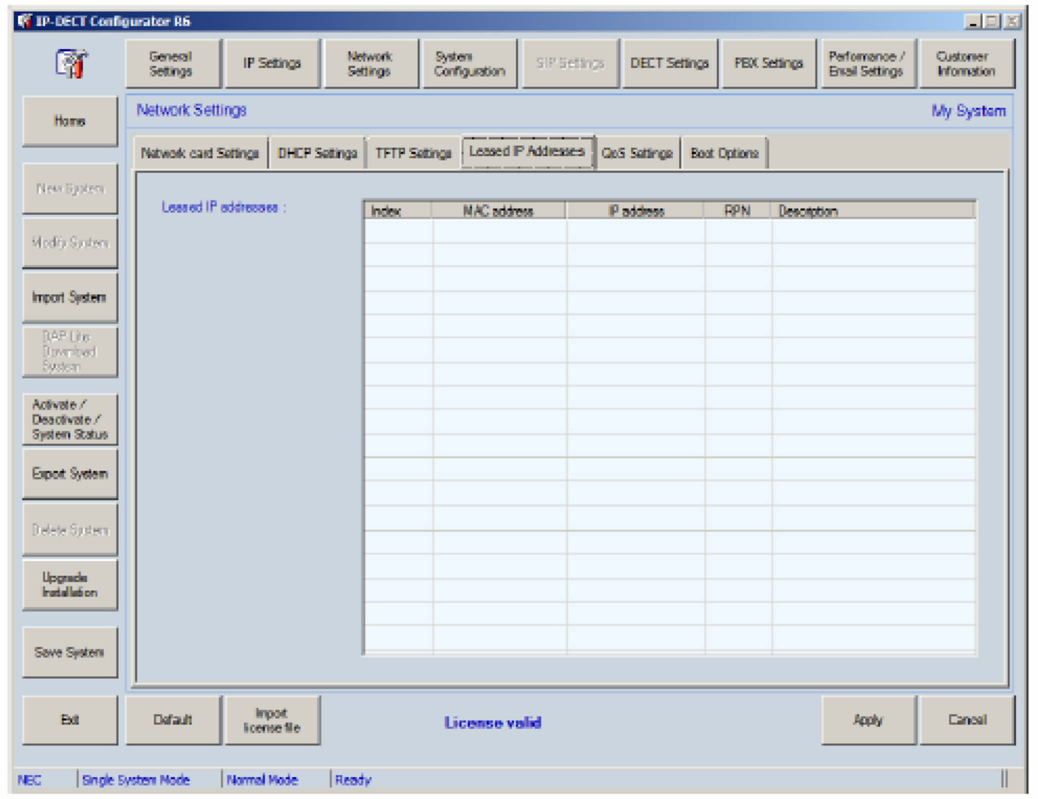
  This is the IP address of the machine where the TFTP server is running. When you have chosen to use the built-in TFTP server, you cannot change this IP address because it is the IP address of your machine.

- ❍ Monitor TFTP Server

  This allows you to monitor the TFTP activity of the built-in TFTP server. You see the results in the System Status Window, which is opened when you click the button “Activate / Deactivate / System Status”. Refer to .

4.4 Network Settings, tab “Leased IP Addresses”.

Please click the tab: Leased IP Addresses. Now you see a list of Leased IP addresses in the Built-in DHCP Server.



Leased IP addresses :

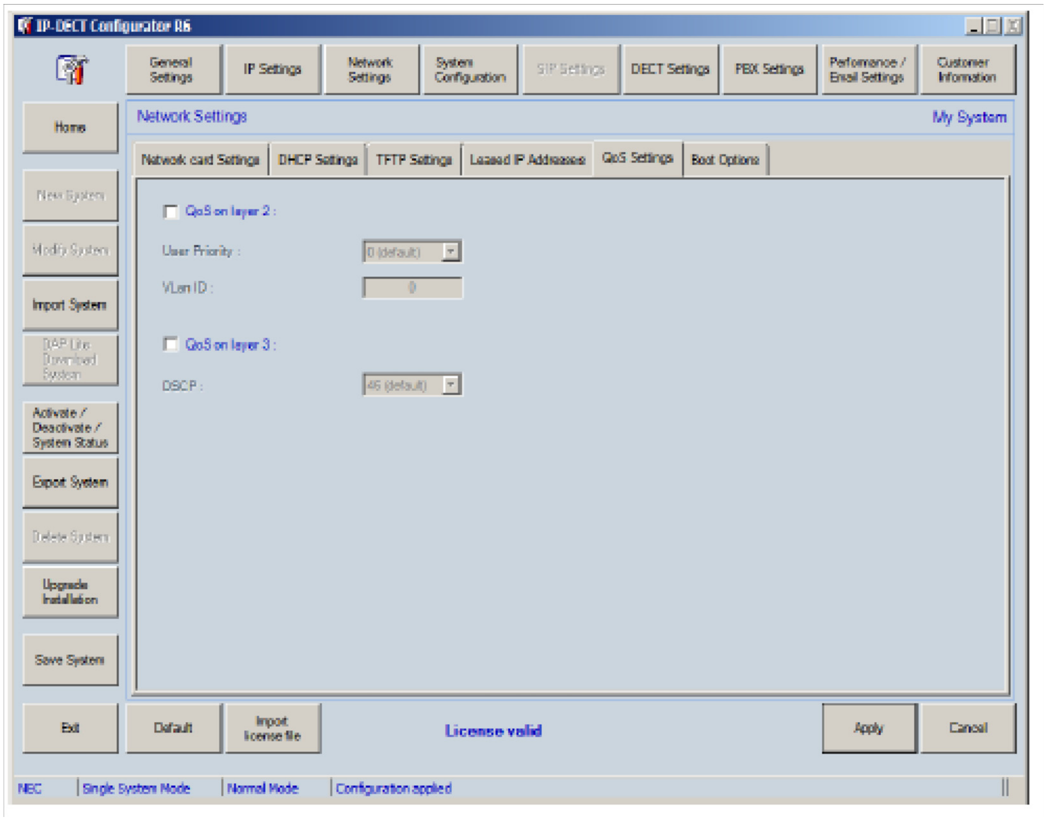
Index	MAC address	IP address	RPN	Description

Figure 9-11 Leased IP Addresses Settings

In this window, you can delete/change/add the relationship between MAC addresses and leased IP addresses. You have access to these settings by means of right mouse clicking a line in the Leased IP Addresses window.

4.5 Network Settings, tab “QoS Settings”

Please click the tab: QoS Settings. Now the following fields can be edited:



□ QoS on layer 2 :

User Priority : 0 (default)

VLan ID : 0

□ QoS on layer 3 :

DSCP : 46 (default)

License valid

NEC | Single System Mode | Normal Mode | Configuration applied

Figure 9-12 QoS Settings

❍ QoS on Layer 2

When you check this checkbox, the IEEE802.1p/q field in the layer 2 data package will be used.
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.

❍ User Priority

The Priority value is a three bit value which must be entered as decimal value 0 ... 7, where 7 is the highest priority.

❍ VLAN ID

Here you can specify a VLAN ID. Note that “0” means no VLAN specified.

- QoS on Layer 3

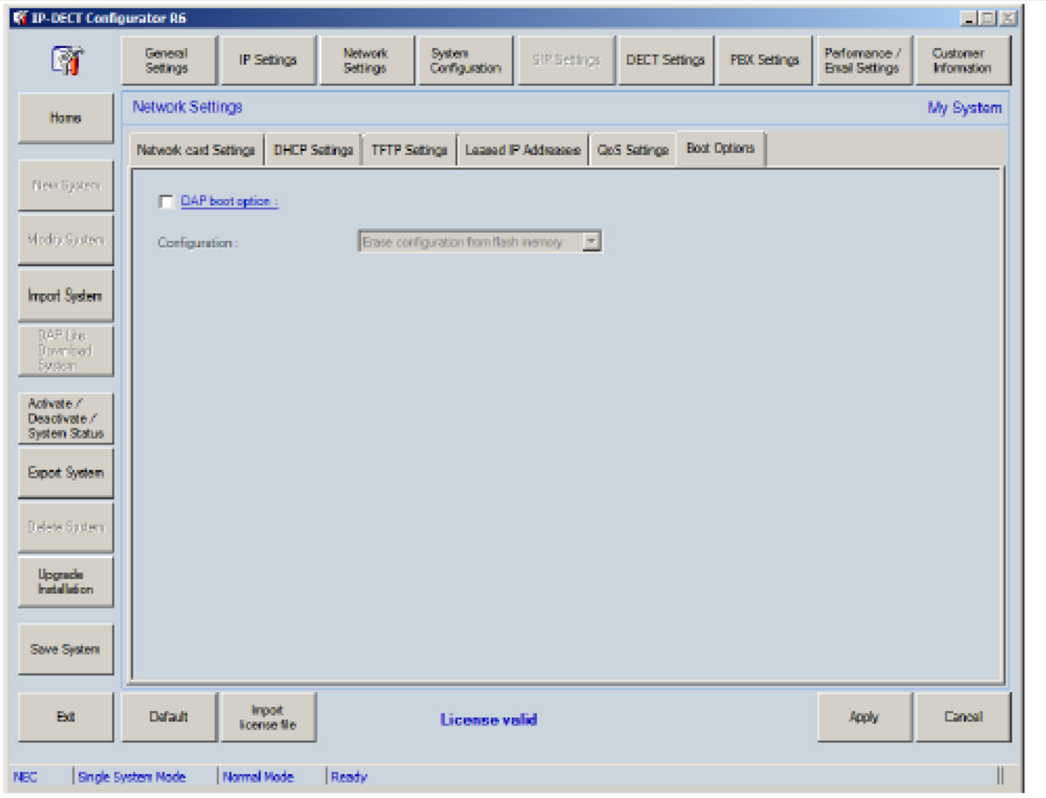
  Here you can enable Quality of Service on Layer 3.

- DSCP

  If you have enabled QoSon layer 3, 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).

4.6 Network Settings, tab “Boot options”

Please click the tab: Boot Options. Now the following fields can be edited:



☐ DAP boot option :

Configuration : Erase configuration from flash memory

Figure 9-13 Boot Options Settings

- DAP Boot options.

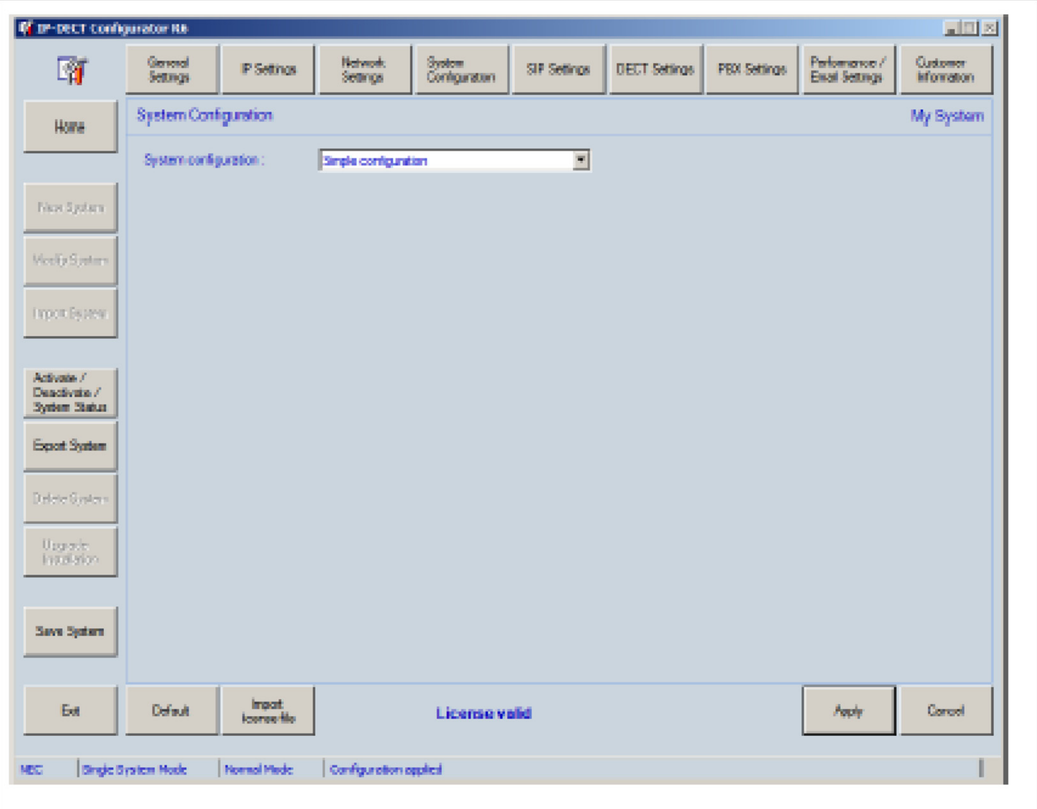
  This allows you to store the IP address data and Configuration data into Flash memory in the DAP. When stored, a DAP does not need a DHCP/ TFTP server anymore. Note that you can “Store” or “Erase” data.

✎ *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 "System Configuration".

SECTION 5 SYSTEM CONFIGURATION

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



System Configuration My System

System configuration : Simple configuration

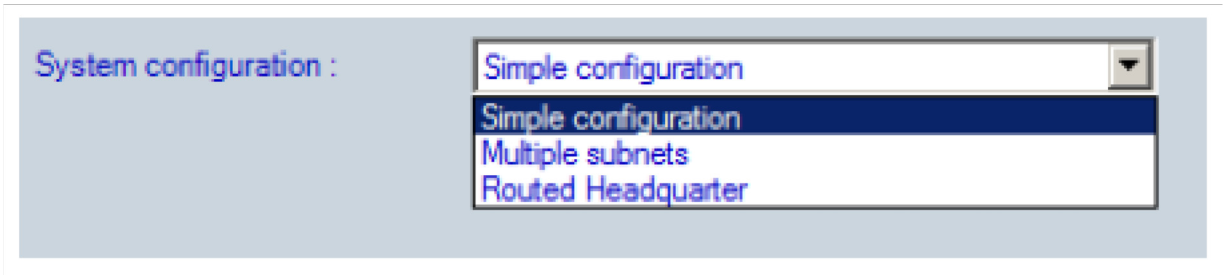
License valid

NEC | Single System Mode | Normal Mode | Configuration applied

Figure 9-14 System Configuration Settings

You can select the type of system that you want to use. Refer to Chapter 4 Network Configurations for more information. Once you have decided which network configuration you need, continue with the information in this chapter and setup the configuration as needed.

When you click the pull down icon, you will see the following options displayed. Simple Configuration selection



System configuration : Simple configuration

Figure 9-15 Simple Configuration Screen

5.1 Simple Configuration

A simple configuration consists of one network segment. All IP DECT components are in that segment, including the PBX.

5.2 Multiple Subnets

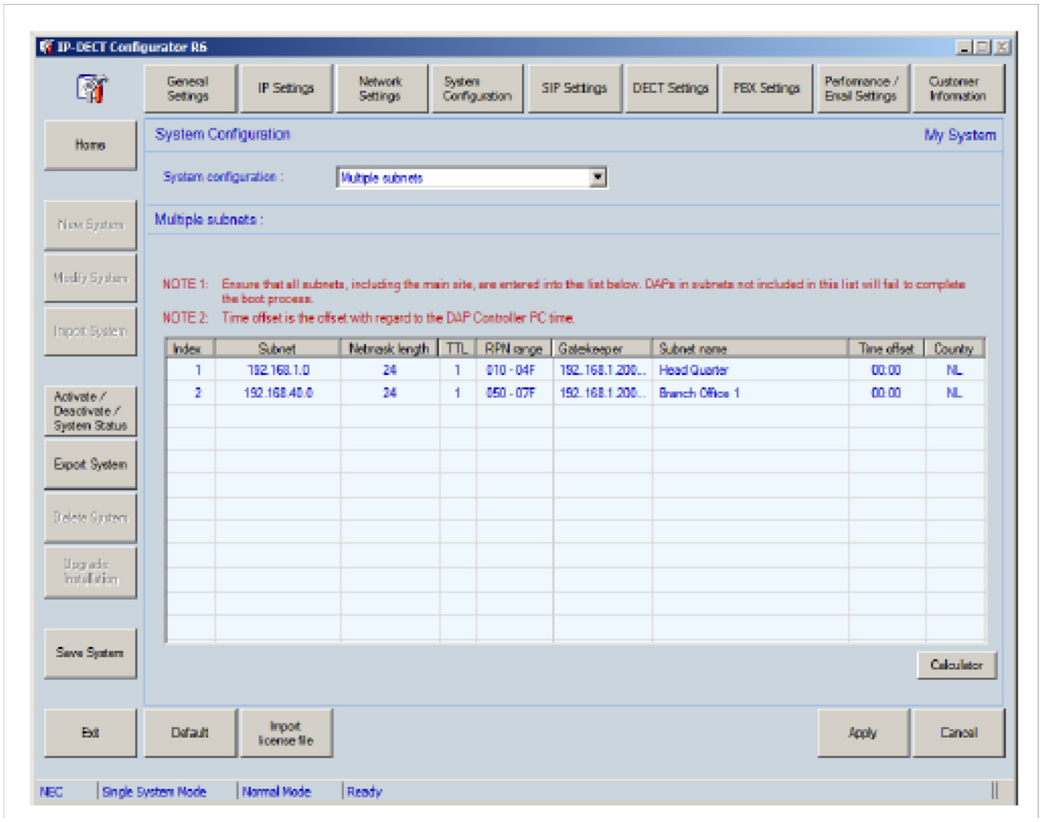
This configuration allows you to have the IP DECT system over various subnets. A number of configurations are possible. You will need this configuration window to setup:

- A Head Quarter with Branch Office.
- A Routed Head Quarter with Branch Office.
- A Routed Head Quarter with a Routed Branch Office.

Consult Chapter 4 Network Configurations for more information.

The window “Multiple Subnets” offers the possibility to specify a certain RPN range per Branch Office Subnet. Note that you should set the RPN range wide enough to allow future system expansion.

You will see the following screen:



System Configuration My System

System configuration : Multiple subnets

Multiple subnets :

NOTE 1: Ensure that all subnets, including the main site, are entered into the list below. DAPs in subnets not included in this list will fail to complete the boot process.

NOTE 2: Time offset is the offset with regard to the DAP Controller PC time.

Index	Subnet	Netmask length	TTL	RPN range	Gatekeeper	Subnet name	Time offset	Country
1	192.168.1.0	24	1	010 - 04F	192.168.1.200...	Head Quarter	00:00	NL
2	192.168.40.0	24	1	050 - 07F	192.168.1.200...	Branch Office 1	00:00	NL

Figure 9-16 Multiple Subnets Settings

In this window you can right mouse click a line in the shown table. Then you can add, edit or delete a Branch Office configuration. The following items must be specified:

❍ Subnet

In almost all configurations, this is the subnet address. It is the first address in the subnet range, e.g. 192.168.1.0/24.

However, note that this subnet can also be an Aggregated Subnet. An “Aggregated Subnet” is a Virtual network definition which determines the network boundaries for an IP DECT Network in which seamless handover is possible AND which is running over more than one IP subnet, An Aggregated Subnet is a kind of “virtual” subnet that combines several real subnets
This is used when your IP DECT system is operational on one location on more than one subnet, with seamless handover.
All DAPs within the Aggregated Subnet allow seamless handover between each other, although they are spread over different real subnets with

Routers in between. So, if you have IP DECT running on more than one IP subnet, where seamless handover is required, you must calculate the Aggregated subnet and fill it in, in this window

Example of an Aggregated Subnet:
There are two subnets in which IP DECT is installed. The Router supports IP Multicast and there is seamless handover between the DAPs in different IP subnets. One subnet is 192.168.1.0/24 and the other is 192.168.4.0/24. The aggregated subnet is 192.168.0.0/21. This covers both subnets.

All subnet addresses outside the Aggregated subnet, will be regarded as Branch Offices.

✎ *The Aggregated Subnet, together with the Aggregated Subnet Mask are only applicable for IP DECT. So, never use Aggregated Subnet mask on your Network card or other network devices.*

❍ Mask Length

This is the subnet mask length, the number of bits used to identify the network part.
In general, this will be a real netmask length, applicable for one network segment.

Example:
When your subnet mask is 255.255.255.0, it means 24 bits for the network part and 8 bits to identify the host part. So, in this example you must fill in 24.

✎ *The Mask Length can be the Aggregated subnet mask length. See the bullet above (Subnet) where the Aggregated subnet is explained.*

❍ RPN range

Lowest RPN and highest RPN in this Branch Office.

✎ *Make sure that you enter all subnet. DAP in subnets, not included in this list will fail to complete the boot process.*

❍ 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”, Router(s) will not forward multicast traffic for the associated Multicast Group. If the Time to Live is higher than “1”, Router(s) will forward multicast traffic for the associated Multicast Group (depending on settings in a Router).
If you are using an Aggregated subnet (see bullet “Subnet” above), multicast routing is required between the different Subnets and therefore the TTL must be set to a value higher than 1 (advised 32).

If the subnet that you have filled in, is a real subnet, not Aggregated, you must make sure that the Time to Live is always 1.

❍ Gate Keeper

This is the Proxy address for the DAPs in this Subnet.

❍ Subnet name

Can be any given name. It is used to identify the Branch Office.

❍ Time Offset

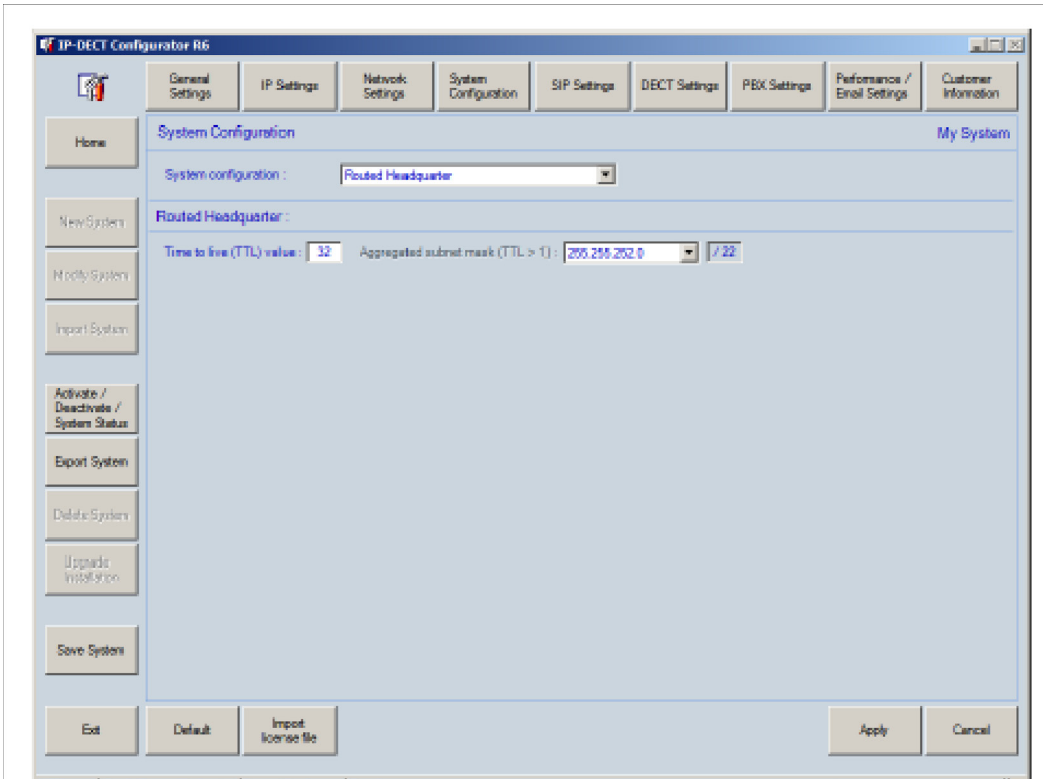
Self explaining.

❍ Country

This is important to make sure that the frequencies and tones are according to the country requirements

5.3 Routed Headquarter

In this configuration, there are more than one network segments in the Headquarter. The routers in this configuration must forward IP Multicast packages.



System Configuration My System

System configuration : Routed Headquarter

Routed Headquarter :

Time to live (TTL) value : 32 Aggregated subnet mask (TTL > 1) : 255.255.252.0 / 22

Figure 9-17 Routed Headquarter Settings

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.
Because you have selected the Router Head Quarter configuration, the Time to Live will always be higher than one. Advised value is 32.

❍ 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. 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. 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, refer to and .

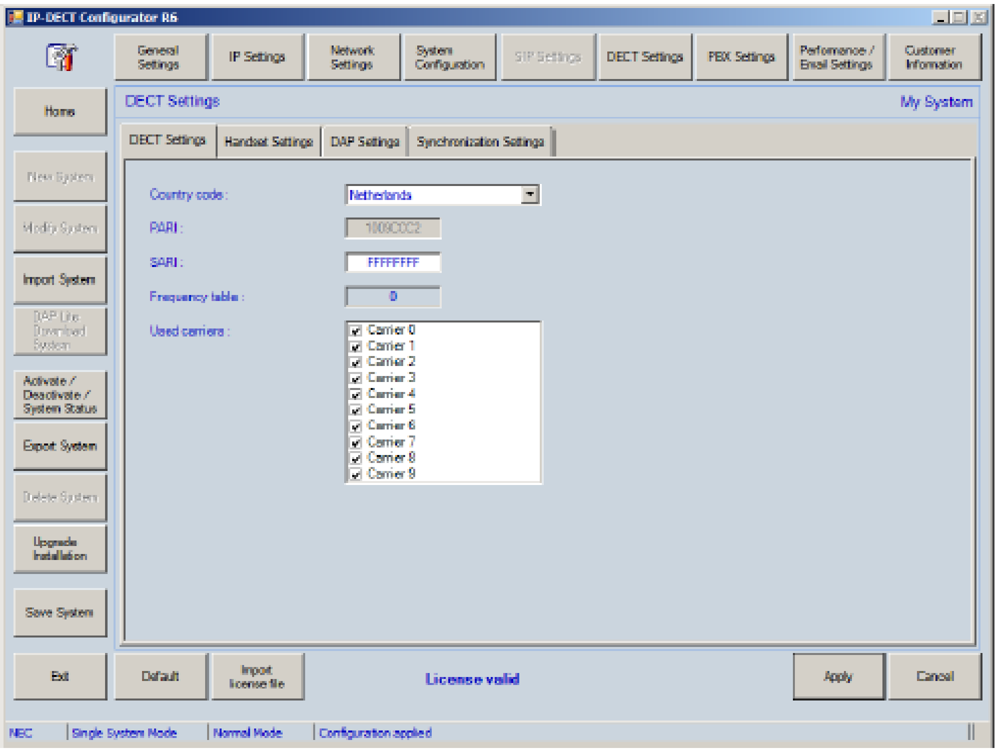
SECTION 6 SIP SETTINGS

Button is greyed out, due to the SV8300 being Protims-based.

SECTION 7 DECT SETTINGS

7.1 DECT Settings, tab “DECT Settings”

Please click the tab: DECT Settings. Now the following fields can be edited:



Country code : Netherlands

PARI : 1009C0C2

SARI : FFFFFFFF

Frequency table : 0

Used carriers :
☑ Carrier 0
☑ Carrier 1
☑ Carrier 2
☑ Carrier 3
☑ Carrier 4
☑ Carrier 5
☑ Carrier 6
☑ Carrier 7
☑ Carrier 8
☑ Carrier 9

License valid

NEC | Single System Mode | Normal Mode | Configuration applied

Figure 9-18 DECT Settings

- Country Code

  The Country code specifies the tone plan for IP DECT and also selects the correct frequency range and transmitter output power.

- PARI

  Primary Access Rights Identifier. This is the Unique DECT System Identifier. It is an 8 digit hexadecimal string. It is a worldwide Unique Identifier which you should have received together with your DECT system.

- 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”.

- ❍ Frequency Table

  This shows which DECT frequency range is used. This differs per part of the world.

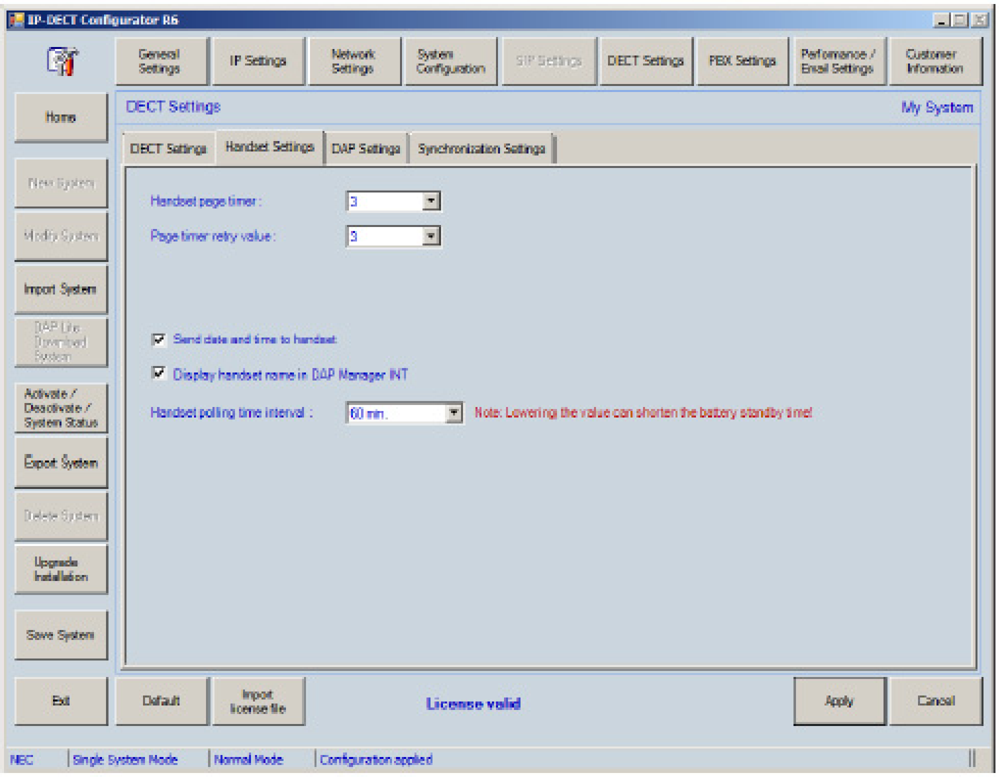
  Note that you cannot change the setting here, it is a result of the country that you have selected.

- ❍ 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.

7.2 DECT Settings, tab “Handset Settings”

Please click the tab: Handset Settings. Now the following fields can be edited:



DECT Settings — My System

Handset page timer : 3

Page timer retry value : 3

☑ Send date and time to handset

☑ Display handset name in DAP Manager INT

Handset polling time interval : 60 min. Note: Lowering the value can shorten the battery standby time!

License valid

NEC | Single System Mode | Normal Mode | Configuration applied

Figure 9-19 Handset Settings

- ❍ Handset Page Timer

  The Page Timer specifies the time in seconds between two page requests (retries).

- ❍ Page timer retry value

  The Page Retry Value specifies the maximum number of paging retries that are issued, if paging a handset fails.

- ❍ Send date and time to handset

  Self explaining.

- ❍ Display handset name in DAP Manager INT

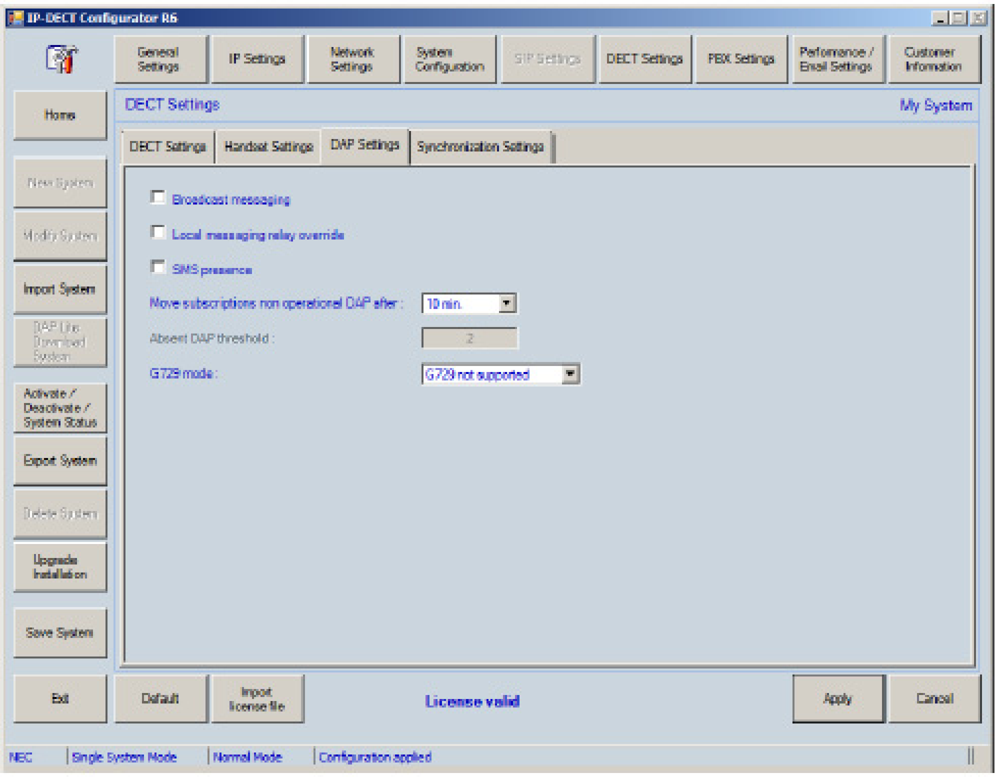
  When enabled, the handset name (if present in the handset) will be displayed in the DAP Manager, in the Subscriptions window, in the Comment field. The handset name will be displayed between brackets.

- ❍ Handset Polling time interval

  This is a mechanism to check if the handset is still reachable. Here you specify the polling interval time. If the handset is does not respond, it will be switched absent in the IP DECT system.

7.3 DECT Settings, tab “DAP Settings”

Please click the tab: DAP Settings. Now the following fields can be edited:



☐ Broadcast messaging

☐ Local messaging relay override

☐ SMS presence

Move subscriptions non operational DAP after : 10 min.

Absent DAP threshold : 2

G729 mode : G729 not supported

Figure 9-20 DAP Settings

- Broadcast Messaging

  This enables broadcast messaging.

- Local Message relay override

  When “Local Message Override” is not checked, and the TCP/IP DECT Messaging port (default 28001) is in state “Connected” (from e.g. a Messaging device) it is not possible to do handset-to-handset messaging anymore without intervention of an external messaging system. However, if you check the “Local Message override” check box, handset-to-handset messaging remains possible even if the TCP/IP port is in the state “connected”. This setting can be required for the messaging functionality of “Business Connect” however, it should not be checked in case of the Messenger@Net.

- SMS Presence

  Send the absent/present status to dedicated applications via DMLS.

- Move subscriptions non operational DAP after

  When a DAP is down and the DAP Controller is up- and-running the subscription records from that DAP will be moved to other DAPs. The time interval can be specified here.

- Absent DAP Threshold

  When the number of absent DAPs is more than 2, the subscription data will NOT be moved to other DAPs.
  Please note that this is a fixed system parameter, and cannot be changed.

- G729 mode:

  The following items can be selected:

  - **Use G729 when required** = Setting as in previous versions of IP DECT. G.729 used in case of connection to Branch Office DAPs.

    ✎ G.729 voice compression (G7A unit installed in AP300/ AP400) could be the answer for applying DECT in networks with limited bandwidth. The downside however is that the voice quality will be less compared to uncompressed voice. But under more demanding circumstances like environments with background noise, the voice quality may become unacceptable if used in combination with G.729. Therefore we advise not to apply G.729 on sites with a background noise.

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

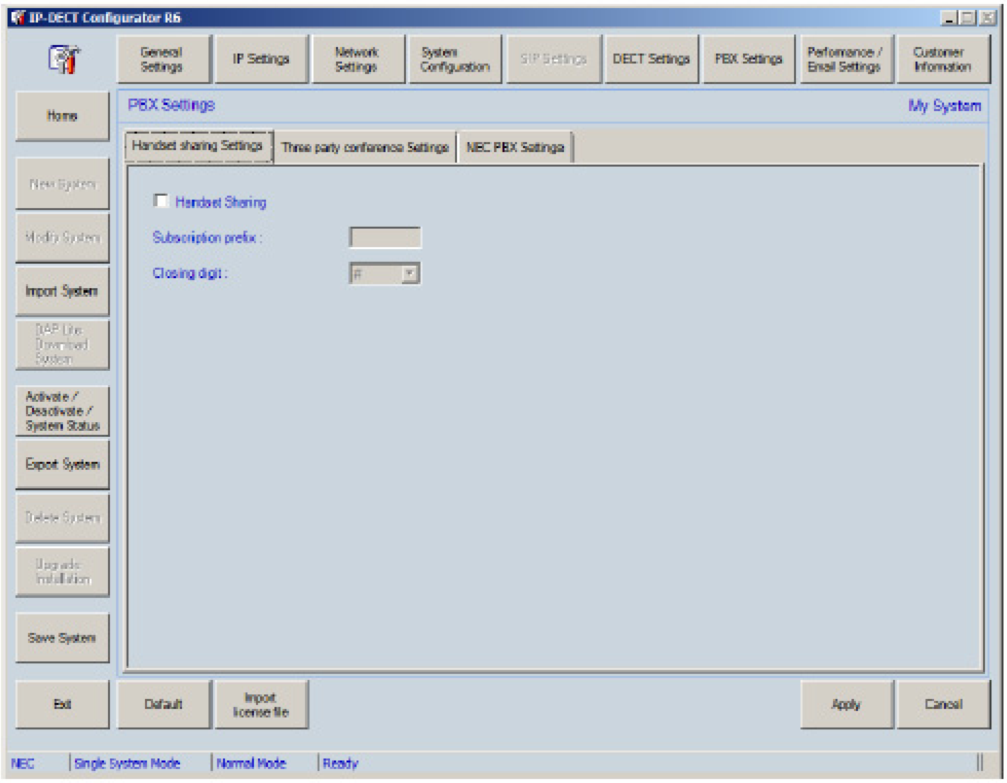
7.4 DECT Settings, tab “Synchronization Settings”

When you see a tab called “Synchronization Settings”, it indicates that you have a license for IP DECT in an environment with a lot of metal causing reflections. The license offers additional functionality to reduce the effects of the reflections. However, it is only available on “Project Base” which means that it has to be installed by special maintenance engineers. Therefore, the Synchronization Settings window is not explained here.

SECTION 8 PBX SETTINGS

8.1 PBX Settings, tab “Handset Sharing”

When you click the "Handset Sharing" tab , the following window is displayed:



☐ Handset Sharing

Subscription prefix :

Closing digit : #

Figure 9-21 Handset Sharing Settings

- ❍ Handset sharing

  Checking this box, enables Portable/handset sharing, refer to .

- Subscription prefix

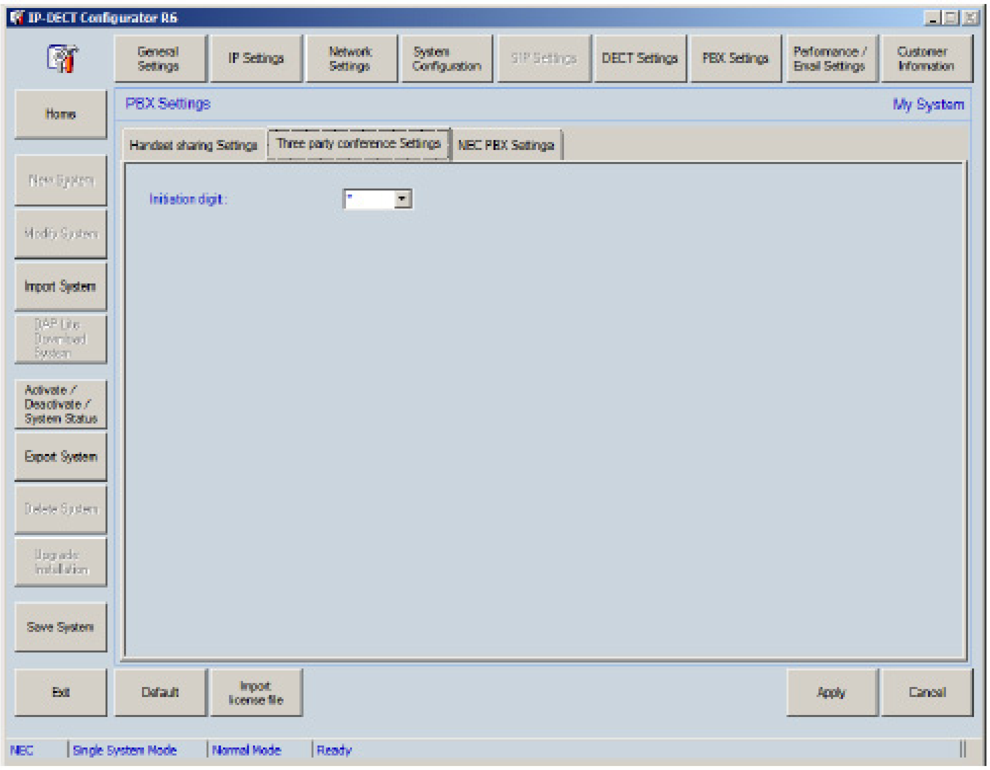
  First digit(s) of the subscribed number. If the first digit(s) of a subscription matches with the digit(s) defined here, the handset is enabled for portable sharing.

- 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.

8.2 PBX Settings, tab “Three Party Conference Settings”

When you click the "Three party conference Settings" tab, the following window is displayed:



Initiation digit : *

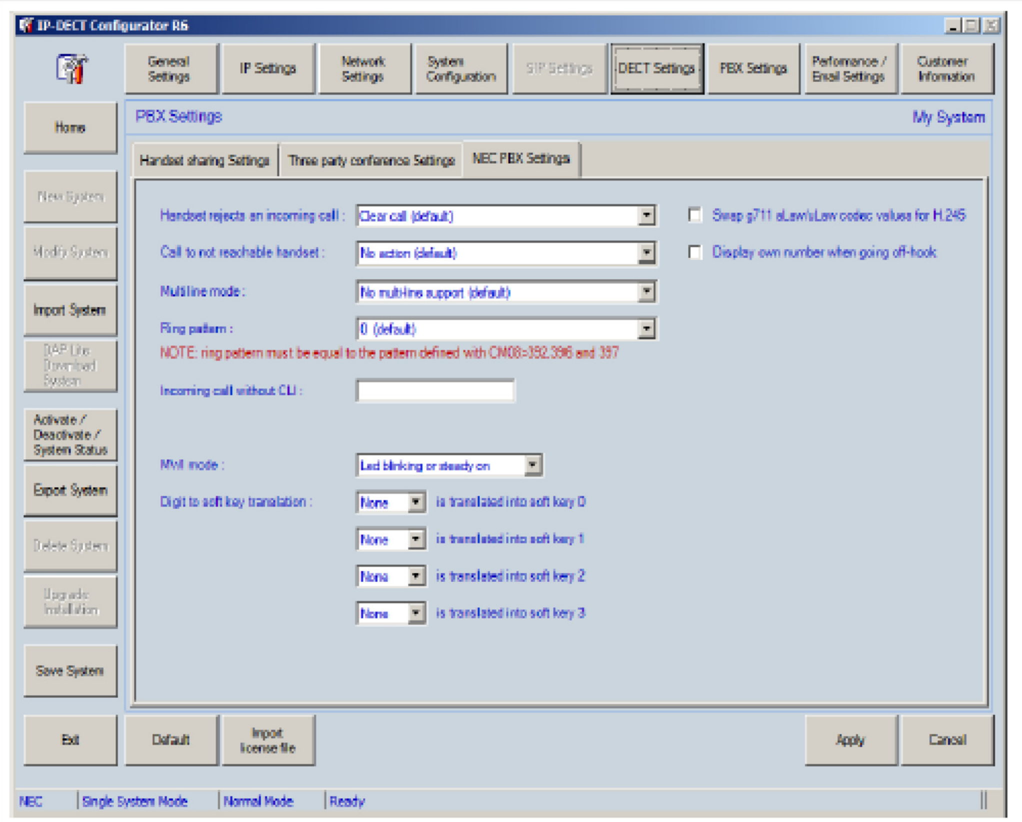
Figure 9-22 Three Party Conference Settings

- Initiation digit

  Digit that must be dialled to start the three party conference. The default setting is: *.

8.3 PBX Settings, tab “NEC PBX Settings”

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



Handset rejects an incoming call : Clear call (default)

Call to not reachable handset : No action (default)

Multiline mode : No multi-line support (default)

Ring pattern : 0 (default)

NOTE: ring pattern must be equal to the pattern defined with CM08>352.396 and 397

Incoming call without CLI :

MWI mode : Led blinking or steady on

Digit to soft key translation : None is translated into soft key 0

None is translated into soft key 1

None is translated into soft key 2

None is translated into soft key 3

☐ Swap g711 aLaw/uLaw codec values for H.245

☐ Display own number when going off-hook

Figure 9-23 NEC PBX Settings

The following items can be set or changed:

❍ Handset rejects an incoming call:

Select the preferred action in case the handset rejects an incoming call.

❍ Call to not reachable handset:

Select the preferred action in case the handset is not reachable.

❍ Multiline mode

In the multi line mode, you can select:

❒ Multiline enabled

Multiline mode for MRGs up to three members.

- ❐ Multiline with line pre-selection

  When there is a call, the CLI of the calling party is displayed and the call can be picked up by means of the off-hook key. After a certain time, the call can only be picked up by means of the line key.

- ❐ Multi line with pre-selection only

  The call can only be picked up by means of a line key.

- ❐ Multiline enabled with delayed setup and release for MRG

  This should be used for MRG with more than 3 members.

  ✎ The number of members in a Multiple Ring Group should not be more than 4 when the members are located in the environment of one DAP. When spread over a number of DAPs, the maximum number of members per MRG is limited to 10.

- ❍ Ring Pattern

  Select the required ring pattern. Note that this must comply with CM08>392, 396, 397.

- ❍ Incoming call without CLI

  When there is an incoming call without CLI, the information entered in this field will be displayed on the handset.

- ❍ MWI mode:

  For SV8300, this setting must always be set to “Led Steady on”!

- ❍ Digit to Softkey translation

  This simulates the function of the softkeys on an IP DTerm *when having busy tone*.

- ❍ Swap g711aLaw/uLaw CODEC values for H.245.

  This is only applicable for the 2000IPS in combination with IP D-Terms from the years 2003 and 2004.In those versions, the aLaw and uLaw notations were swapped. So, when aLaw was requested, uLaw was actually performed. If you do not get speech between IP DECT and IP D-Terms from the years 2003 and 2004, you should check this box, in order to swap the aLaw and uLaw CODEC. values.

- ❍ Display own number when going off-hook.

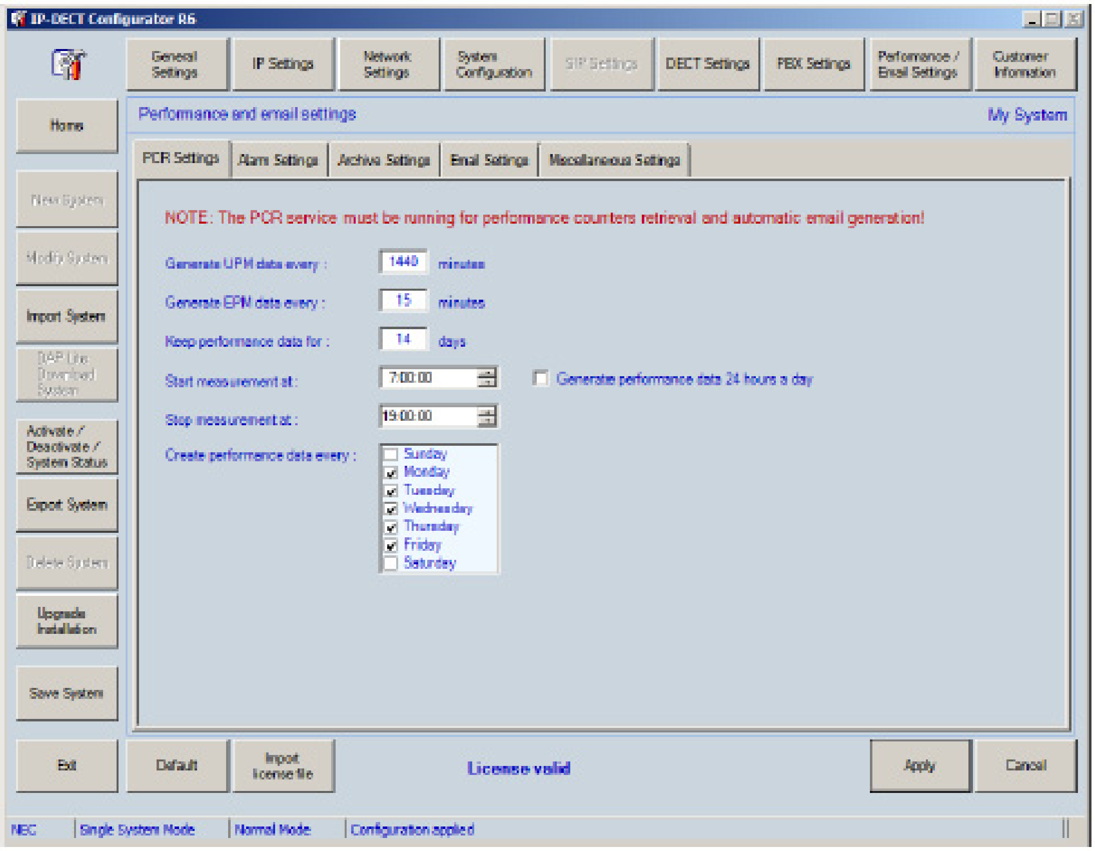
Self explaining.

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

SECTION 9 PERFORMANCE / E-MAIL SETTINGS

9.1 Performance / E-mail Settings, tab “PCR Settings”

When you click the “PCR Settings” tab, the following window is displayed:



NOTE: The PCR service must be running for performance counters retrieval and automatic email generation!

Generate UPM data every : 1440 minutes

Generate EPM data every : 15 minutes

Keep performance data for : 14 days

Start measurement at : 7:00:00 □ Generate performance data 24 hours a day

Stop measurement at : 19:00:00

Create performance data every :
□ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
□ Saturday

License valid

NEC | Single System Mode | Normal Mode | Configuration applied

Figure 9-24 PCR Settings

The following parameters are available:

- 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.

❍ Keep Performance data for . . . days

Number of days that the performance data should be kept on the Hard Disk.

❍ Start measurement at:

Each day performance measurement should take place, the performance measurement will start at the time specified here.

❍ Stop measurement at:

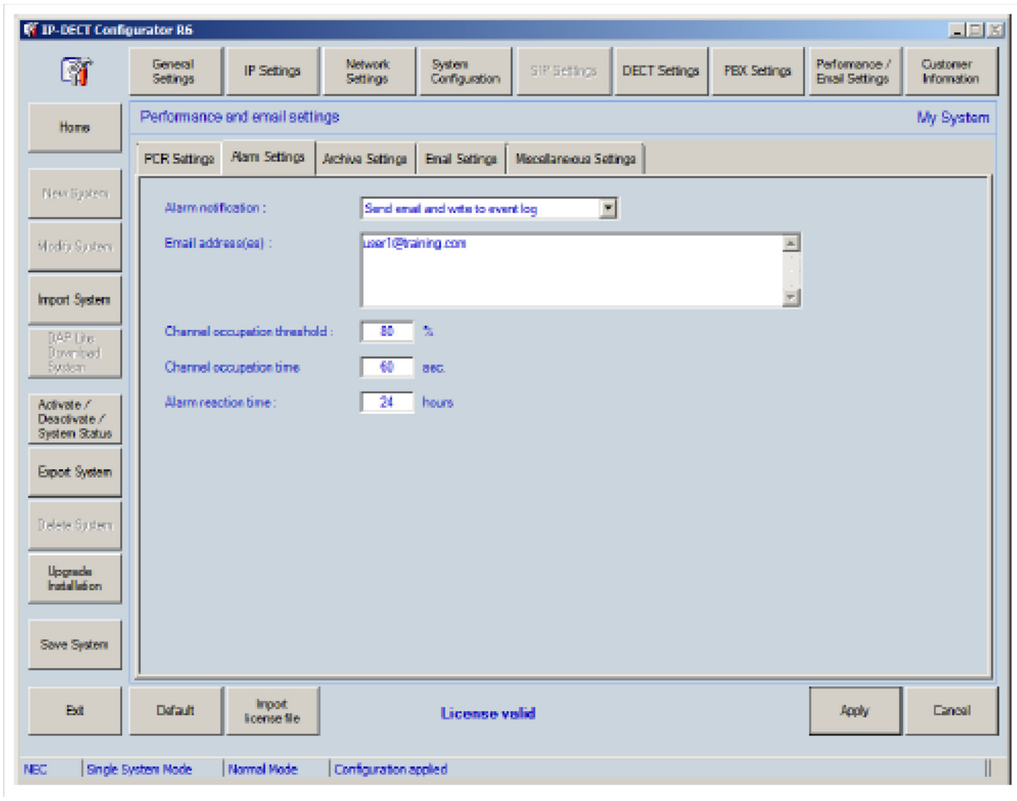
Each day performance measurement should take place, the performance measurement will stop at the time specified here.

❍ Create Performance counters every:

Specify the days that performance counter retrieval should take place.

9.2 Performance / E-mail Settings, tab “Alarm Settings”

When you click the “Alarm Settings” tab, the following window is displayed:



Alarm notification : Send email and write to event log

Email address(es) : user1@training.com

Channel occupation threshold : 80 %

Channel occupation time 60 sec.

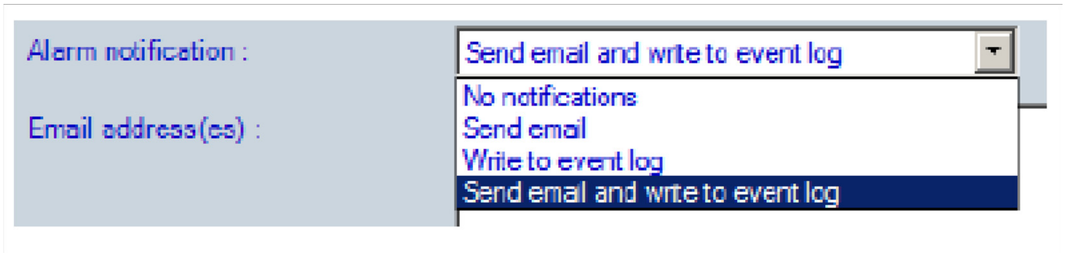
Alarm reaction time : 24 hours

Figure 9-25 Alarm Settings

E-mails can be send automatically when a DAP goes down or when the channel occupation threshold is exceeded for more than a number of seconds or when the DDS goes down. Note that this will only work when the PCR service is running on the DAP Controller/Manager PC.

❍ Alarm Notification

Alarm notification can be send as an e-mail and/or to the Windows Event Log. Please not that it is possible to convert the events, written to the event log, into SNMP Traps (consult the Advanced Data Manual.)



Alarm notification : Send email and write to event log

Email address(es) :

Figure 9-26 Alarm Notification

- E-mail addresses

  Enter the destination email address(es). Note that you can enter more than one email address. Separate the individual addresses with a ; (semi colon).

- Channel occupation Threshold

  If the channel occupation is higher than this percentage of the available channels for a specified time period, an email and or Event is generated. The threshold is specified in percentage, the time is specified in minutes.

- Channel occupation time

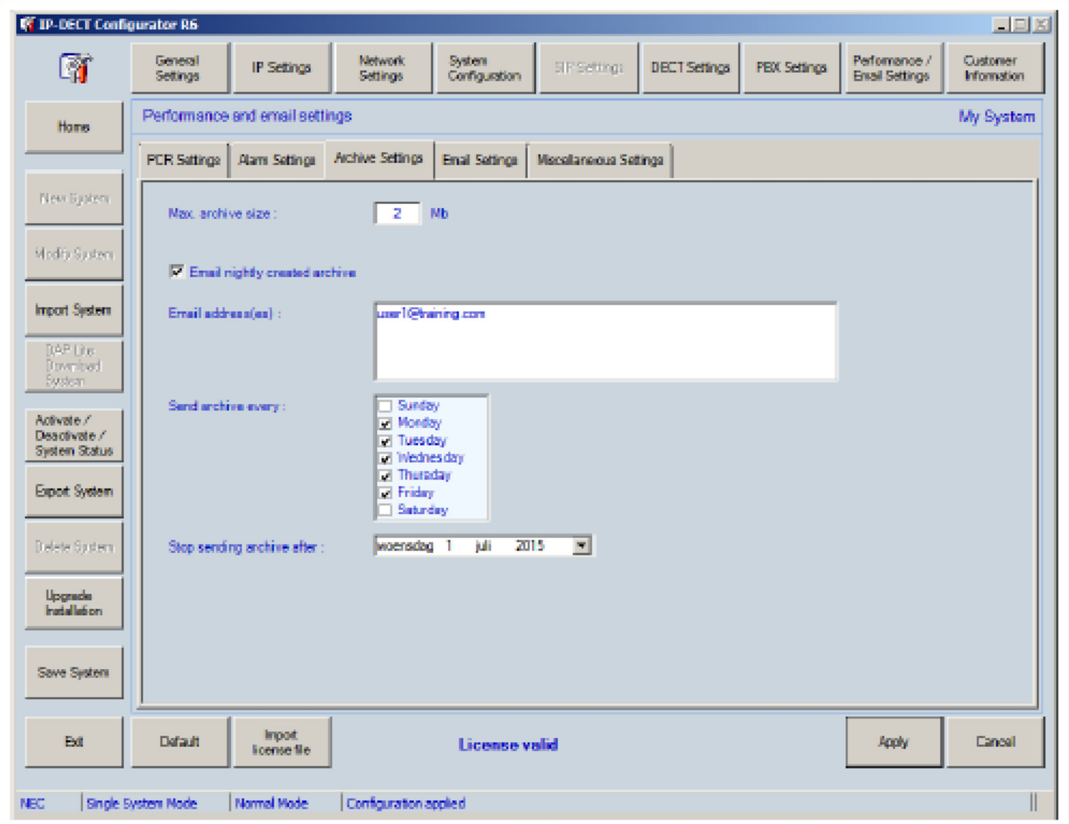
  If the channel occupation is higher than a percentage of the available channels for a specified time period, an email is generated. The time is specified in minutes.

- 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.

9.3 Performance / E-mail Settings, tab “Archive Settings”

When you click the “Archive Settings” tab, the following window is displayed:



Performance and email settings

Max. archive size : 2 Mb

☑ Email nightly created archive

Email address(es) : user1@training.com

Send archive every :
☐ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☐ Saturday

Stop sending archive after : woensdag 1 juli 2015

License valid

NEC | Single System Mode | Normal Mode | Configuration applied

Figure 9-27 Archive Settings

The following parameters can be adjusted:

- Max. attachment size

  This is the maximum attachment size. If the archive is larger than the size specified here, it will be chopped into pieces of the specified size.

- E-mail nightly created archive

  This enables automatic sending an email with the nightly created archive file as attachment.

- E-mail address(es)

  Enter the destination email address(es) as destination for the nightly created archive. Note that you can enter more than one email address separated by ; (semi colon).

- ❍ Send archive every

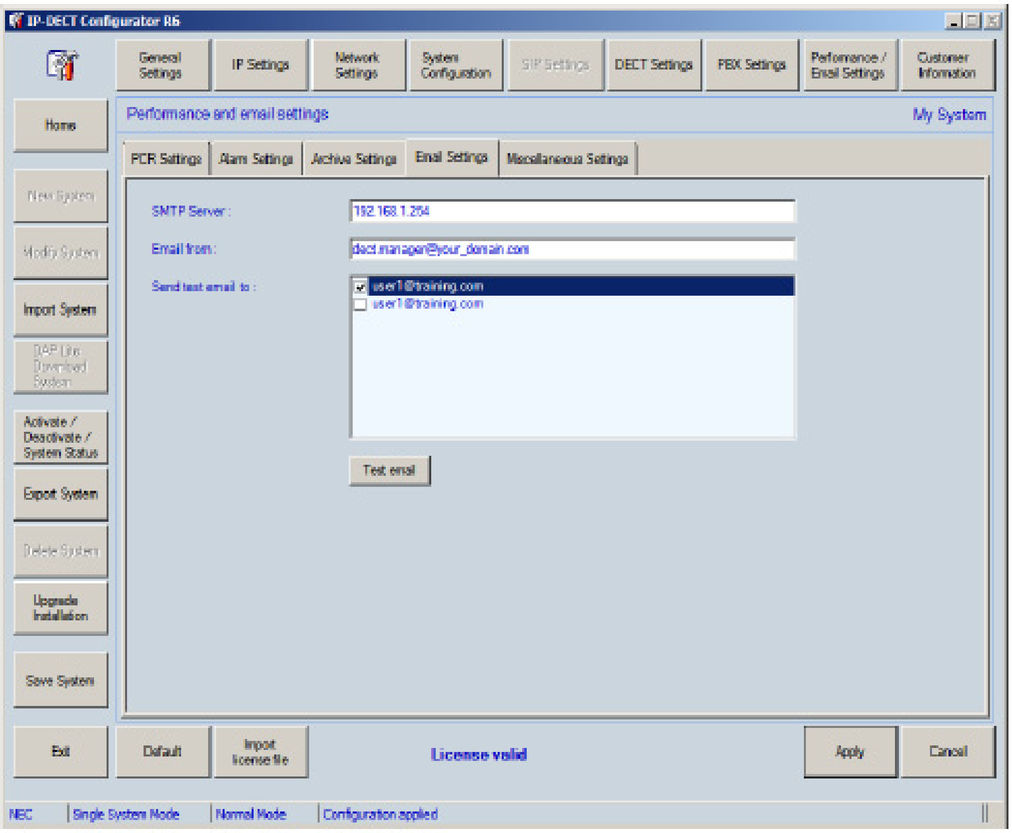
  Specify the days that the Archive should be send.

- ❍ Stop sending archive after

  After this date, archives are not automatically sent anymore.

9.4 Performance / E-mail Settings, tab “E-mail Settings”

When you click the “E-mail Settings” tab, the following window is displayed:



SMTP Server : 192.168.1.254

Email from : dect.manager@your_domain.com

Send test email to :
☑ user1@training.com
□ user1@training.com

Figure 9-28 E-Mail Settings

The following items are available:

- ❍ SMTP Server

  Enter the DNS name or the IP address of the SMTP mail server.

- ❍ E-mail 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.

- ❍ Send test e-mail to

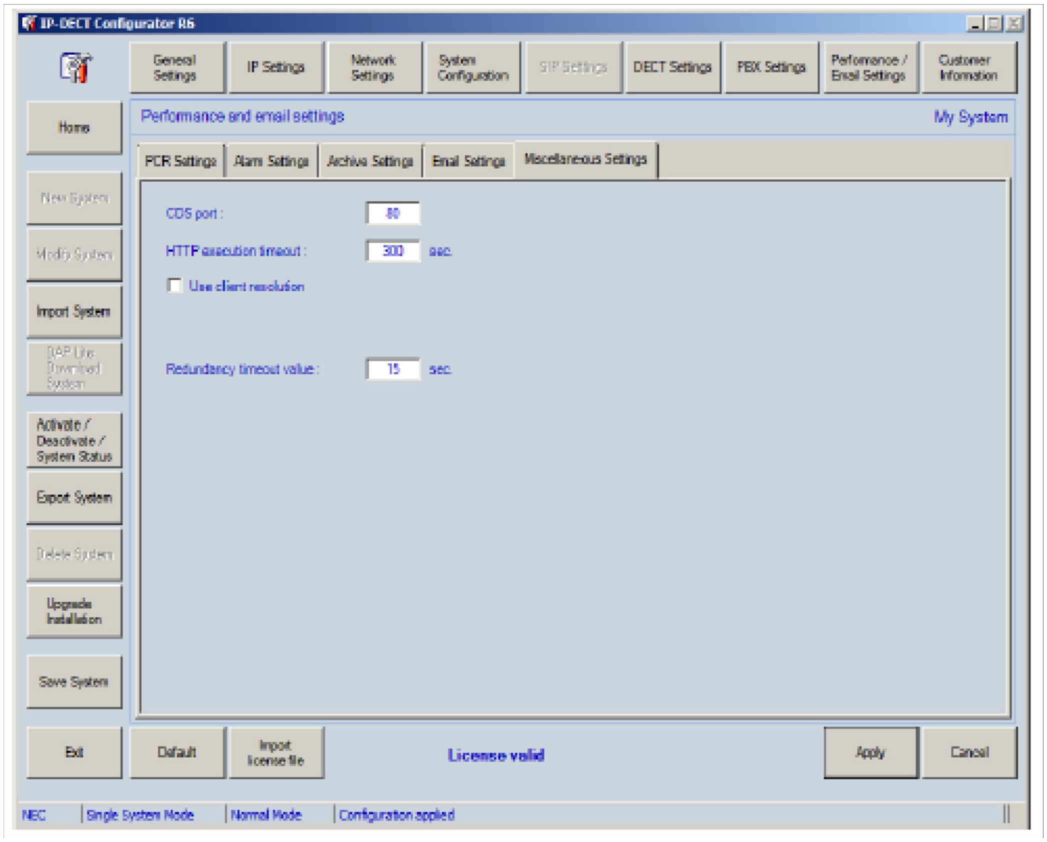
  Select the addresses to which an e-mail should be send. Please note that these addresses come from the Alarm Settings and Archive settings.

- ❍ Test e-mail

  Click this button to send an email to the addresses that have checked checkboxes.

9.5 Performance / E-mail Settings, tab “Miscellaneous Settings”

When you click the “Miscellaneous” tab, the following window is displayed:



CDS port : 80

HTTP execution timeout : 300 sec.

☐ Use client resolution

Redundancy timeout value : 15 sec.

License valid

NEC | Single System Mode | Normal Mode | Configuration applied

Figure 9-29 Miscellaneous Settings

❍ CDS port

Here you can change the port number of the CDS. The CDS takes care of showing the WEB pages. When you change the port here, the port of the WEB server (IIS) for CDS is changed. This means that you must enter the new port number in the URL that you use to reach the WEB page. .

❍ HTTP execution time out

This is a guarding timer for the ASP scripts. E.g. if the ASP web pages try to send an archive and it takes longer than the time specified here, it will be terminated.

The time is specified in seconds.

- ❍ Use client resolution

  If you check this box, you cannot scroll anymore through lists but the available information is chopped up into pages. You can select pages using tabs. If this box is unchecked, information is presented in a way that you can scroll through it using the scroll bar. Note the information is still chopped up into pages, but the pages contain (much) more information.

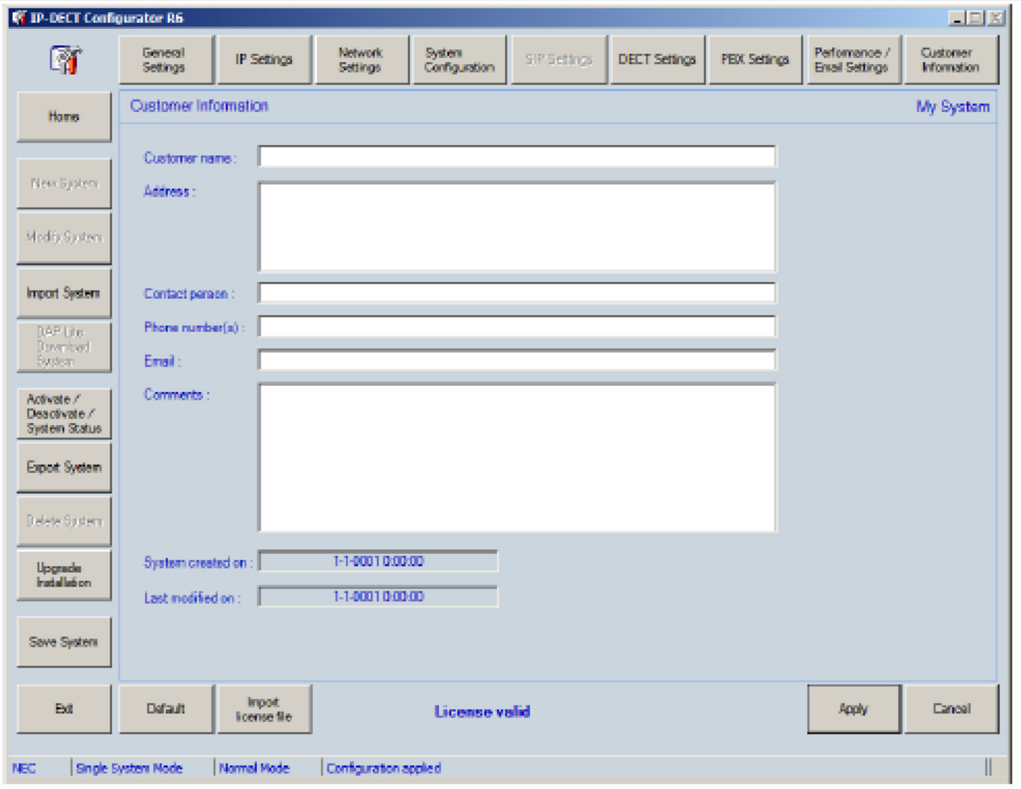
- ❍ Redundancy Time out value

  This value is the polling time from the DAPs to the DAP Controller. When it times out, the DAPs will try to connect to another redundant DAP Controller.

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

SECTION 10 CUSTOMER INFORMATION

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



Customer Information My System

Customer name :

Address :

Contact person :

Phone number(s) :

Email :

Comments :

System created on : 1-1-0001 0:00:00

Last modified on : 1-1-0001 0:00:00

Figure 9-30 Customer Information

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 Section 11 Save System and Start System.

SECTION 11 SAVE SYSTEM AND START SYSTEM

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

✎ *If you use another TFTP server or DHCP server than the build in TFTP/DHCP server, consult Chapter 5, first..*

1. Click the **Save System** button (left side of the DAP Configurator window), to save the changes you have made.
2. If the firmware file is not yet in the TFTP directory, copy the firmware file(s) `4910avxx.dwl` (AP300) and/or `4920avxx.dwl (AP400)` into the TFTP directory. When having AP400, also copy the Loader file `49920111.dwl` into the TFTP directory. This directory will normally be the following directory:
   `C:\Documents and Settings\All Users\Application Data\Nec\DAP Controller\<system name>\.`
   When you are using Windows 7 or Windows 2008, the directory is:
   `C:\ProgramData\Nec\DAP Controller\<system 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 .

SECTION 12 FINISHING ADVICE

When the system is running correctly, generate a `visadm.txt` file (in the WEB Page `http://<DAP Controller IP Address>/cds/perfform.aspx`) and analyze the file, using the SyncAnalyser tool.

If necessary, re-arrange the synchronization structure.

SECTION 13 LICENSE HANDLING

13.1 Install a new License File

You can easily install a new license file by means of the “Import license file” which is available at the bottom side of the DAP Configurator.

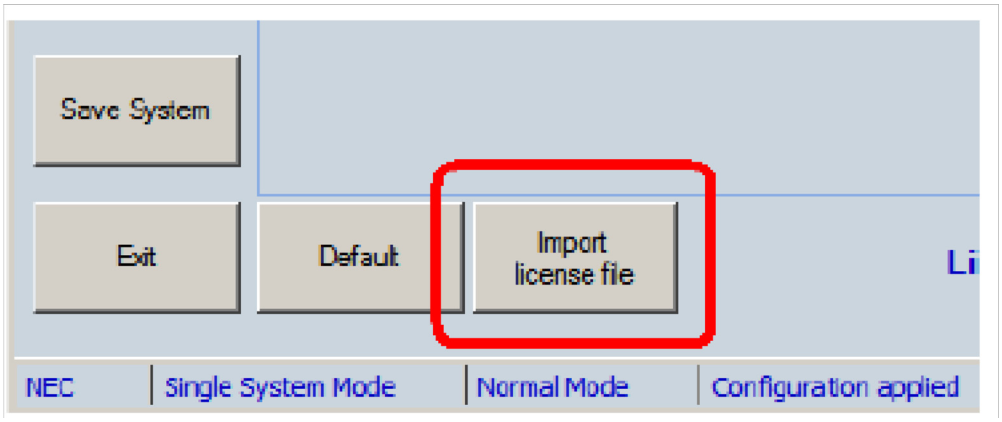
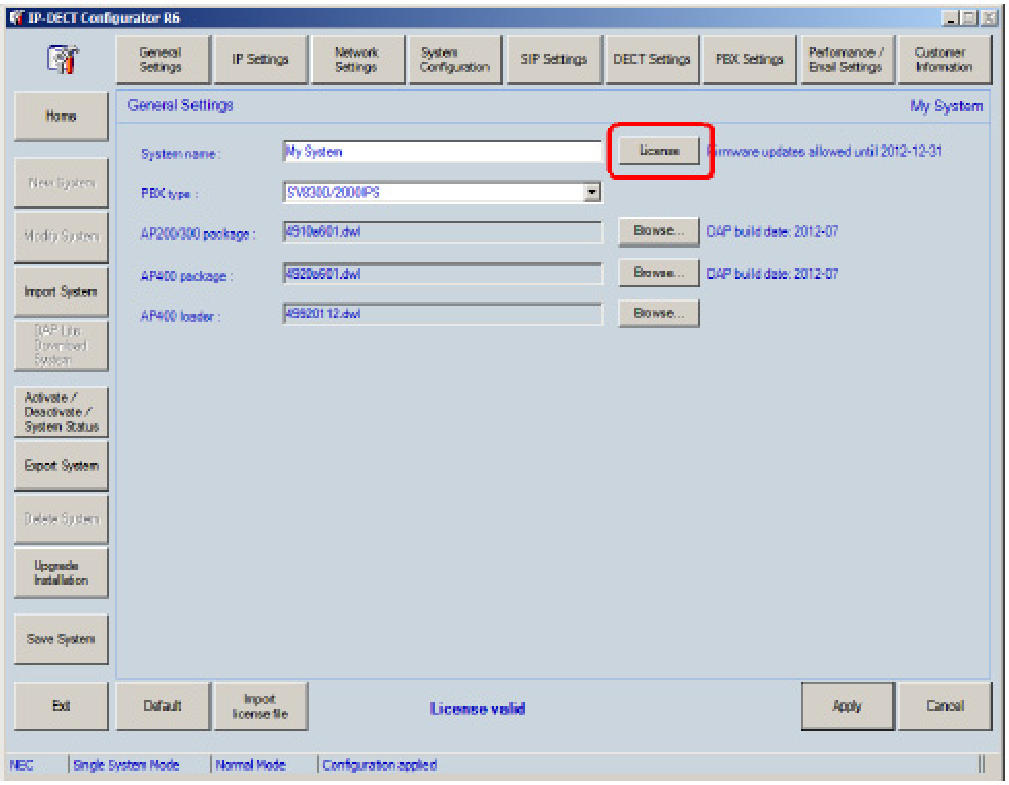


Figure 9-31 Import License File

The license file should have a file extension: `.txt`

13.2 Reading out the Licenses

You can read out the license data by means of the License button in the General Settings window.



General Settings — My System

System name : My System

Firmware updates allowed until 2012-12-31

PBX type : SV8300/2000IPS

AP200/300 package : 4910e601.dwl — DAP build date: 2012-07

AP400 package : 4920e601.dwl — DAP build date: 2012-07

AP400 loader : 4992012.dwl

License valid

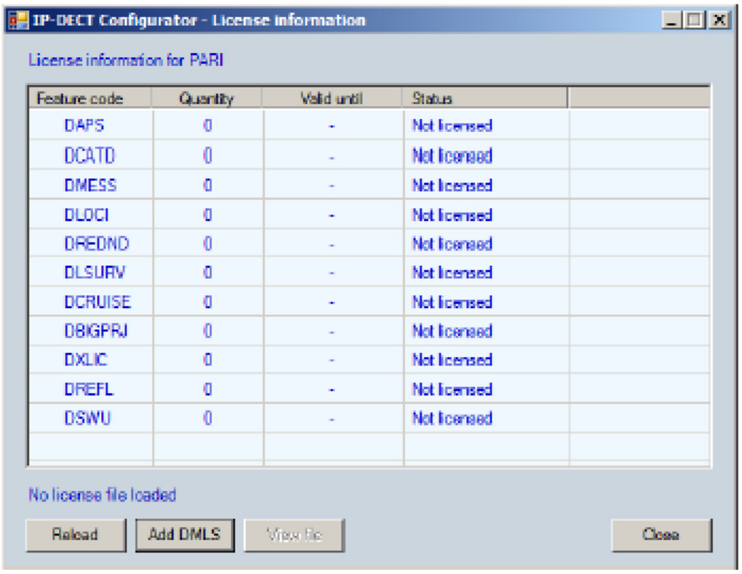
NEC | Single System Mode | Normal Mode | Configuration applied

Figure 9-32 License Information

When you click the button, you will see the licenses presented as shown in the following sub-section.

13.3 License Information Window

Below, two examples of the License information window.

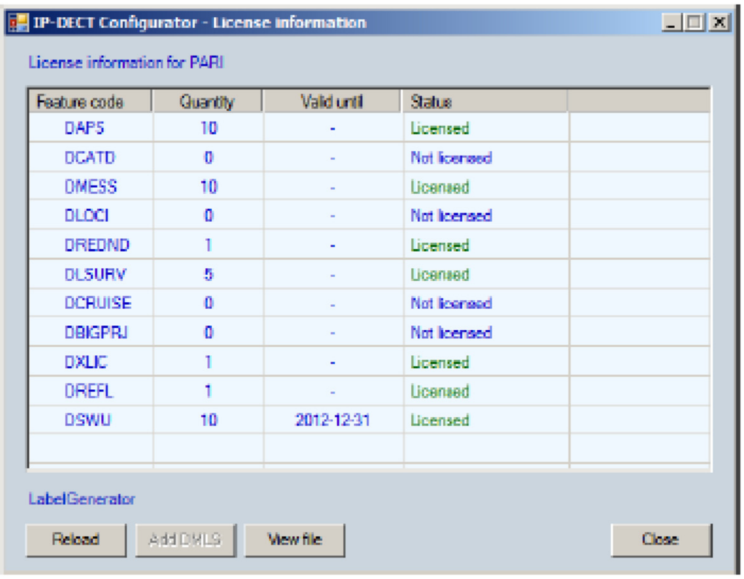


IP-DECT Configurator - License information

License information for PARI

Feature code	Quantity	Valid until	Status
DAPS	0	-	Not licensed
DCATD	0	-	Not licensed
DMESS	0	-	Not licensed
DLOCI	0	-	Not licensed
DREDND	0	-	Not licensed
DLSURV	0	-	Not licensed
DCRUISE	0	-	Not licensed
DBIGPRJ	0	-	Not licensed
DXLIC	0	-	Not licensed
DREFL	0	-	Not licensed
DSWU	0	-	Not licensed

No license file loaded



IP-DECT Configurator - License information

License information for PARI

Feature code	Quantity	Valid until	Status
DAPS	10	-	Licensed
DCATD	0	-	Not licensed
DMESS	10	-	Licensed
DLOCI	0	-	Not licensed
DREDND	1	-	Licensed
DLSURV	5	-	Licensed
DCRUISE	0	-	Not licensed
DBIGPRJ	0	-	Not licensed
DXLIC	1	-	Licensed
DREFL	1	-	Licensed
DSWU	10	2012-12-31	Licensed

LabelGenerator

Figure 9-33 License Information Window

The items in the windows have the following meaning:

Table 9-1 License Information

ITEM	EXPLANATION	LICENSE TYPE
DAPS	Number of DAPs allowed	Number of DAPs in steps of 10.
DCATD	*For Future use:* CAT-iq Data allowed	0= no 1= yes
DMESS	DECT Messaging allowed on DMLS.	Number of DAPs in steps of 10.
DLOCI	DECT Messaging and Location allowed on DMLS	Number of DAPs in steps of 10.
DREDND	DAP Controller Redundancy (Central DAP Controller)	0= no 1= yes
DLSURV	Survivability (Local DAP Controllers)	0 ... 10
DCRUIS E	Special functionality for Cruise Lines	0= no 1= yes
DBIGPRJ	Special functionality for configurations with more than 256 DAPs in one system with seamless hand-over.	0= no 1= yes
DREFL	Reflective environment license. Allows additional settings for reflective environments.	0= no 1= yes
DSWU	DECT software upgrade license.	Number of DAPs + expiry date.

✎ *Please note that the licenses DAPS, DMESS, DLOCI and DSWU are based on the number of DAPs.*

✎ *Licenses that are based on the number of DAPs must always have the same number of DAPs as licensed in the first item: DAPS. So, if the number of DAPS is 40, the other licenses (if required) that are based on the number of DAPs should be forty as well. They cannot be less than the number of DAPs.*

✎ *When you have a DMLS license for the DAP Controller License mechanism, the license information is automatically copied into the DMLS, when the DMLS starts up (make sure that you have the latest DMLS.)*
When you have a DMLS license for the DMLS itself, (to import into the DMLS directly), you can enter that license into the DAP Controller, by means of the button “Add DMLS”.

THIS PAGE INTENTIONALLY LEFT BLANK

Using Other TFTP Server 10

SECTION 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 paths etc. are automatically set correct. However, if you have chosen to use another TFTP server, paths must be set correct and files needs to be copied into the TFTP root directory. Consult the following section.

SECTION 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”

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.

Table 10-1 Overview of TFTP Servers

TFTP Server	Default Path	Preferred Path
3com	C:\Documents and Settings\All Users\Application Data\Nec\DAP Controller\<system name>\ OR for Windows 7 and 2008: C:\ProgramData\Nec\DAP Controller\<system name>	C:\Documents and Settings\All Users\Application Data\Nec\DAP Controller\<system name>\ OR for Windows 7 and 2008: C:\ProgramData\Nec\DAP Controller\<system name>
Windows	C:\tftpdroot\	C:\tftpdroot\
Other	Unknown	C:\Documents and Settings\All Users\Application Data\Nec\DAP Controller\<system name>\ OR for Windows 7 and 2008: C:\ProgramData\Nec\DAP Controller\<system name>
Other on other PC	unknown	unknown

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

❍ Firmware file: `4910avxx.dwl` (the one that you have specified in Section 2 General Settings on page 9-1.

❍ 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.

1. The `dapcfg.txt` file is by default stored in the directory: `C:\Documents and Settings\All Users\Application Data\Nec\DAP` Controller`\<system name>\`. OR when you are using Windows 7 or Windows 2008, the directory is `C:\ProgramData\Nec\DAP Controller\<system 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 another TFTP server, copy the `dapcfg.txt` from the directory `C:\Documents and Settings\All Users\Application Data\Nec\DAP Controller\<system name>\` to the TFTP directory that your TFTP Server is using as upload directory. For

Windows 7 or Windows 2008, the path is: `C:\ProgramData\Nec\DAP Controller\<system name>`

2. 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.
3. The DAPs should be able to start-up now.

THIS PAGE INTENTIONALLY LEFT BLANK

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”

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, assign licenses to your IP DECT system via the DECT Manager interface.

   ✎ *The DECT Manager interface is described in the IP 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. Note, that you cannot make phone calls when the SV8300 is not yet setup for IP DECT. Therefore continue with the next Chapter to setup the SV8300. After that, check that you can make phone calls.

THIS PAGE INTENTIONALLY LEFT BLANK

Setting Up The SV8300 Configuration 12

SECTION 1 IMPORTANT NOTES

In the SV8300, you must setup the configuration for IP extensions. An IP DECT extension behaves as if it is an IP Dterm. Before executing the procedure in the next section, read the following important notes.

✎ *Make sure that you have the sufficient licences for "IP Dterm" extensions. Each DECT telephone extension is regarded as one IP Dterm extension. If you do not have sufficient licenses, you can subscribe a handset, but you do not get dial tone when going off-hook. You do NOT get an error message either.*

✎ *An SV8300 can be equipped with a remote PIM. Generally, an IP DECT cluster is either assigned to the main system or to a remote PIM. If you need to have DECT in the main system and in the remote PIM, there are a few options:*

✎ *1. Install individual Business Mobility IP DECT systems on both: the main system and the remote PIM.*

✎ *2. Create a Branch Office configuration where Gate Keeper IP address in the Branch Office DAPs refer to the IPLA CPU) in the Remote PIM.*

✎ *Use the functionally of Multiple Gate Keepers. See Section* *3.4 IP Settings, tab “PBX IP Configuration” on page 9-7.*

SECTION 2 STEP-BY-STEP PROCEDURE

2.1 Setting Up SV8300

The following procedure guides you through setting up the SV8300 for Business Mobility IP DECT.

PROCEDURE:Setting up the SV8300

1. Make sure that the "Nation Code Assignment" is set to "Asia/Africa/ Europe/Latin America/Middle East/Russia".

   Use the following command for assigning the Nation Code:

   CM 310>0>05<Execute>

2. The IP DECT system uses automatic login for IP Dterms. For this automatic login it is necessary to set a the following system options correct.

   Use the following command to set the login to automatic login:

   CM 08>513>1<Execute>

   Use the following command to set disable station number encoding:

   CM 08>514>1<Execute>

   Use the following command to set disable password encoding:

   CM 08>515>0<Execute>

✎ *Although in the previous step password encryption is disabled, it is possible to enable password encryption (command: 08>515>1, but only if you use Proprietary password encryption (command: 08>517>1).*

✎ *Also Protected Login is supported. The password is the same as the Station Number.*

✎ *For more info on Login commands, consult 12.2.2. "Additional Info on Login in SV8300".*

3. Make sure that the SV8300 has a fixed IP address. If not, assign an IP address to the (IPLA in) SV8300. Also assign the subnet mask and default gateway address.

   Use the following command for assigning the IP address:

   CM 0B101>00><IP address><Execute>

   e.g. assign IP address 192.168.1.1

CM 0B101>00>192168001001<Execute>

Use the following command for assigning the subnet mask:

CM 0B101>01><subnet mask><Execute>

e.g. assign subnet mask 255.255.255.0

CM 0B101>01>255255255000<Execute>

Use the following command for assigning the IP address of the default gateway:

CM 0B101>02><default gateway><Execute>

e.g. assign default gateway 192.168.1.254.

CM 0B101>02>192168001254<Execute>

4. Make sure that the SV8300 has the default RAS (Registration Admission Status) UDP port. The default port number is 3456. (Normally this is OK.)

5. Assign the extension numbers (station numbers) of the DECT handsets to the Virtual Port Numbers. Use command CM1001. The command syntax is as follows:

   CM1001>ZZZZ>FXXXXXXXX<Execute>

   Where:

   `ZZZZ =` Virtual Port Number in the range 0000 ... 1499.

   `F =` Indicator that the extension is a Dterm (digital extension). Necessary for DECT extensions!

   `XXXXXXXX =` Extension number (DECT extension number).

   ✎ ***The command allows you to assign 8 digit numbers, however, IP DECT supports extension numbers of up to 6 digits Therefore do not use extension numbers with more than 6 digits.***

   Example of assigning extension number 300 to port number 0100:

   CM1001>0100>F300<Execute>

   (Make sure that the extension numbers that you assign are part of your internal numbering scheme, see command 200.)

6. When you assign a station number to a Virtual Port, the Prime line is assigned automatically. You don’t need to execute command 93 anymore, only if you want to check whether the Prime line is correctly assigned.

7. When you assign a station number to Virtual Ports, command 9000 automatically assigns the station number to line key 01.

   ✎ ***Because MyLine is automatically assigned to key 01 and IP DECT requires MyLine to be assigned to key 16, you must remove the MyLine from key 01 and assign it to key 16 for all IP DECT extensions.***

   Remove the Station numbers as "MyLine". Use command 9000. The command syntax is as follows:

   CM9000>ZZZZZZ,01>ZZZZZZ<Execute>

   Where:

   `ZZZZ =` Extension number / Station number. (Can be 1 to 6 digits)

   `01 =` Key number.

   Example of removing extension number 300 as MyLine from key 01:

   CM9000>300,01>CCC<Execute>

   Execute this command for all DECT extension/station numbers.

   Assign these Station numbers as "MyLine" to key 16. Use command 9000. The command syntax is as follows:

   CM9000>ZZZZZZ,16>ZZZZZZ<Execute>

   Where:

   `ZZZZ =` Extension number / Station number. (Can be 1 to 6 digits)

   `16 =` Key number. This must always be key number 16 for IP DECT!

   Example of assigning extension number 300 as MyLine:

   CM9000>300,16>300<Execute>

   Execute this command for all DECT extension/station numbers.

   ✎ ***Note that the following steps instruct you how to setup “Logout”. These steps are mandatory, even if you don’t use Logout.***

8. Assign the Logout code to each individual DECT Station number under key 15. Use command 9000.

   The command syntax is as follows:

   CM9000>ZZZZZZ,YY>F0B39<Execute>

   Where:

   `ZZZZ =` Extension number / Station number. (Can be 1 to 6 digits)

`YY =` Key number. This must be key number 15!

Example of assigning the Logout code to extension number 300:

CM9000>300,15>F0B39<Execute>

9. Allow “logout” in Service Restriction Class A.

   CM15143>15>0<Execute>

10. Assign this Service Restriction Class A to each individual DECT Station number.

    CM1202>”ext.nr”>1515<Execute>

    Example of assigning the Service Restriction Class A to extension number 300:

    CM1202>300>1515<Execute>

11. Allow “Call Forwarding-Logout” in Service Restriction Class C.

    CM15481>15>03<Execute>

12. Assign this Service Restriction Class C to the IP DECT Station numbers.

    CM1207>”ext.nr”>15<Execute>

    Example of assigning the Service Restriction Class C to extension number 300:

    CM1207>300>15<Execute>

    ✎ ***The following steps sets up the VoIP parameters in the SV8300. Be aware of the fact that this is just an example. The real setup of the Location Groups and CODEC list depends on the application of types of VoIP devices and trunk lines in the system.***

13. The following VoIP parameters must be set correctly in the SV8300:

    ❍ CODEC Priority:

    First priority = G.711 aLaw

    Second priority = G.729

    ❍ Payload: 40 msec.

    ✎ ***The advised payload is 40 msec. Other payload settings are possible, however, make sure that the payload is always equal for G.729 and G.711!***

    The following commands show an example for Location Group 00 and CODEC list 0.

Use command 42 for the CODEC settings:

`CM42>100>02<Execute>` set CODEC list "0" to G.711 and aLaw (first priority)

`CM42>101>04<Execute>` set CODEC list "0" to G.729 (second priority)

`CM42>110>04<Execute>` set CODEC list "0" to 40 msec. payload for G.711.

`CM42>111>04<Execute>` set CODEC list "0" to 40 msec. payload for G.729.

Use command 67 for the Location Group and CODEC list relation:

`CM6700>0000>0<Execute>` Location Group “00” to Location Group “00” uses CODEC list “0”.

By default, Location Group “00” is assigned to station numbers. To change this relation, use CM1239 (local) for DECT extensions. To change the “Location Group - IP-PAD” relation use CM0A09.

14. Save the data (CM>EC6) and reset the SV8300.

    After having entered the data, you must save the configuration data followed by a reset of the Main Processor (MP). Use PCPro to save the data and to execute a reset.

SECTION 3 ADDITIONAL INFO ON LOGIN IN SV8300

A DECT handset can login to the SV8300 using Automatic Login mode or Protected Login mode. The command structure is shown in Figure 12-1 "Login Structure in SV8300."

Note that when you use Protected Login mode, the password must be the same as the station number!

Note that when you use Automatic Login, a password is not required.

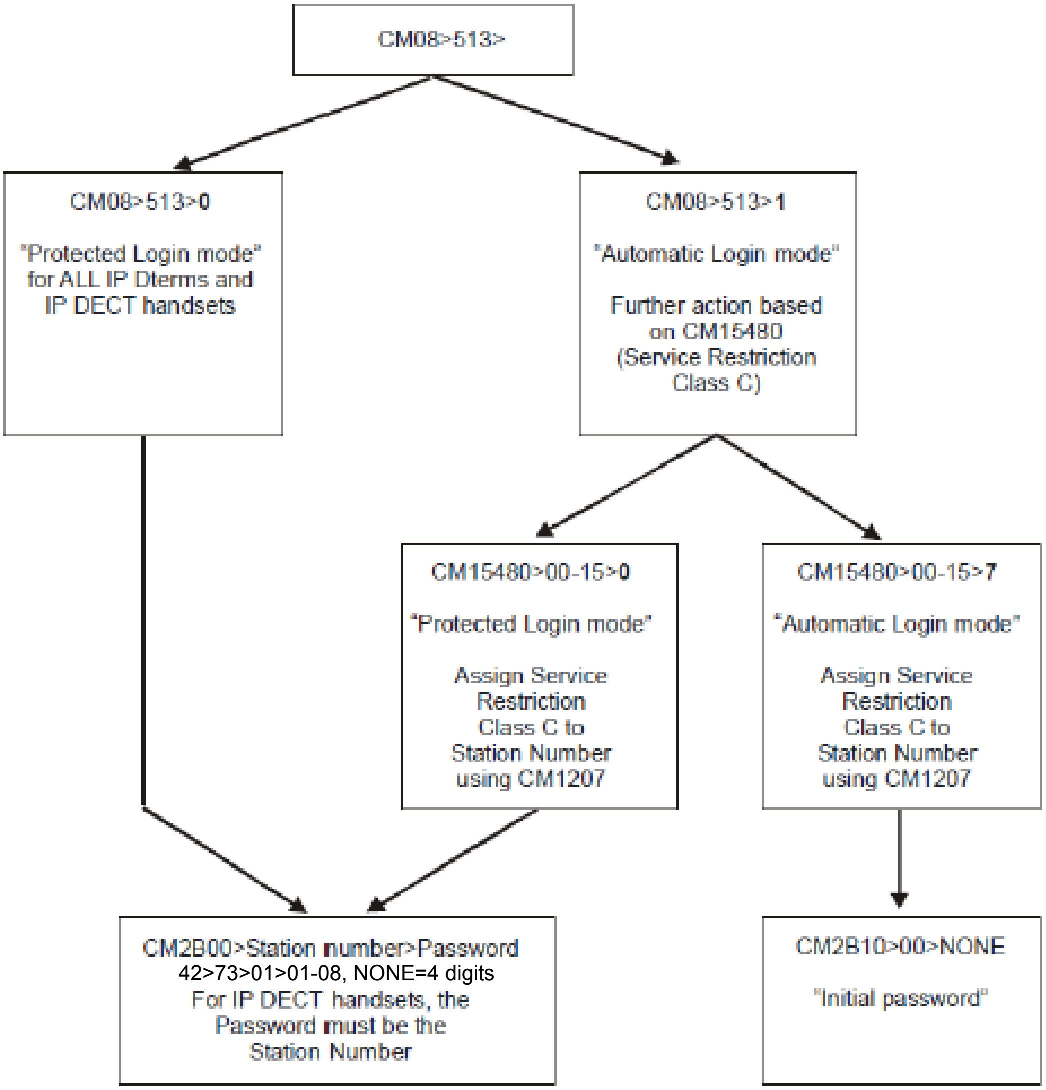

CM08>513>
CM08>513>0
"Protected Login mode" for ALL IP Dterms and IP DECT handsets
CM08>513>1
"Automatic Login mode"
Further action based on CM15480 (Service Restriction Class C)
CM15480>00-15>0
"Protected Login mode"
Assign Service Restriction Class C to Station Number using CM1207
CM15480>00-15>7
"Automatic Login mode"
Assign Service Restriction Class C to Station Number using CM1207
CM2B00>Station number>Password
42>73>01>01-08, NONE=4 digits
For IP DECT handsets, the Password must be the Station Number
CM2B10>00>NONE
"Initial password"

Figure 12-1 Login Structure in the SV8300

THIS PAGE INTENTIONALLY LEFT BLANK

Features (SV8300)

13

SECTION 1 LOGOUT FUNCTIONALITY

1.1 Logout Function

In the previous Chapter Setting Up The SV8300 Configuration, you have setup the SV8300 for IP DECT, including setting up the “Logout” functionality for IP DECT handsets. This subsection explains how “Logout” operates on IP DECT handsets.

Logout on IP DECT handsets works the same as Logout for IP Dterms. It can be used for Call Forwarding on Logout” and “Call Forwarding on not Reachable”. However, you cannot “Logout” using a “Logout” button. Instead, a DECT handset performs a Logout automatically under the following conditions:

❍ Switch off the DECT Handset

When you switch off a DECT handset, all new handset types from the year 2008 and onwards, it sends a detach signal to the DAP Controller/Manager. The DAP Controller/Manager sends a Logout command to the SV8300. This removes the MAC address for the handset from the SV8300. Logout is now active for the handset.

✎ ***This feature is only available on all new handset types from 2008 and onwards. Other types of DECT handsets are not capable of sending a detach signal.***

❍ DECT Handset in Charger and Silent Charging switched on

When you put a DECT handset, or all handset types from 2008 and onwards, in the charger, or charger rack, and "Silent Charging" is switched on in the handset, it sends a detach signal to the DAP Controller. The DAP Controller sends a Logout command to the SV8300. This removes the MAC address for the handset from the SV8300. Logout is now active for the handset.

✎ ***This feature is only applicable on all handset types from 2008 and onwards. All other types of DECT handsets are not capable of sending a detach signal and therefore do not support this feature.***

✎ ***Call Forwarding on Logout (not Reachable) will not be activated when the handset goes out of radio range. However, there is a polling mechanism that polls the all handsets to check whether the handsets are reachable. If the system detects that a handset is not reachable, a logout is sent to the SV8300. This mechanism is applicable for all handset types! Polling interval time depends on the system configuration and can be more than one hour.***

Logout is automatically enabled when you have executed the PROCEDURE: 2.1 Setting Up SV8300 on page 12-2. You can check correct operation of Logout using command 1290. The following procedure shows an example, how to check the logout function.

PROCEDURE: Checking Logout

1. Switch the handset off. After a few seconds, switch the handset on again.

2. Execute command CM1290 for the extension number of the handset:

   CM1290>”ext.nr”><DE>.

   When executing this command for extension 300 the command looks as follows:

   CM1290>300><DE>.

   The result should be as follows:

   1290>300:08066F300FFF

   The (virtual) MAC address that is displayed contains the Station number and indicates that the handset is logged in.

3. Switch off the handset and wait a few seconds. Then execute command CM1290 again.

   CM1290>”ext.nr”><DE>.

   When executing this command for extension 300 the command looks as follows:

   CM1290>300><DE>.

The result should be as follows:

1290>300:NONE

The (virtual) MAC address is erased which indicates that the handset is logged out.

SECTION 2 CALL FORWARDING ON LOGOUT / CALL FORWARDING NOT REACHABLE

Based on “Logout”, you can set a call forwarding relation (called: “Call Forwarding on Logout” or “Call Forwarding on not Reachable”). You must choose whether you want to set a fixed Call Forwarding destination or a Call Forwarding destination that can be set from the extension by means of dialling a prefix. Below you find an example of how to set a fixed destination.

CME606>”orig. ext.nr”>”dest. ext. nr”<Execute>

2.1 Twinning

2.1.1 General

It is possible to setup a twinning relation between two DECT handsets or between an IP DECT extension and a Dterm / IP Dterm. The following subssections explain how to setup the two configurations.

2.1.2 Twinning two DECT handsets

The following gives an example of a twinning relation between two DECT handsets.

Let us assume that there are two DECT handsets, station number 2000 and station number 2100.

PROCEDURE:Programming Twinning between DECT handsets.

1. Make sure that both extensions/handsets are setup correctly according to the procedures for setting up an IP DECT extension in the SV8300.
2. Assign MyLine 2000 to station number 2100 under key 8. (Key number must be in the range 1...8.)

   Use the following command:

   CM9000>2100,08>2000<Execute>

3. Assign MyLine 2100 to station number 2000 under key 8. (Key number must be in the range 1...8.)

   Use the following command:

   CM9000>2000,08>2100<Execute>

4. Allow “ringing line pickup” in Service Restriction Class C (in this example the default Service Restriction Class, 15).

   Use the following command:

   CM15082>15>0<Execute>

5. Allow “ringing line pickup by speaker button” in Service Restriction Class C (in this example the default Service Restriction Class, 15).

   Use the following command:

   CM15086>15>0<Execute>

6. Assign Station number 2000 to Service Restriction Class C (in this example the default Service Restriction Class, 15).

   Use the following command:

   CM1207>2000>15<Execute>

7. Assign Station number 2100 to Service Restriction Class C (in this example the default Service Restriction Class, 15).

   Use the following command:

   CM1207>2100>15<Execute>

8. Make sure that system option 199 is set to “1”. This allows Multi Line key functionality for incoming and outgoing calls. This is mandatory for IP DECT Release 5 systems with Multi Line configuration types 1 and 2.

   Use the following command to set option 199 to “1”

   CM 08>199>1<Execute>

9. Call pickup on Myline or on Prime Line. Select which type you want and execute the associated commands:

   ❍ Call pickup as MyLine

   With call pickup as MyLine, the extension that picked up the call will be busy. To set this configuration, use the following command for both handsets (as example).

   CM9004>2000,08>0<Execute>

```
CM9004>2100,08>0<Execute>
```

- ❍ Call pickup as PrimeLine

With call pickup as PrimeLine, the Prime Line number will be busy when a call is answered. To set this configuration, use the following command for both handsets (as example).

```
CM9004>2000,08>1<Execute>
CM9004>2100,08>1<Execute>
```

How does it work?

- ❍ When there is a call for station 2000, both handsets (2000 and 2100) starts ringing. Only on extension 2000, the CLI is displayed. On 2100 “Internal” is displayed. If 2000 answers the call, it will be “busy”, which means that a call to extension 2000 results in busy tone. However, if 2100 answers the call (on the Multi Line key) and a second call is coming in for extension 2100, extension 2000 doesn’t display the CLI but will start ringing.
- ❍ It is possible to pick up a call as if it is answered by the Prime Line. The following possibilities are available:

1. Call pickup as MyLine

   With call pickup as MyLine, the extension that picked up the call will be busy. To set this configuration, use command 9004.

2. Call pickup as PrimeLine

   With call pickup as PrimeLine, the Prime Line number will be busy when a call is answered. To set this configuration, use command 9004.

2.1.3 Twinning Relation between DECT Handset and (IP) Dterm

Twinning an IP Dterm and a DECT handset is the same as for twinning two DECT handsets. However, on the IP Dterm you can use any free key to assign the Myline.

✎ Twinning is possible for calls from internal and external when system option 199 is set to “1”. Always set this system option to “1” when using IP DECT Release 5!

In case you want to twin a DECT handset with a Dterm (or an IP Dterm) it can be useful to setup a configuration where the two lines behave as if it is one extension, which means behaving as if both have the same extension number. If one of the extensions sets up a call to a destination, the destination will show one Calling Line ID, independently from which extension the call is made. The following gives an example of a twinning relation between a DECT handset and an IP Dterm (or Dterm) as if they are one extension.

PROCEDURE:Twinning between DECT handset and (IP) Dterm, as if they are one extension.

Assumption: Station Number DECT Handset=1000. Station number (IP)Dterm=2000.

1. Make sure that both extensions are setup correctly and are operational.
2. Assign MyLine 2000 to (IP) Dterm (station number 2000) under key 1.

   Use the following command:

   CM9000>2000,01>2000<Execute>
3. Assign the DECT Handset as SubLine to the Dterm.

   Use the following command:

   CM9000>2000,02>1000<Execute>
4. Assign station number 1000 as Prime line to the (IP) Dterm. This means that subline 1000 is used when going off-hook or when the speaker button is pressed. This also causes that if one of the twinned extensions is busy on station number 1000, the other will be busy as well and cannot be used for phone calls.

   Use the following command:

   CM93>2000>1000<Execute>
5. You must program the CLI of the DECT handset for the (IP) Dterm in case of ISDN calls.

   Use the following command:

   CM1212>2000>1000<Execute>
6. Assign MyLine 2000 to station number 1000 under key 8. (Key number must be in the range 1...8.

   Use the following command:

   CM9000>1000,08>2000<Execute>

7. Allow “ringing line pickup” in Service Restriction Class C (in this example the default Service Restriction Class, 15).

   Use the following command:

   CM15082>15>0<Execute>

8. Allow “ringing line pickup by speaker button” in Service Restriction Class C (in this example the default Service Restriction Class, 15).

   Use the following command:

   CM15086>15>0<Execute>

9. Assign Station number 1000 to Service Restriction Class C (in this example the default Service Restriction Class, 15).

   Use the following command:

   CM1207>1000>15<Execute>

10. Assign Station number 2000 to Service Restriction Class C (in this example the default Service Restriction Class, 15).

    Use the following command:

    CM1207>2000>15<Execute>

How does it work?

The IP DECT handset and the (IP) Dterm now behave as two extensions sharing the same line. Internal and external calls towards 1000 will cause both extensions to start ringing. The Calling Line ID of the caller is displayed on both extensions. Either extension can answer the call.

If one of the extensions is busy, the other extension cannot be used for a call. When there is a call for one of the extensions while the other is busy, busy tone is send to the originator.

Calls originated from either extension will show the same CLI (1000).

Call forwarding activated on the (IP) Dterm can be deactivated on the IP DECT extension but not the other way round.

Station number 2000 should be handled as dummy number. Calls to 2000 will get ringback tone but cannot be answered.

MyLine number display should be disabled, otherwise number 2000 will be displayed on the (IP) Dterm.

SECTION 3 THREE/FOUR PARTY CONFERENCE

IP DECT supports three or four party conference. It makes use of the three/four party conferencing as available in the SV8300. Therefore, make sure that your SV8300 configuration/setup supports three/four party conference for IP phones.

PROCEDURE:How to setup a three party conference call

1. Setup a call to an extension.
2. When the call is active and you are in a conversation mode, press the “Enquiry” button (normally “R”) and dial the extension number of the third party that you want to involve.
3. When the third party answers the phone and the connection is established, press the * (star) key. This activates the three party conference.
4. If you want to add another party into the conference (four party conference), press the “Enquiry” button on your handset. Dial the fourth party that you want to involve. After the voice connection is established, press the * (star) key again, to activate the four party conference.

Important Remarks

❍ Speech path re-arrangement

❑At three party conference activation, the speech paths are disconnected and setup again. However, the user doesn’t notice it. Speech paths are not peer-to-peer, but will be routed via the SV8300 switching network, using the IP-PAD / IPLA.

❍ Digit for Activating the three party conference.

❑The digit for activating the three/four party conference is default * (star). You can change this using the DAP configurator tool.

SECTION 4 PORTABLE SHARING

4.1 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 SV8300. 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 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 I755, G266, G566 and later types of handsets, will 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 Disconnect” enabled.

  The handset type I755, G266, G566 and later types of handsets, will 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.

✎ When any type of handset 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 on I755, G266, G566 and later types of handsets. On other types of 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 station numbers in the 2000IPS/SV8300. These numbers must start with the same “prefix”. This prefix must be specified in the DAP Configurator and could be e.g. “00”.

4.2 How to Implement

✎ The numbers that you use for Portable Sharing may never be existing (subscription) handsets numbers. So you must always create extra Station numbers which can be used as a pool of Station numbers for handsets using Portable Sharing.

PROCEDURE:Implementing

1. Determine a subscription number range for the handsets that are you want to make available for Portable Sharing. This number range must be a range of numbers that does not exist in the SV8300!

2. e.g. You could use the number range 00100 . . . 00999 as subscription number range for portables that are designated to use Portable Sharing. Note that in this example, the “start” digits for the subscription numbers are “00”. You need to assign the start digits later on. Be aware of the fact that the actual station number is received from the SV8300 when the user executes the “Login”.

3. Start-up the DAP Configurator. Go to “PBX Settings” and then click the tab “Handset Sharing Settings”.

4. Check the checkbox “Handset Sharing” to enable Portable Sharing. In the field “Subscription Prefix” enter the stating digit(s) of the subscription number range that you have designated to Portable Sharing. Using the example in “step 1”, the prefix would be “00”.

5. The “closing digit” is a “#” by default. Generally this is always OK, do not change the default.

6. Click the “Apply” button and then click Save System”. Follow the instructions on the screen”.

7. Make sure that the `dapcfg.txt` file is stored in the TFTP directory for the DAPs. Now Reboot the DAPs

8. In the SV8300, assign all the Station Numbers that you want to make available for Portable Sharing as station numbers according to the procedures in Chapter 12, Setting Up The SV8300 Configuration. Note that these are the real station numbers and NOT the subscription numbers as in Step 1.

   Make sure that you have assigned the Logout functionality to key 15 of the stations numbers used for DECT.

9. When you go off-hook with a subscribed handset that is enabled for portable sharing, you should see the Login. Enter the Station number that you want to use and enter the closing digit (“#” by default). The handset should operate with the new station number now. Note that

Portable Sharing is only available on the handsets that are subscribed to the designated subscription number range for Portable Sharing. On other handsets the Portable Sharing functionality is not available.

10. To logout, refer to 1.1 Logout Function on page 13-1.

4.3 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 hard disk of the DAP Manager PC.

SECTION 5 “RECALL” BUTTON SIMULATION IN SHUTTLE CONDITION

In case of a call in a shuttle condition, you can disconnect from a third call by means of pressing the “Recall” button on a Dterm. However, IP DECT handsets do not have such a button. The # button on the DECT handset simulates the “Recall” button. The following example explains this functionality.

Example:

❍ Party “A” calls Party “B”.

❍ Party “B” puts party “A” on hold, using the “R” button.

❍ Party “B” calls party “C”, but party “C” has a CFA to its GSM/Cell Phone.

❍ The GSM/Cell Phone responds with the Voice Mail.

❍ Party “B” can will shuttle back to Party “A”, since it is useless to transfer Party “A” to a Voice Mail box. (The Voice Mail of the GSM/Cell phone is put in the hold condition.)

❍ If Party “B” hangs up the phone, Party “A” will be connected to the Voice Mail box of the GSM/Cell Phone which is useless! So, here, Party “B” should press the “Recall” button to terminate the call to the Voice Mail box and be transferred back to Party “A”. In case of a DECT phone, you do not have the “Recall” button. You must simulate the “Recall button”, by means of pressing the # button. (The # button simulates the function of the Recall button.)

SECTION 6 LED INDICATION ON HANDSET.

6.1 General

The LED indication on the handset may indicate “incoming call” and/or “voice message waiting”.

The SV8300 allows you to manipulate the behavior of the LED on the handset.

✎ A limited number of types of handsets support this feature. So, the availability of this feature depends on the type of handset.

6.2 LED Indication for Incoming Call

When you want to enable/disable the LED for incoming calls, use command 9003.

Example of disabling the LED indication on incoming call for station number 500:

For SV8300:

```
CM9003>500,16>0<Execute>
```

The example above, is applicable for line key 16. (Line key 16 should always be used for Myline, in case of IP DECT.) However, when you have sub line keys assigned as well, you must execute the same command but for the sub line key(s). See following example for key 3 on station number 500:

For SV8300:

```
CM9003>500,3>0<Execute>
```

6.3 LED Indication for Voice Message Waiting

To enable/disable the LED for Message Waiting, use command 1303.

See the following example to enable the LED for Voice Message Waiting for station number 500:

```
CM1303>500>0<Execute>
```

IP DECT Mobility In SV8300

14

SECTION 1 GENERAL

User Mobility allows a user to use one handset on both, the Main SV8300 and one or more Remote Units. The handset will keep its own Station Number, independently on where it is. Figure 14-1 User Mobility with IP DECT System with Branch Office(s) on page 14-3 shows the configuration of a SV8300 Main system and a Remote Unit with one IP DECT system with a Branch Office location in the Remote Site. There is a second possibility: using two IP DECT systems (with or without using a SARI). Refer to Figure 14-2 User Mobility with More Than One IP DECT System on page 14-4.

The IP DECT Mobility solution in a SV8300 with Remote Unit also supports Survivability. This means that when the Main Site cannot connect to the Remote Unit anymore, you can still use your handsets either in the Main Site or in the Remote Site. Even when the Main site goes down, you can still use the handsets in the Remote Unit. The same is true, when the Remote site goes down, you can still use the handsets in the Main Site. When the connection between the two Sites is restored, registration data is synchronized again between the two sites.

✎ *Make sure that you have sufficient licenses for the Remote Site. Use command F88>16> to read out the number of Remote Site licenses.*

✎ *The “Zenia” handset is not supported for IP DECT Mobility using a SARI.*

SECTION 2 SETTING UP THE CONFIGURATION IN SV8300

Setting up the configuration in the SV8300 for DECT Mobility is the same as for User Mobility in an SV8300 Remote Unit. Setting up such a configuration is described in the “SV8300 Networking Manual”, chapter “Remote Unit”. Please consult the SV8300 Networking Manual.

✎ *Once you have made changes in the Main Unit, do not forget to send the changes to the remote Unit, using the EC8 command.*

SECTION 3 SETTING UP USER MOBILITY IN IP DECT

In IP DECT, there are two configuration possibilities that can be used for User Mobility:

❍ One IP DECT System connected to the Main site SV8300 and one or more IP DECT Branch Office(s) connected to the Remote Unit(s).

❍ Individual IP DECT Systems (using a SARI), one the Main Site and another on the Remote Unit.

3.1 IP DECT System with Branch Offices

In Figure 14-1 User Mobility with IP DECT System with Branch Office(s) an IP DECT System with one Branch Office is shown. Note that the DAP Manager must always be connected, because there are Branch Offices involved and the handsets will move between the Head Quarter and the Branch Offices.

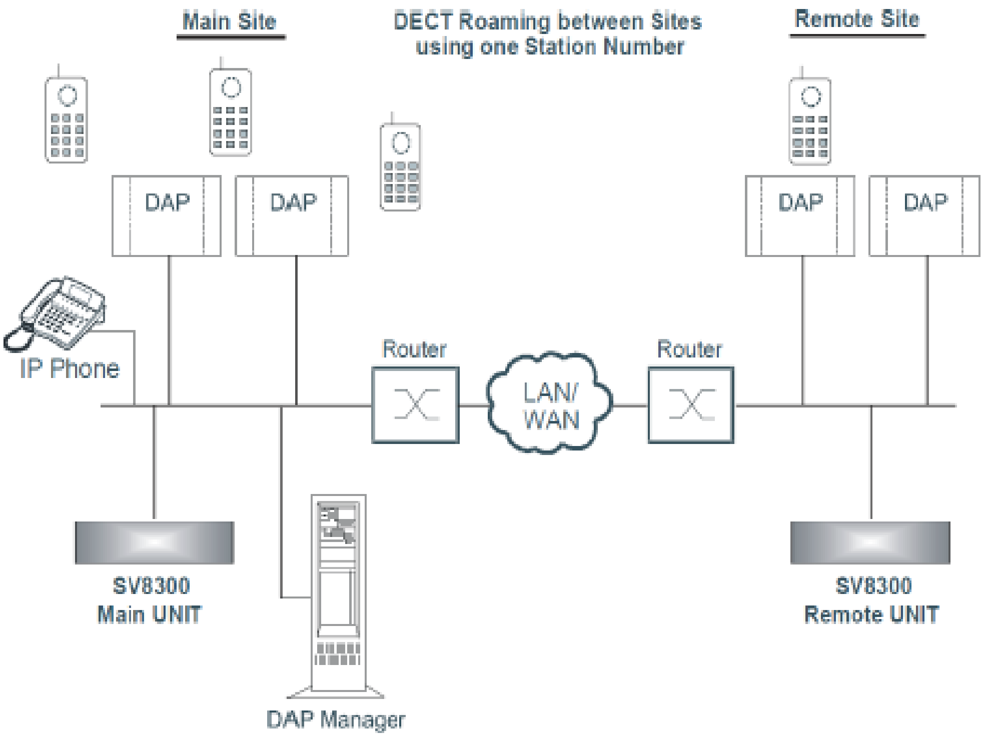


Figure 14-1 User Mobility with IP DECT System with Branch Office(s)

How it works:

When a handset enters the environment of the Branch Office DAP(s), the handset executes a Location Registration. This means that the subscription record is moved to one of the Branch Office DAPs (if it wasn’t there). The Branch Office DAP that receives the Subscription record sends a “Registration”/”Login” request to the Gatekeeper IP address. The Gatekeeper IP address is specified in the configuration file for the DAP, the `dapcfg.txt` file. The Gatekeeper IP address in this file must point to the IP address of the IPLA in the Remote Unit! This means that the registration in the SV8300 is done in the Remote Unit. Now you can make and receive calls in the Remote Site. When the handset moves back to the Main Site, the same mechanism is used but now in the Main Unit. However, the DAPs in the Main Site must use the IPLA IP address of the Main Unit as Gatekeeper address. This means that the configuration files for the DAPs in the Head Quarter (Main Site) must have a different Gatekeeper IP address as the DAP(s) in the Remote Site. Therefore, you must have (at least) two different `dapcfg.txt` files in the IP DECT system.

3.2 Individual IP DECT Systems

Figure 14-2 User Mobility with More Than One IP DECT System shows the configuration with more than one IP DECT System.

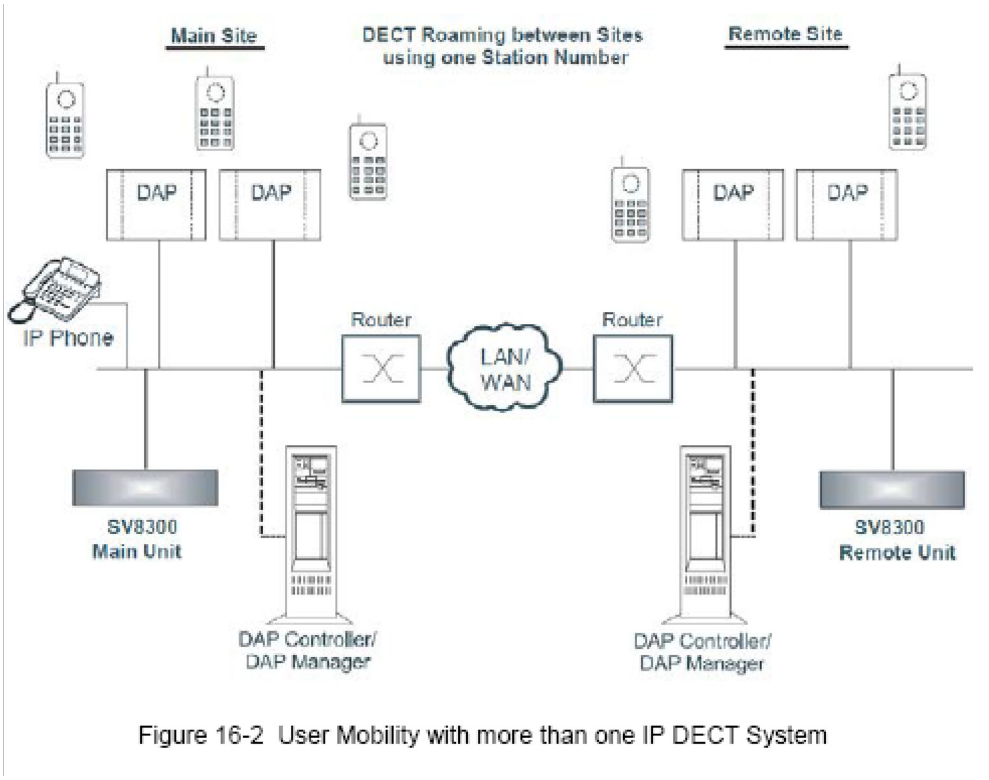


Figure 14-2 User Mobility with More Than One IP DECT System

How it works:

When a handset enters the environment of the Remote Site, the handset executes a Location Registration. This means that the DAP holding the subscription record sends a “Registration”/“Login” to the Remote PIM for the Station Number of the handset . The Remote PIM supports User Mobility and accepts the Login. From now on you can use the handset in the Remote Site. Now you can make and receive calls in the Remote Site. When the handset moves back to the Main Site, the same mechanism is used but now in the Main Site. However, the DAPs in the Main Site uses the MP IP address of the Main Site as Gatekeeper address.

DAP Controller Redundancy 15

SECTION 1 GENERAL

DAP Controller Redundancy means that you will have one or more redundant DAP Controller(s) in you network. If the main DAP Controller goes down, another DAP Controller takes over the functionality.

✎ *DAP Controller Redundancy is licensed!*

Please note that there are various configurations possible.

❍ Central DAP Controllers

❑A Central DAP Controller controls the entire IP DECT system, so the main site and, if present, Branch Offices. As Central DAP Controller, there is always a Primary DAP Controller and there can be a Secondary DAP Controller for redundancy. As a matter of fact, the Secondary DAP Controller will take over when the Primary fails or is not reachable anymore.
The maximum number of Central DAP Controllers is two.
For additional redundancy in Branch Office locations, there can be Local DAP Controllers, see next bullet.

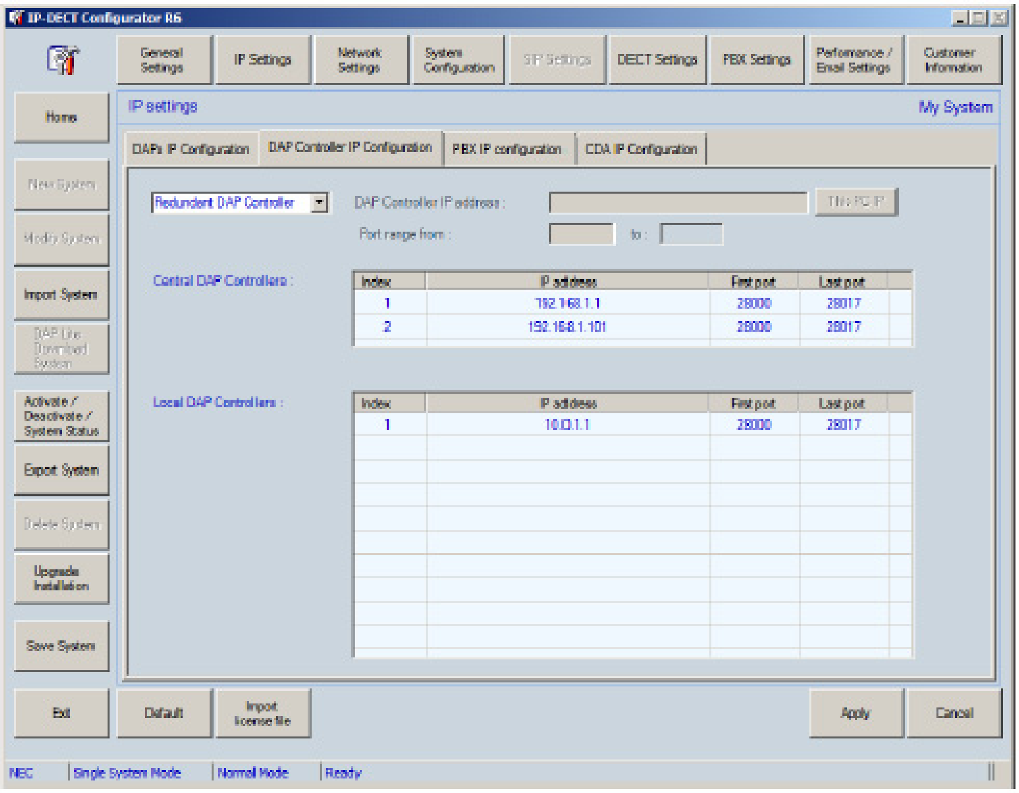
❍ Local DAP Controllers

❑A local DAP Controller is located in a Branch Office, and controls its own Branch Office in case the Central DAP Controller(s) cannot be reached anymore.
A Local DAP Controller never controls another Branch Office other than its own. So, it operates in a Survivability mode for the Branch Office.
The maximum number of Local DAP Controllers is 10.

The difference between a Central and a Local DAP Controller is determined by the configuration that you setup in the "DAP Configurator" in the Primary DAP Controller.

Below, you see the DAP Configurator screen in which you must setup the configuration. Please note that you determine the difference between the Central and the Local DAP Controller here together with the priority.

So, for the Central DAP Controller, you specify a Primary and if required, a Secondary DAP Controller.



Redundant DAP Controller

DAP Controller IP address :

Port range from : to :

Central DAP Controllers :

Index	IP address	First port	Last port
1	192.168.1.1	28000	28017
2	192.168.1.101	28000	28017

Local DAP Controllers :

Index	IP address	First port	Last port
1	10.0.1.1	28000	28017

Figure 15-1 Redundancy Settings

A special “service” (Redundancy Service) in the DAP Controller takes care of the redundancy tasks.

✎ *All configuration actions are done by means of the DAP Configurator in the Primary DAP Controller*

SECTION 2 DAP CONTROLLER REDUNDANCY FOR ROAMING

Handset roaming requires that the subscription record of the handset is always reachable in one of the DAPs in the network. If not, the handset is not usable. In two cases, roaming redundancy can be required:

- ❍ If DAP goes down

  When a DAP goes down, the subscription records in such a DAP are not reachable anymore, and therefore the handsets having a subscription record in that DAP, will not be operational anymore. When the DAP Controller is up-and-running in the network, it will take care that the subscriptions records will be put in another DAP (after a short time). From that time on, the handsets are operational again. This offers a high availability of the handsets. But, this means that the DAP Controller must be up-and-running. To make this mechanism even more reliable, the DAP Controller can be made redundant.

- ❍ Moving between Branch Office locations.

  In a Branch Office configuration, the subscription record moves with the handset to another Branch Office, when the handset moves to the other Branch Office. The DAP Controller takes care of this functionality. To make this mechanism more reliable, the DAP Controller must be made redundant.

SECTION 3 DAP CONTROLLER REDUNDANCY IN MESSAGING CONFIGURATION

DAP Controller Redundancy in a messaging configuration, means that you have two DAP Controllers and two DMLS services. Please note that in this description, we assume that we have Central DAP Controllers (Primary and Secondary), and no Local DAP Controllers. However, there could be a Local DAP Controller as well. (The characteristics of the Local DAP Controller are explained in one of the following subsections.).

The Messaging Application could have been duplicated as well, or it can have an IP connection to each of the DMLS services.

The following figures show examples of the redundant configuration.

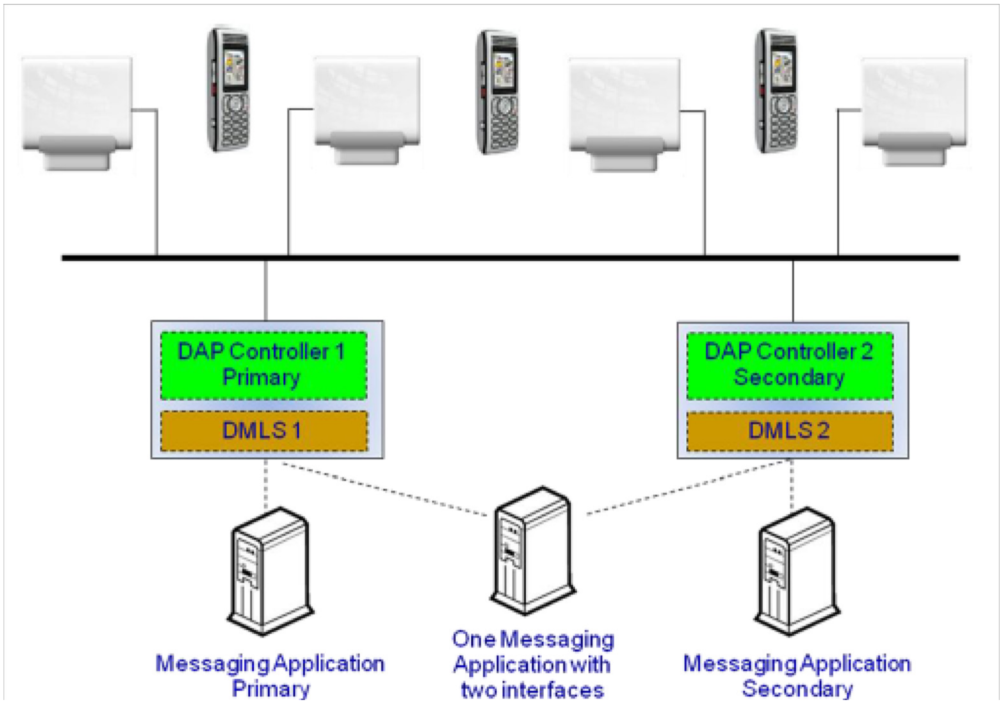


Figure 15-2 Example of a Redundant IP DECT configuration with Messaging

In the example above, there is only one IP DECT system, with two DAP Controllers, the Primary and the Secondary. As you can see, there are two options: one messaging system with two connections to the DMLS services, or duplicated Messaging Applications.

✎ *The Duplicated Messaging Application must be capable to run in redundant mode as well, one operational, one standby. Or in case of one Messaging Application, it must be capable to handle two IP interfaces and detect which interface is operational.*

✎ *In all cases, the Messaging application should check which DAP Controller and therefore which DMLS is up and running.*

❍ Message to the handsets when Primary DAP Controller is active

Figure 15-3 Messaging When Primary DAP Controller is Activeshows that, when the Primary DAP Controller is active, the Messaging Application will send the message to the DMLS (DMLS 1) that is connected to the Primary DAP Controller. The DMLS will send the message to the Primary DAP Controller. The Primary DAP Controller will issue a paging request via all DAPs in the system, to page the handset. When the handset responds, the message is sent to the handset.

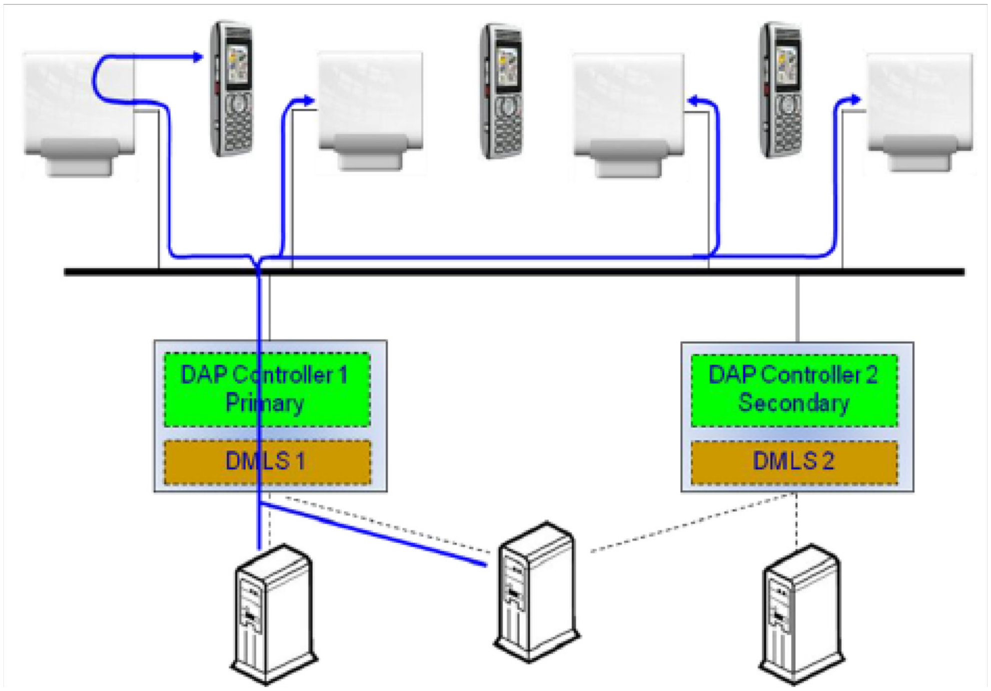


Figure 15-3 Messaging When Primary DAP Controller is Active

- ❍ Message to the handset when Primary DAP Controller is down.

  Figure 15-4 Messaging to Handset When Primary DAP is Down shows that, when the Primary DAP Controller is down, the Messaging Application will send the message to the DMLS (DMLS 2) that is connected to the Secondary DAP Controller. The DMLS will send the message to the Secondary DAP Controller. The Secondary DAP Controller will issue a paging request via all DAPs in the system, to page the handset. When the handset responds, the message is sent to the handset.

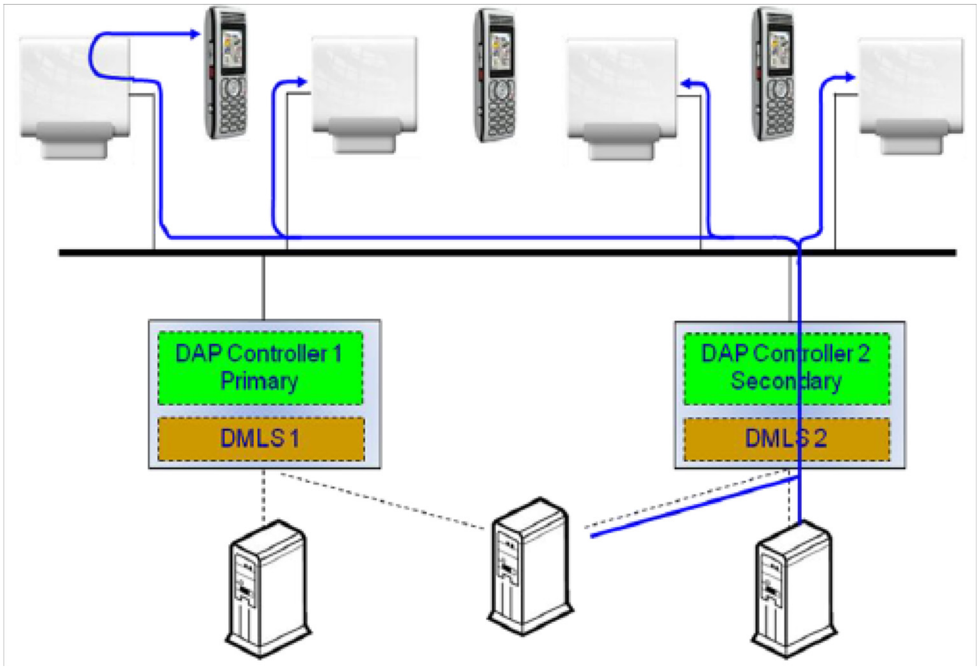


Figure 15-4 Messaging to Handset When Primary DAP is Down

- ❍ Message from the handset when Primary DAP Controller is active.

  Figure 15-5 Messaging From Handset When Primary DAP Controller is Active shows the path of a message from a handset. It will go from the handset to the Primary DAP Controller. Only if the Primary DAP Controller is down or not reachable, the DAP will send the message to the Secondary DAP Controller (not shown in the figure.)

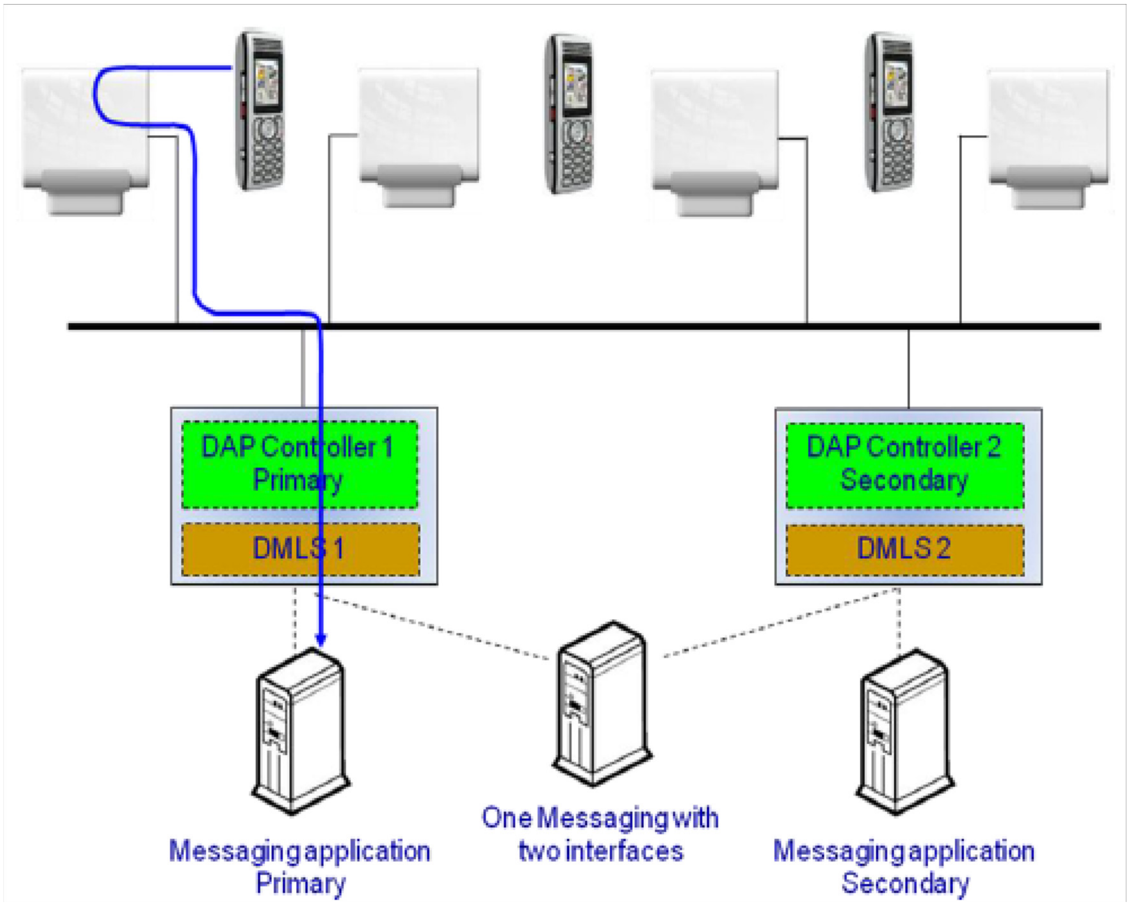


Figure 15-5 Messaging From Handset When Primary DAP Controller is Active

Please note that the DAP determines where to send the message to: the Primary or the Secondary DAP Controller. The DAP checks if the Primary DAP Controller is up-and-running. If it is up-and-running, it will send the message to the Primary DAP Controller. If not running, it will send the message to the secondary DAP Controller.

SECTION 4 DAP CONTROLLER REDUNDANCY – HOW DOES IT WORK

In the DAP Controller Redundancy, there is a Primary DAP Controller and a Secondary DAP Controller. Please note that in an operational configuration, both DAP Controllers are up-and-running. The Primary DAP Controller contains the actual and up-to-date configuration. The Secondary DAP Controller keeps itself updated with the configuration data from the Primary by means of a Presence Check and info exchange.

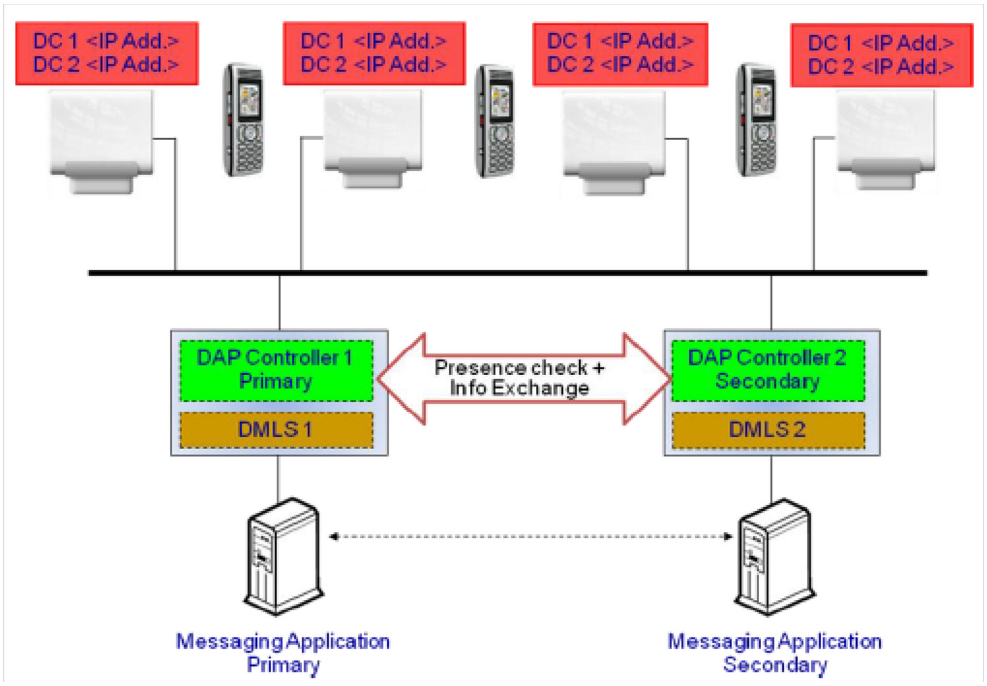


Figure 15-6 DAP Controller Redundancy

❍ The DAPs select to which DAP Controller they will connect,

The DAPs select to which DAP Controller they will connect, based on the priorities in the list of DAP Controllers. A DAP will try to connect to the DAP Controller that is first in the priority list (Primary DAP Controller). If that fails, it will try to connect to the second DAP Controller in the list (Secondary DAP Controller). If that fails it will try to connect to the Local DAP Controller that is in the list (see the screen capture in Figure 15-1 Redundancy Settings on page 15-2).

- The Messaging Application.

  In the Messaging Application configuration, most likely, one of the Applications is operational, the other stand-by. The Messaging Application is able to detect if Primary DMLS/DAP Controller is active or not. If operational, the primary Messaging Application will be active. If the Primary DMLS/DAP Controller is not active, the Messaging Application detects that, and will make the secondary Messaging Application active.

- When the Primary DAP Controller Fails

  If the Primary DAP Controller fails, the DAPs will notice that the DAP Controller, is not operational anymore, and therefore, the DAPs will try to connect to the Secondary DAP Controller, based on the on-board priority list of DAP Controllers. The Secondary DAP Controller detects that the Primary is not reachable anymore, and will not allow to do any manual changes in subscriptions anymore. Refer to Figure 15-6 DAP Controller Redundancy on page 15-8.

- When the Primary DAP Controller becomes operational gain.

  When the Primary becomes operational again, the following will happen:

  - The DAPs continuously poll the Primary DAP Controller to check if it is back again. Because of that, they will detect that the Primary DAP Controller is up again. Then they will “lock” on the Primary DAP Controller.
    Then the Primary DAP Controller will retrieve the configuration data (subscription data etc.) from the DAPs, to make the system consistent again.
  - The Secondary DAP Controller polls the Primary DAP Controller continuously. When it detects that the Primary DAP Controller is back again, it will request for configuration data from the Primary DAP Controller. The Primary DAP Controller already received the latest configuration data from the DAPs, and is up-to-date. The Secondary DAP Controller will get the configuration data from the Primary, and then the IP DECT System is consistent again.

- What happens when there is a change in the configuration data in the Primary DAP Controller.

  When there is a change in the configuration data in the Primary DAP Controller (e.g. a handset is subscribed, the Redundancy Service sends a notification to all other DAP Controllers (Secondary and Local DAP Controllers).

SECTION 5 LOCAL DAP CONTROLLERS

Besides the Central DAP Controllers, there can be Local DAP Controllers. A Local DAP Controller is located in a Branch Office and takes care of the DAP Controller functionality in the associated Branch Office only, in case the Central DAP Controllers (Primary and/or Secondary) are not reachable anymore. It performs a kind of Survivability task.

There can be up to 10 Local DAP Controllers.

The DAPs in the Branch Office will check if the Central DAP Controllers are reachable. If not, they will check if the Local DAP Controller is reachable, and they lock on the local DAP Controller.

Figure 15-7 Example of Mixed DAP Controllers, Central and Local shows a configuration with mixed DAP Controllers, Central and Local. Although capable to send/receive messages, the Local DAP Controllers are not used for messaging in this example. However, if the Messaging Application supports it, the Messaging Application could connect to a Local DAP Controller, to assure that messaging works to the Branch Office.

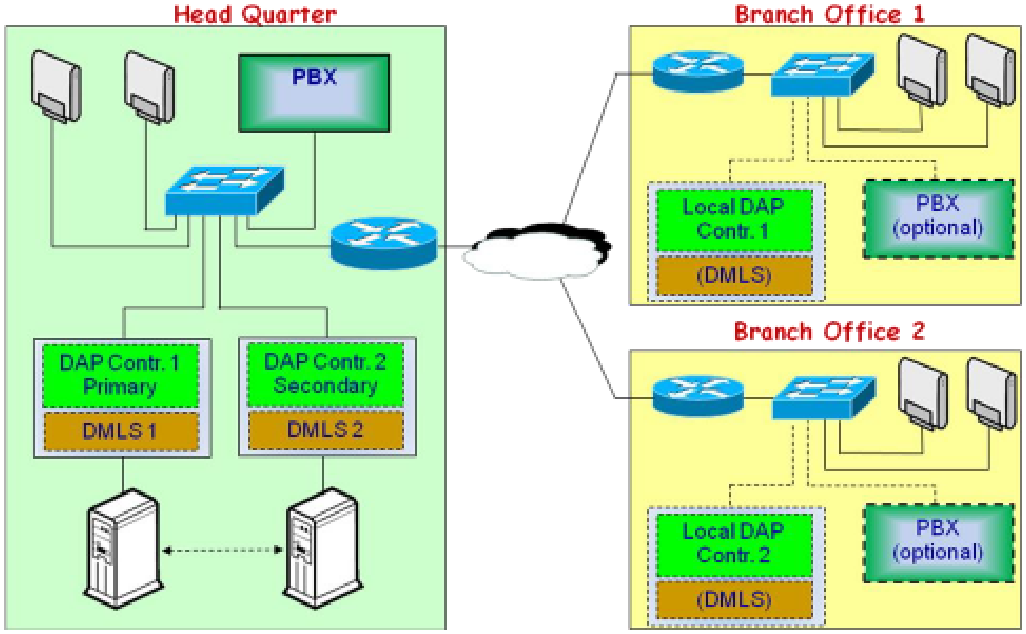


Figure 15-7 Example of Mixed DAP Controllers, Central and Local

SECTION 6 SECONDARY DAP CONTROLLER IN BRANCH OFFICE LOCATION.

As a matter of fact, the Secondary DAP Controller does not necessarily have to be located in the Head Quarter, but can be located anywhere else, e.g. in a Branch Office. Refer to

In this configuration the Secondary DAP Controller controls the entire IP DECT system when the Primary DAP Controller fails. The Messaging Application can connect to the Secondary DAP Controller, via the IP network.

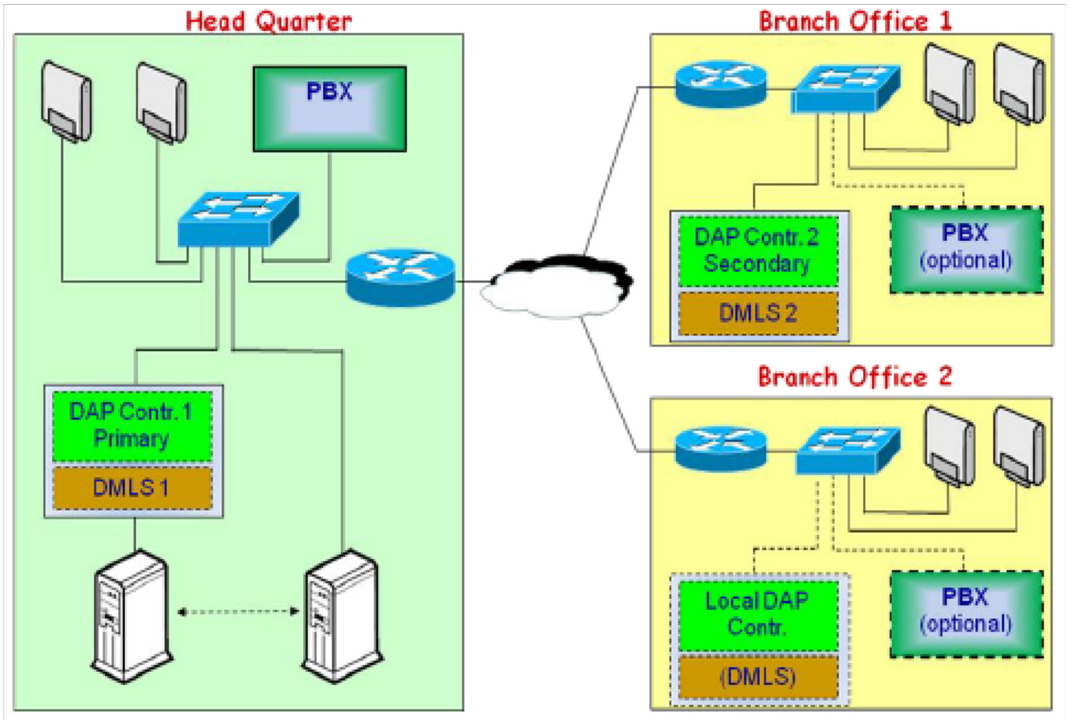


Figure 15-8 Example of DAP Controller Redundancy with Secondary DAP Controller in the Branch Office.

SECTION 7 DECT MANAGEMENT

❍ At the Primary DAP Controller

❑Normally you will do DECT Management on the Primary DAP Controller, and you will have full DECT Management functionality available.

❍ At the Secondary DAP Controller

❑When you open the WEB page on the Secondary DAP Controller with address “Localhost”, you will be redirected to the Primary DAP Controller and you will have full DECT Management functionality available. When the Primary DAP Controller is not up-and-running, you will not be redirected, but you will see the Secondary DAP Controller DECT Manager window in Read Only mode. When the Primary DAP Controller comes back again, you will automatically be redirected to the Primary DAP Controller.

SECTION 8 HOW TO CREATE AN ARCHIVE

When you open a WEB Page on the Secondary DAP Controller, you will see the WEB Page (DAP Manager screen) on the Primary DAP Controller. So, when you click the Archive Button, an Archive is created of the *Primary* DAP Controller, but stored on the *Secondary* DAP Controller!

When you want to make an Archive of the Secondary DAP Controller, you cannot do that via the WEB Page (DAP Manager), unless the Primary DAP Controller is down. So, you must use the button “Archive” in the DAP Configurator of the Secondary DAP Controller.

SECTION 9 ACTUAL STATUS INDICATION.

In the top right corner of the DECT Manager WEB interface, the Redundancy status is displayed. The redundancy status is either Redundant or Stand Alone. See screen capture below.

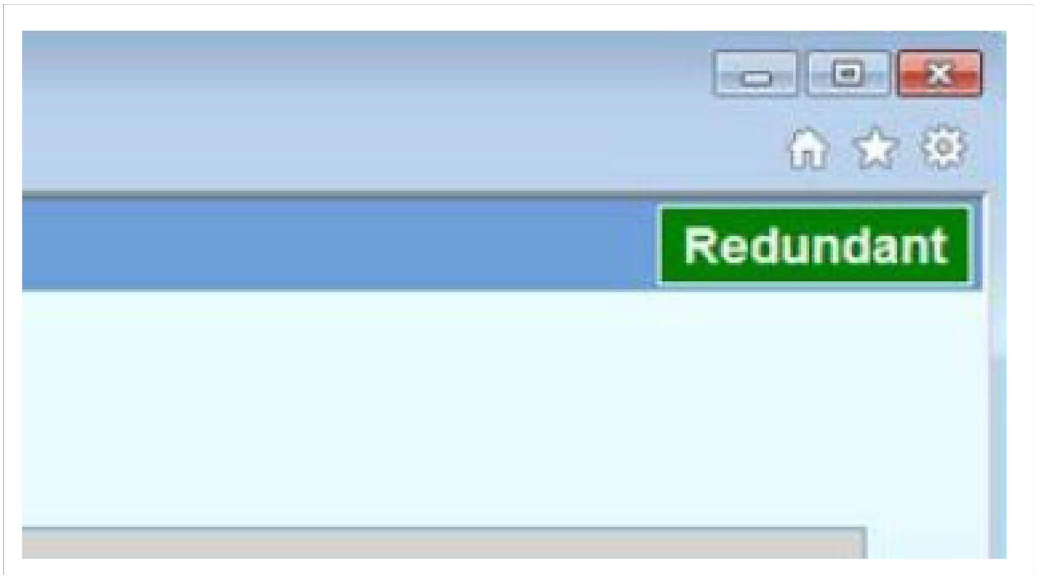


Figure 15-9 Display Redundancy Mode

Upgrade To Latest Release

A

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

THIS PAGE INTENTIONALLY LEFT BLANK

AP300 Versus AP200

B

SECTION 1 OVERVIEW OF DIFFERENCES

From November 2009 onwards a new DAP will be introduced, the AP300 as a successor of the AP200.

In this Appendix you will find an overview of the differences between the AP200 and the AP300.

✎ *For more information on the characteristics of the AP300, please consult the AP300 Installation Manual.*

Differences are as follows:

Table B-1 Differences Between AP200 and AP300

ITEM	AP200	AP300
Compact Size	A5	2/3 of A5
Mounting	Vertical	Vertical or Horizontal
Localization support	Various types	One type of AP300 suitable for all regions. Country and region selection in the DAP Configurator.
G.729	AP200 only, not in AP200S.	Available via daughter board on the AP300.
Power supply	Local via AC adaptor and PoE support IEEE802.3af	PoE IEEE802.3af. No local power supply.
DC voltage on DAP via PoE	36 - 60 Volt	36 - 57 Volt
PoE Class	Class 0	Class 2

Table B-1 Differences Between AP200 and AP300

ITEM	AP200	AP300
Service/ maintenance	One LED for AP200 status.	Two LEDs, one for AP300 status, another for AP300 network status indication.

Table B-2 Physical Differences

ITEM	AP200	AP300
Dimension s	235 x 45 x 172 mm (w x d x h)	145 x 43 x 174 (w x d x h)
Weight	540 gram (including packaging)	307 gram (excluding packaging)
Protection	IP20	IP40
Color	Light grey (color code 70109)	Light Grey, RAL 9010
Antenna	Fixed position	Adjustable: horizontal or vertical position

Table B-3 Outdoor Cabinet Differences

ITEM	AP200	AP300
Dimensions	430 x 330 x 200 mm (w x d x h)	275 x 225 x 80 mm (w x d x h)
Weight	6 kg (AP200 inclusive)	
Material	Glass enforced polyester	
Relative humidity	5 to 95 %	5 to 95 %
Color	Grey (RAL 7032)	
Protection	IP66	IP66
Operating temperature	-15º to +60º C	-20º to +45º C

AP400 Versus AP300

SECTION 1 OVERVIEW OF DIFFERENCES

From June 2012 onwards the AP400 will be introduced, as a successor of the AP300.

In this Appendix you will find an overview of the differences between the AP300 and the AP400. Please note that the AP300 and the AP400 are similar in many aspects.

SECTION 2 DIFFERENCES

The differences between the two AP types are shown in table below.

Table C-1 AP300 vs. AP400 Differences

ITEM	AP300	AP400
Outside Temperature	0 C . . . 45 C	-5 C . . . 45 C
CAT-iq Data facilities	-	Not applicable yet.
DAP Type: Generic type, NEC branded	AP300	AP400
DAP Type: Generic Type, un-branded	-	-
DAP Type: Type to be used on NEC SMB systems.	AP300C	AP400C
DAP Type: Generic type with connectors for external antennas	-	-

Table C-1 AP300 vs. AP400 Differences

ITEM	AP300	AP400
DAP Type: Type to be used on NEC SMB PBXs, but with a max. of 4 DAPs per system.	-	AP400S
Boot Package	In Read Only Memory	In Flash memory. Name: 49920xxx.dwl
Firmware Package	Name: 4910axxx.dwl	Name: 4920axxx
IGMP Version	IGMPv2	IGMPv3

LRMS Messaging

D

SECTION 1 GENERAL

✎ *Messaging can only be used with handsets that support LRMS (E2) messaging.*

IP DECT supports LRMS (Low Rate Message Services). There are two options:

❍ Handset - Handset Messaging

This means that handsets can send messages between each other. Depending on the connection to the Messaging Server, handset to handset messaging is possible or not.

❍ Messaging Server - Handset Messaging

You can connect a Messaging Server to IP DECT to send and receive messages to/from handsets. The DAP Controller offers an interface for Messaging to and from handsets. However, the DAP Controller supports a proprietary protocol, which requires a converter program called: DMLS (DECT Messaging and Location Services). The DMLS offers a rich, yet simple, interface for Third Party messaging servers.
For more information about Messaging Server applications, please contact your IP DECT supplier.

The following figure shows the message path between a Messaging Server and IP DECT.

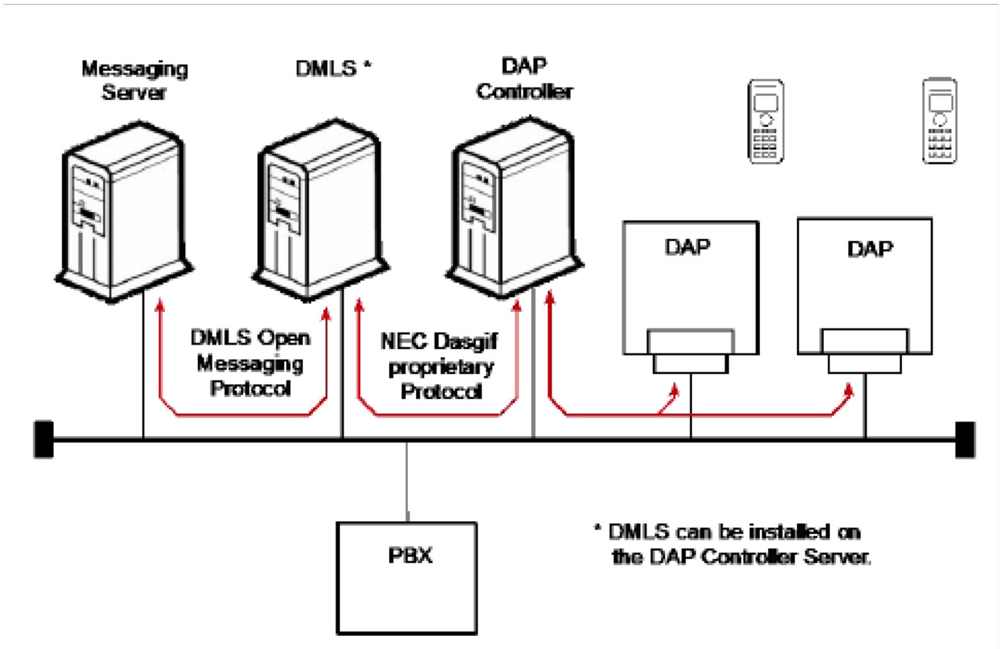

Messaging Server
DMLS *
DAP Controller
DAP
DAP
DMLS Open Messaging Protocol
NEC Dasgif proprietary Protocol
PBX
* DMLS can be installed on the DAP Controller Server.

Figure D-1 Message Path in IP DECT - Messaging Server Configuration

Note that the messaging between the Messaging Server and IP DECT, always goes via the DAP Controller/Manager. It is a TCP/IP connection. The TCP port for messaging on the DAP Controller/Manager is always the lowest port number + 1 (default 28001). The moment that there is a connection to this port, all messages will be handled by the Messaging Server and handset to handset messaging is only possible via the Messaging Server.

✎ *When the option “Local Message Relay Override” is selected in the DAP Configurator, the Messaging Server can send messages to handset and handset to handset messaging is still possible.*

❍ Messaging Server - Handset Messaging with Local Message Relay Override

In the DAP Configurator, there is an option “Local Message Relay Override”. When you activate this option, you can send messages between handsets and the Messaging Server can send messages to handsets. Note that you cannot send messages from handsets to the Messaging Server when “Local Relay Override” is active.

SECTION 2 TYPES OF MESSAGES

When sending a message to a handset, there are three types of messages distinguished. The message types indicate the emergency level.

- ❍ Normal Message

  When this type of message is send to a handset, the handset displays the message and will alert with a short ringing. The user of the handset cannot confirm the message. The handset sends back a technical “ACK” to the originator of the message (e.g. DECT Server) to indicate that the message arrived on the handset.

- ❍ Urgent Message

  When this type of message is sent to a handset, the handset displays the message and alerts with a ringing type that gets louder and louder until the handset user confirms the message (or a timer expires). The user can confirm the message by pressing the “OK” button or the “Delete” button. When the message is send to the handset, a timer is started. The user must confirm the message within the time period of the timer (default 30 sec.). If not confirmed within this time, ringing stops and a “NACK” is send to the originator of the message, to indicate that the user didn’t confirm the message.

- ❍ Emergency Message

  When this type of message is send to a handset, the handset displays the message and alerts with a very compelling ringing type. This forces the user to confirm the message by pressing the “OK” button or the “Delete” button. Confirmation must be done within a certain time period, which is the same as for an Urgent message. (Also 30 seconds by default.) If not confirmed within this time, ringing stops and a “NACK” is send to the originator of the message, to indicate that the user didn’t confirm the message.

The originator of the message determines the urgency type of the message. Note that if the handset is the originator, there are only two message types possible: Normal and Urgent. When the Messaging Server is the originator, three message types are possible: Normal, Urgent, Emergency.

SECTION 3 BROADCAST MESSAGING

3.1 General

Broadcast Messaging is implemented from IP DECT Release 4.2 onwards. Broadcast messaging will normally be used in case of an emergency situation where a large group of people needs to be reached in a very short time.

Broadcast Messaging has the following characteristics:

❍ It uses a kind of “connection-less” data transfer.

❍ To improve message delivery, the Messaging Server can repeat the message a few times. The handset will ignore duplicate messages.

❍ Neither the portable nor the end-user can confirm reception of the message.

❍ No traffic bearers are occupied. This avoids congestion.

✎ The maximum message length is 54 characters.

✎ Broadcast Messaging is optional in IP DECT. It must be enabled using the DAP Configurator tool.

Broadcast messaging works with groups. If a handset is member of a group, it is capable of receiving messages for that group. Note that all handsets are always part of the default group (“000”).

3.2 Additional Broadcast Message Types

There are three (additional) message types defined for broadcast messaging. The Message Server must be capable of sending these messages, because the handset is not able to send broadcast messages, it is only able to receive broadcast messages.

❍ Broadcast Messages

A Broadcast message is a real message which is addressed to a group of portables. A three digit number identifies the group. (A handset must have been made member of a group before it can receive messages for the group.)
All portables that support broadcast messages are automatically member of the group ‘000’. Next to this group a portable can be member of 5 other groups.
Note that these messages are not acknowledged. Therefore it is possible that a portable did not receive this message, because it was for instance out of reach, powered down, in silence charging mode or because of bit-errors in the air. It is the responsibility of the Messaging Server to repeat the same message, to get a higher chance of correct reception by all portables.
Although these messages are not acknowledged, it is still useful to distinguish between normal, urgent and very urgent broadcast messages, because it determines also how the message is presented to the user.

❍ Group Membership

This is not a user message send to the display of the handset. It is a membership message send to the handset. A message Server can instruct a portable to become member of a group or give-up membership of a group by means of this message type. It is also possible to instruct a portable to give-up membership of all groups except ‘000’.
It is the responsibility of the messaging server to keep track of the group membership of each individual portable, since a portable has to acknowledge this type of message.

❍ Broadcast Group Membership

(This is not a user message send to the display of the handset.) By means of this type of message a Messaging Server can instruct a group of portables to give-up membership of one group or all groups (except of course of group “000”.) Note that these messages are not acknowledged.

✎ *Group Membership arrangement is the task of the Messenging Server. IP DECT only forwards the group membership messages to the handsets.*

3.3 How about Normal, Urgent, Emergency Messages

Sending a broadcast message to a handset still supports urgency levels: Normal, Urgent and Emergency. However, there is no B-channel used and there is no acknowledge send back.

Using broadcast messaging the behavior of Normal, Urgent and Emergency messages is as follows:

❍ Normal Broadcast Message

A normal broadcast message appears on the handset as if it is a normal message.
The difference is a technical difference. In case of a normal unicast message the handset will respond and an ACK is sent to the Messaging Server.

❍ Urgent broadcast Message

When the handset receives a broadcast Urgent message, it appears on the handset as if it is unicast Urgent message. The ringing rhythm is the same. To stop the ringing, the handset user has to acknowledge the message by means of pressing the “OK” or “Delete” button. *Note that pressing this button does NOT send a confirmation to the system, it only stops ringing.* If the user does not press the “OK” or “Delete” button, the handset will terminate the ringing when a timer in the handset expires. This timer is always longer that 30 seconds and normally shorter than one minute. The time value may be different per handset type.

- Urgent and Emergency broadcast Message

  When the handset receives a broadcast Emergency message, it appears on the handset as if it is unicast Emergency message. The ringing rhythm is the same. To stop the ringing, the handset user has to acknowledge the message by means of pressing the “OK” or “Delete” button. *Note that pressing this button does NOT send a confirmation to the system, it only stops ringing.* If the user does not press the “OK” or “Delete” button, the handset will terminate the ringing when a timer in the handset expires. This timer is always longer that 30 seconds and normally shorter than one minute. The time value may be different per handset type.

Overview Of Default IP Ports

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

✎ *The table below, gives an overview of the ports used by IP DECT Equipment. Please note that the interface on the SV8300 uses ports that are described in the SV8300 documentation.*

Table E-1 Default Ports Used in Business Mobility IP DECT

Protocol	Interface/ Device	Default Destination port
DHCP	DHCP Server	67
	DAP	68
Proprietary IP DECT protocol and messaging port (28001).	DAP Controller	28000-28017
IP DECT Proprietary signalling (IP Unicast and IP Multicast), Protims Protocol and RTP (Real Time Protocol)	DAP	3000-22635
TFTP	TFTP Server	69 (only for initial communication) then:1024-65535
DRS	SV8300 MP	3456

THIS PAGE INTENTIONALLY LEFT BLANK

UNIVERGE® SV8300

IP-DECT Installation Guide

NEC Corporation of America
Issue 1.0