IP-DECT Base Station
(software version 10.2.X)

Mitel®

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

TRADEMARKS

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

1 INTRODUCTION

This document describes commissioning and administration of the following equipment:

- IPBS [1]

The document is intended as a guide for the System administrators:

For information on the IP-DECT system, see the System Description documentation for IP-DECT.

For information about supported Mitel Call Servers, see:

- MiVoice MX-ONE
- MiVocie Business
- MiVocie 250 consult the corresponding CPI documentation.

1.In previous documentation, *IPBS Base Station* (or *IPBS*) was sometimes referred to as *IP-DECT Base Station*.

1.1 ABBREVIATIONS AND GLOSSARY

Base Station	Common name for IPBS, DECT Base Station (IPBS4x2 and IPBS4x0).
DECT	Digital Enhanced Cordless Telecommunications: global standard for cordless telecommunication.
Device	A device can be an IPBS
DHCP	Dynamic Host Configuration Protocol
DTMF	Dual Tone Multiple-Frequency
FER	Frame Error Rate
GUI	Graphical User Interface
ICE	Interactive Connectivity Establishment: a protocol for finding and selecting a working network path between two media endpoints
IP	Internet Protocol: global standard that defines how to send data from one computer to another through the Internet
IPBS	Also referred to as *IPBS Base Station (IPBS432 /IPBS442)*. Previously called *IP-DECT Base Station*
LAN	Local Area Network: a group of computers and associated devices that share a common communication line.
LDAP	Lightweight Directory Access Protocol
LLDP	Link Layer Discovery Protocol: is a vendor-neutral link layer protocol used by network devices for advertising their identity, capabilities, and neighbours on an IEEE 802 local area network.
PBX	Private Branch Exchange (MiVoice MX-ONE, MiVoice Business, MiVoice 250): telephone system within an enterprise that switches calls between local lines and allows all users to share a certain number of external lines.
PSCN	Primary receiver Scan Carrier Number: defines the RF carrier on which one receiver will be listening on the next frame.
RFP	Radio Fixed Part. DECT base Station part of the DECT Infrastructure.
RFPI	Radio Fixed Part Identity
RSTP	The RFPI, Radio Fixed Part Identity, is the broadcast identity which uniquely identifies a RFP geographically.
RSSI	Radio Signal Strength Information
RTP	Real-Time Transport Protocol
SST	Site Survey Tool
ToS	Type of Service
VLAN	Virtual Local Area Network

2 IP SECURITY

2.1 IP SECURITY TERMINOLOGY

2.1.1 TLS (FORMER SSL)

Note: Secure Socket Layer (SSL) has been renamed Transport Layer Security (TLS). TLS 1.0/1.1/1.2 is based on SSL 3.0/3.1. This document hereafter uses the term TLS.

TLS is a security mechanism based on cryptography (see *2.1.3 Cryptography*) and is used for encrypting communications between users and TLS-based Websites. The encryption prevents eavesdropping and tampering with any transmitted data.

TLS operates on the OSI Model Level 5 and uses PKI (see *2.1.2 Public Key Infrastructure*).

Mutual TLS refers to the process when both the user and the website authenticate each other through verifying the provided digital certificates.

2.1.2 PUBLIC KEY INFRASTRUCTURE

Public Key Infrastructure (PKI) is a component of Public Key Cryptography (PKC) that uses:

- Public Key Certificates, see *Public Key Certificates (Digital Certificates)*
- Certificate Authorities, see *Certificate Authorities*

Public Key Certificates (Digital Certificates)

Public Key Certificates are used for key exchange and authentication. They are simply electronic documents (files) that incorporate a digital *signature* to bind together a *public key* with an *identity* (information such as the name or a person or organization, their address, and so forth).

The signature may be signed by a trusted entity called a Certificate Authority (CA), see *Certificate Authorities*.

The most common use of public key certificates is for TLS certificates (https websites).

Certificate Authorities

A Certificate Authority or Certification Authority (CA) is a trusted entity which issues public key certificates. The certificates contain a public key and the identity of the owner. The CA asserts that the public key belongs to the owner, so that users and relying parties can trust the information in the certificate.

Certificate Signing Request (CSR) or **Certification Request** is a message that is generated and sent to a CA in order to apply for a TLS certificate. Before the CSR is created a key pair is generated, the private key kept secret. The CSR will contain the corresponding public key and information identifying the applicant (such as distinguished name). The private key is not part of the CSR but is used to digitally sign the entire request. Other credentials may accompany the CSR.

If the request is successful, the CA will send back an identity certificate that has been digitally signed with the CA's private key.

A CSR is valid for the server where the certificate will be installed.

2.1.3 CRYPTOGRAPHY

Cryptography is the encoding of messages to render them unreadable by anyone other than their intended recipient(s). Modern cryptography uses complex algorithms implemented on modern computer systems.

Cryptography tasks can be divided into the two general categories Encryption and Authentication.

Encryption

Encryption is the scrambling of information so that the original message cannot be determined by unauthorized recipients by applying an *encryption algoritm* to the message *plaintext* producing *ciphertext* (appearently random bits). A *decryption algoritm*, if given the correct key, converts the ciphertext back into plaintext. Public key algoritms use paired keys, one for encryption and another for decryption.

Authentication

Authentication is the verification of a message's sender. This requires the message to be protected so it cannot be altered, usually by generating a *digital signature* formed by a hash of the message. Only the correct key can generate a valid signature.

2.2 INTRODUCTION TO IP SECURITY IN IP-DECT

A secure system requires more planning than an unsecured system.

2.2.1 SECURE WEB ACCESS (HTTPS)

For IP-DECT devices

• https access should be enabled
• http access should preferably be disabled

For more information see 4.9.3 *Configure the HTTP settings* on page 96.

2.2.2 TLS CERTIFICATES

Security in Web-based applications rely on cryptography. Cryptographical systems are only as secure as their *keys.* This makes *Key Management* a critical and often neglected concern. *TLS Certificates* have emerged as a clever way of managing large scale key distribution.

Two certificate management tasks are needed for TLS:

1   Trust relationships when the device must know which third parties (e.g. IP-PBX) it shall trust in, see *1. Trust Relationships*.

2   Device certificates to authenticate the device against third parties, see *2. Certificate Handling Options with Device Certificates*.

1. Trust Relationships

Trust relationships are defined by a trust list in the device. The list contains the certificates to be accepted by the device for TLS secured connections (e.g. HTTPS, SIPS).

For more information see *Trust List* on page 49.

2. Certificate Handling Options with Device Certificates

There are four certificate handling options:

- **Default Device certificate**
  The default certificate is supplied with the device. It is a self-signed certificate. Self-signed certificates provide only encryption, not authentication.

  For more information see *Default Device Certificate* on page 50.

- **Self-signed certificates**
  This option is for customers not planning on having their certificates signed by public or private CAs. Self-signed certificates provide encryption but do in most cases not provide authentication.

  For more information see *Self-signed Certificates* on page 51.

- **Certificates signed by a Certificate Authority (CA)**
  Two options are possible:
  - **A)** Certificates signed by the customer's own CA. Customers possessing the knowledge and infrastructure to house their own CA could build an internal enterprise CA, enabling them to sign (approve) their own certificate requests. This would make the customer a private CA.

  - **B)** Certificates signed by a trusted public third party entity/organization. There are only about a dozen issuers who have the authority to sign certificates for servers worldwide. An example is VeriSign. To use a public CA for certificate approvals the IP-DECT system would in most cases need to be connected to the Internet and hold a fully qualified domain name.

  For more information see:

  - *Certificate Signing Request (CSR)* on page 52.
  - *Import of Certificate Including Private Key (PKCS #12 file)* on page 53

2.3 IP-DECT ADMINISTRATIVE FUNCTIONS

2.3.1 CONFIGURATION - HTTP

The HTTP tab is used to configure the type of web access that should be allowed for the device, includes a field for configuring https access.

For more information see 4.9.3 *Configure the HTTP settings* on page 96.

2.3.2 CONFIGURATION - CERTIFICATES

The *Certificates* tab lists the certificate used by web browsers to authenticate the identity of the device (Web server).

For more information see 4.1.10 *Certificates* on page 48.

2.3.3 CONFIGURATION - SIPS

SIP Secure (SIPS) is used to encrypt the signalling communication between the IPBS and the IP-PBX. SIPS uses the TLS protocol for encryption. The signalling between the IPBSs is also encrypted by default and there is no possibility to disable it.

For more information see 4.6.23 *Configure Gatekeeper* on page 79.

2.3.4 CONFIGURATION - SECURE RTP

Secure RTP (SRTP) is used to encrypt the voice communication between the end user equipments.

For more information see 4.6.17 *Secure RTP* on page 74.

3 CONFIGURATION

This section describes how to configure the IPBS using the web interface. The recommended order to configure the equipment in the IP-DECT system is as follows:

1   Configure the Mobility Master, see 3.4 *Configure the Mobility Master* on page 23.

2   Configure the Standby Mobility Master, see 3.5 *Configure the Standby Mobility Master* on page 23.

3   Configure the Pari Master, see 3.6 *Configure the Pari Master* on page 24.

4   Configure the Standby Pari Master, see 3.7 *Configure the Standby Pari Master* on page 25.

5   Configure the Master, see 3.8 *Configure the Master* on page 25.

6   Configure the Standby Master, see 3.9 *Configure the Standby Master* on page 26.

7   Configure the Radios, see 3.11 *Configure the Radio* on page 27.

Note: When the IPBS is reconfigured to another role (for example from being a Standby Master to becoming a Master), a factory reset should be done. See 4.29 *Reset Using the Reset Button* on page 126.

3.1 REQUIREMENTS

The following is required in order to configure the IP-DECT system:

• PC

- 10/100base-T Ethernet connection

3.1.1 WEB BROWSER REQUIREMENTS

To use the interface properly, the web browser has to meet the following requirements:

- HTTP 1.1 protocol
- HTML 4.0 protocol
- XML/XSL Version 1.0

3.2 ACCESS THE GUI

Note: To access the GUI for an IPBS using secure web access (https), you can install the certificate for the IPBS in the web browser to avoid getting certificate error messages. See Appendix F: *Import Server Certificate in the Web Browser* on page 156.

The GUI interface is accessed through a standard web browser. It is possible to use the name, ipbs-xx-xx-xx (IPBS1), ipbs2-xx-xx-xx (IPBS2), where xx-xx-xx is the end of the MAC address.

It is also accessed by entering http://xxx.xxx.xxx.xxx. In this address, *xxx.xxx.xxx.xxx* should be replaced with the IP address determined in 3.2.1 *Determine the IP Address* on page 15.

Access the GUI and change the default password as described in 3.2.2 *Change the Default Password* on page 17.

If mutual TLS authentication is used, a window comes up where a trusted client certificate must be chosen and confirmed before proceeding to the login page.

Note: If the GUI cannot be accessed with Internet Explorer 8 or newer, check that the **TLS 1.0/1.1/1.2** option is activated in the web browser under menu **Tools** > **Internet Option** > **Advanced** > **Use TLS 1.0/1.1/1.2**

3.2.1 DETERMINE THE IP ADDRESS

The factory setting of the DHCP mode for the LAN1 port is "automatic", at first power up it will act as a DHCP client. If the network has a DHCP server, it will assign an IP address to the IPBS. If there is no DHCP server in the network, the IPBS can be assigned a predefined IP address. The factory setting of the DHCP mode is to the fixed IP address 192.168.0.1, see 8.2.1 Set 4.2.1 *Set DHCP Mode for IPv4* on page 53.

Note: After the first startup the DHCP mode should be changed from "automatic" to either "client" or "off", see 4.2.1 *Set DHCP Mode for IPv4* on page 53.

This section describes how to determine the dynamically allocated IP address. The address is used to access the IPBS using a web browser. Two methods are described:

- *In a Network without a DHCP Server* on page 16.
- *In a Network with a DHCP Server* on page 16.

In a Network without a DHCP Server

If the network does not have a DHCP server, and the DHCP mode is set to "automatic" (factory default), follow the steps below.

Note: If the IPBS has been used before, it must be restored to factory default settings by performing a long hardware reset, see 4.29 *Reset Using the Reset Button* on page 126.

1   Connect an Ethernet cable between the IPBS and the computer.

NOTE: For IPBS, a power adapter must be used.

2   Ensure that the computer has an IP address within the same IP address range as the IPBS (192.168.0.1).

3   Perform a hardware reset by shortly pressing the **reset** button.
      The IPBS will be assigned the IP address 192.168.0.1 and the netmask 255.255.255.0.

4   Enter **http://192.168.0.1** in the browser to access the IPBS GUI.

5   After the first startup, do the following:
      On the IPBS: Select **LAN1** > **DHCP**

6   In **Mode** drop-down list, change the DHCP mode from **automatic** to **disabled**.

In a Network with a DHCP Server

If the network has a DHCP server the IP address is determined following the steps below.

The IPBS MAC address can be found on the label on the box and on the label on the backside. The hexadecimal numbers (xx-xx-xx-xx-xx-xx) represent the MAC address.

Note: To determine the IP address it is necessary that the computer is connected to the same LAN (broadcast domain) as the IPBS.

Determine the IP address following the steps below:

Note: If the IPBS has been used before, it must be restored to factory default settings by performing a long hardware reset, see 4.29 *Reset Using the Reset Button* on page 126. Then remove the power supply cable and connect it again.

1   Open a command window in windows by selecting **Start** > **Run** and enter **cmd** in the **Open: text** field.

2   Enter the following commands:
               C:\>nbtstat -R
      For IPBS1: **C:\>nbtstat -a ipbs-xx-xx-xx**
      For IPBS2: **C:\>nbtstat -a ipbs2-xx-xx-xx**

      Where xx-xx-xx should be replaced with the last 6 hexadecimal digits of the MAC-address.

3   The IP address is displayed in the command window, see the white frame in figure below.

4   Enter **http://xxx.xxx.xxx.xxx** (where *xxx.xxx.xxx.xxx* is the determined IP
     address) in the browser to access the GUI.

5   After the first startup of the IPBS do the following:
     On the IPBS: Select **LAN1** > **DHCP**

6   In **Mode** drop-down list, change the DHCP mode from **automatic** to **client** or
     disabled.

3.2.2   CHANGE THE DEFAULT PASSWORD

1   Enter the IP address determined in *3.2.1 Determine the IP Address* in the **web
     browser address** field.

2   Select **General** > **Admin**.

3   Enter user name and password in the dialog box.
     Default user name is: **admin**.
     Default password is: **changeme**.

4   Enter a user name in the **User Name** text field.

5   Enter a password in the **Password** text field. Repeat the password in the second
     text field.

6   Click **OK**.

3.3 GUI WEB ACCESS

3.3.1   LOGIN PAGE

When accessing IPBS through a web browser the initial page is the login page. This
page has two hyperlinks: *System Administration* and *User Administration*.

3.3.2 ACCESS LEVELS

Three types of web users (or *Access Levels*) are authorized to access IPBS:

- Auditors
- User Administrators
- System Administrators

The different types of access levels are described in the following table.

Access Level	Authorization	Login hyperlink on login page [a]	Described in section
Auditors	• Read access to device parameter settings • Can generate Service Reports	System Administration	*3.3.3 Auditors*
User Administrators	• Add, update and remove users	User Administration	3.3.4 *User Administrators* on page 18
System Administrators	• Write access to all device parameter settings (for example IP addresses, software upgrades) • Assign and modify access to other System Administrator and User Administrator account settings • Add, update and remove users	System Administration	3.3.5 *System Administrators* on page 19

a.Different users should use the hyperlink related to their access level. The system does not allow login by a link not related to the user's access level.

3.3.3 AUDITORS

Auditors have read access to device parameter settings but are not authorized to update those settings. Auditors are also allowed to generate Service Reports (Administration > Diagnostics > Service Reports).

The login steps for an auditor follow the steps of a normal system administrator login. See 3.3.5 *System Administrators* on page 19 for more information.

3.3.4 USER ADMINISTRATORS

IPBS is not supplied with pre-installed user administration accounts. Therefore, the first user administration account must be created by a system administrator (see 3.3.5 *System Administrators* on page 19). If additional user administration accounts are needed they must also be created by a system administrator, see *Managing User Administrators* on page 21.

User administrators can only administer users. They can view but not create or manage other user administrator accounts.

Login as User Administrator

To login as a user administrator:

1 Follow 3.2 *Access the GUI* on page 15 and access the device using a web browser.

2   *Select **DECT User Administration** from the drop-down list.*

3   Enter user name and password for a user administrator in the fields below the drop-down list.

Note: If mutual TLS authentication is used, the user name is inserted automatically from the certificate. If a user certificate is required, this user name must be used for login. See *4.1.7 Require User Certificate* on page 33.

4   Click **Login**. A welcome screen appears showing the current sessions, the last login date, and the number of failed login attempts. The failed login attempts counter shows only those login attempts when the user is not blocked.

Note: If the login fails, the user is blocked for a certain period of time, and every failed login attempt increases the time while the user is blocked. The minimum blocked time is 5 seconds and the maximum time is 1800 seconds.

5   Click **OK**.

6   The **User Administration** page is displayed.

    See the figure below for a sample.

Figure 1. User Administration Sample.

The right side of the page consists of two list sections:

•   *User Administrators* in the upper right section.
Note: this section is read-only since a user administrator cannot manage other user administrators. See *Managing User Administrators* on page 21.

•   *Users* in the lower right section. Refer to 3.13 *Add Users* on page 29.

3.3.5   SYSTEM ADMINISTRATORS

IPBS devices are factory delivered with a default system administrator account.

Log in as System Administrator

To login as a system administrator:

1   Follow 3.2 *Access the GUI* on page 15 and access the device using a web browser.

2   Select System Administration from the drop-down list.

3   Enter user name and password for a system administrator in the fields below the drop-down list.

Note: If mutual TLS authentication is used, the user name is inserted automatically from the certificate. If a user certificate is required, this user name must be used for login. See *4.1.7 Require User Certificate* on page 33.

4   Click **Login**. A welcome screen appears showing the current sessions, the last login date, and the number of failed login attempts. The failed login attempts counter shows only those login attempts when the user is not blocked.

Note: If the login fails, the user is blocked for a certain period of time, and every failed login attempt increases the time while the user is blocked. The minimum blocked time is 5 seconds and the maximum time is 1800 seconds.

5   Click **OK**.

Following tasks can be done:

- Managing the default system administrator account, see *The Default System Administrator Account* on page 20.
- Managing additional system administrator accounts, see *Additional Administrator Accounts* on page 20.

The Default System Administrator Account

The default system administrator account can be modified but cannot be deleted. To modify the default system administrator account, do as follows:

1   Login as system administrator (see *Log in as System Administrator*).

2   Select **General** > **Admin.**

3   Select/Enter the following settings:

Field name	Description
Device Name	Enter a description for the device.
User Name	Enter a login user name.
Password	Enter a password.
Confirm Password	Confirm the password.

Note: Only changing the password will not result in the settings being saved. For the settings to be saved, both user name and password must be updated at the same time!

4   Click "OK".

Additional Administrator Accounts

Note: To create additional administrator accounts, Kerberos must have been configured (see 4.1.8 *Centralized Management of Administrator and Auditor Accounts Using Kerberos* on page 36).

To create an additional administrator account, do as follows:

1   Log in as system administrator (see *Log in as System Administrator* on page
     19).

2   Select General > Kerberos

3   On the next free account row in the Users section:

     •   Enter User Name
     •   Enter Password
     •   Enter Password again
     •   Select *Administrator* (for System Administrator) or *Auditor* in the drop-down
          list (See 3.3.2 *Access Levels* on page 18 for a description of access levels.)

4   Click **OK**.

     The account row is created.

To modify an additional administrator account, do as follows:

1   Log in as system administrator (see *Log in as System Administrator* on page
     19).

2   Select General > Kerberos

3   On an existing account row in the Users section:

     •   Enter a new user name
     •   Enter a new password
     •   Enter the password again
     •   Select *Administrator* (for System Administrator) or *Auditor* in the drop-down
          list (See 3.3.2 *Access Levels* on page 18 for a description of access levels.)

4   Click **OK**.

     The account row is updated.

To delete an additional administrator account, do as follows:

1   Login as system administrator (see *Log in as System Administrator* on page 19).

2   Select **General** > **Kerberos**

3   On the row to be deleted, select the *Delete* check box.

4   Click **OK**.

     The account row is deleted.

Managing User Administrators

Create a User Administrator

IPBS is not supplied with preinstalled user administration accounts. Therefore, the first
user administration account must be created by a system administrator. If additional
user administration accounts are needed they must also be created by a system
administrator.

1   Log in as System Administrator (see *Log in as System Administrator* on page
     19).

2   Select **Users**.

3   Click **show**.

     The **User Administration** page (see figure 1 on page 19 for a sample) is
     displayed.

4   Click **new**.

5   Select the **User Administrator** radio box. The window layout transforms.

6   Enter a long name.

7   Enter a name

Note: This field is used for login.

8   Enter a password.

9   Confirm the password.

10   Click **OK**.

View and Modify a User Administrator

1   Login as System Administrator (see 3.3.5 *System Administrators* on page 19).

2   Select **Users**.

3   Click **show**

A two-part list page is displayed. At the top are the user administrator accounts and below the user administrators are the user accounts, both listed in alphabetical order.

4   In the **User Administrators** section, click the **hyperlink** to be edited below the Long Name heading. An **Edit User** window is opened.

5   Select/Edit any of the following settings:

- Long Name
- Name

Note: This field is used for login.

- Password
- Confirm Password

6   Click **OK**.

Delete a User Administrator

1   Login as System Administrator (see 3.3.5 *System Administrators* on page 19).

2   Select **Users**.

3   Click **show**

4   In the **User Administrators** section, click the **hyperlink** to be edited below the Long Name heading. An **Edit User** window is opened.

5   Click **Delete**.

The User Administrator is deleted and the windows is closed.

Logout

Click Logout in the upper-right corner to log out of the device and close your session.

For automatic logout settings, see *4.1.4 Set Automatic Logout* on page 33.

3.4 CONFIGURE THE MOBILITY MASTER

In a system with two or more Masters (Multiple Master system), a Mobility Master must be configured. For more information on Multiple Master Systems, see the applicable System Planning documentation for IP-DECT.

This section describes how to configure the Mobility Master. Each configuration step is briefly described in the step list below. For more detailed information see the corresponding subsection in 4 *Operation* on page 33.

1   Determine the address and access the GUI, see 3.2 *Access the GUI* on page 15.

2   Change the default password, see 3.2.2 *Change the Default Password* on page 17.

3   Set a static IP address and set DHCP to off, see 4.2.2 *Set a Static IPv4 Address* on page 54.

4   Set the mode to Mobility Master, see 4.6.26 *Select Mobility Master Mode* on page 83.

5   Write a login name and enter a password, see 4.6.26 *Select Mobility Master Mode* on page 83.

6   Connect to other Mobility Master(s), see 4.6.27 *Connect Mobility Master to other Mobility Master(s)* on page 84.

7   Enter the Time Server address, see 4.1.9 *Configure the NTP Settings* on page 47.

3.5 CONFIGURE THE STANDBY MOBILITY MASTER

It is recommended to have a Standby Mobilty Master in a Multiple Master IP-DECT system. This section describes how to configure the Standby Mobility Master. Each configuration step is briefly described in the step list below. For more detailed information see the corresponding subsection in 4 *Operation* on page 33.

1   Determine the address and access the GUI, see 3.2 *Access the GUI* on page 15.

2   Change the default password, see 3.2.2 *Change the Default Password* on page 17.

3   Set a static IP address and set DHCP to off, see 4.2.2 *Set a Static IPv4 Address* on page 54.

4   Set the mode to Standby Mobility Master, see 4.6.26 *Select Mobility Master Mode* on page 83.

5   Enter the Primary Mobility Master IP address, see 4.6.26 *Select Mobility Master Mode* on page 83.

6   Enter a login name and enter a password, this must be the same as in the Primary Mobility Master. See 4.6.26 *Select Mobility Master Mode* on page 83.

7   Connect to other Mobility Master(s). This should be the same Mobility Master(s) as in the Primary Mobility Master, see 4.6.27 *Connect Mobility Master to other Mobility Master(s)* on page 84.

8   Enter the Time Server address, see 4.1.9 *Configure the NTP Settings* on page 47.

3.6 CONFIGURE THE PARI MASTER

This section describes how to configure the Pari Master. Each configuration step is briefly described in the step list below. For more detailed information see the corresponding subsection in 4 Operation on page 33.

1   Determine the address and access the GUI, see 3.2 Access the GUI on page 15.

2   Change the default password, see 3.2.2 Change the Default Password on page 17.

3   Note: This step is not needed if the Pari Master is configured as Mirror. In that case, jump to the next step.
      Configure LDAP user name and password, select the Write Access check box, see 4.5.1 Configure LDAP Server on page 61.

4   Set a static IP address and set DHCP to off, see 4.2.2 Set a Static IPv4 Address on page 54.

5   Set the mode to Active or Mirror, see 4.6.19 Select Master Mode on page 77.

6   Perform a reset to restart the IPBS in Active or Mirror mode, see 4.28 Reset on page 125.

7   Select system name and password, see 4.6.1 Change System Name and Password on page 68.

8   Change subscription method, see 4.6.2 Set Subscription Method on page 68.

9   Configure authentication code, see 4.6.3 Configure Authentication Code on page 69.

10   Select tones, see 4.6.4 Select Tones on page 69.

11   Set default language, see 4.6.5 Set Default Language on page 69.

12   Set frequency band, see 4.6.6 Set Frequency Band on page 69.

13   Enable carriers, see 4.6.7 Enable/disable Carriers on page 70.

14   Enable local R-key handling, see 4.6.8 enable/disable Local R-Key Handling on page 70.

15   Enable No transfer on hangup, see 4.6.9 enable/disable No Transfer on Hangup on page 70.

16   Configure coder, see 4.6.16 Configure Coder on page 74.

17   Select supplementary services, see 4.6.18 Configure Supplementary Services on page 75.

18   Set Master Id, see 4.6.20 Set Master Id on page 78.

19   Enable Pari function, see 4.6.21 Enable PARI Function on page 78.

20   Enter gatekeeper IP address or ID, see 4.6.23 Configure Gatekeeper on page 79.

21   Connect to a Mobility Master, see 4.6.30 Connect Master to a Mobility Master on page 85.

22   Assign PARI, see 4.6.34 assign PARI on page 86.

23   Enter SARI, see 4.6.35 enter sARI on page 87.

24   Enter CPDM3/WSM3 IP address, see 4.8.1 Configure Messaging on page 92.

25   Enter the Time Server address, see 4.1.9 Configure the NTP Settings on page 47.

26   Reset in order to make the configuration changes take effect, see 4.28 Reset on page 125.

3.7 CONFIGURE THE STANDBY PARI MASTER

It is recommended to have a Standby Pari Master in the IP-DECT system. This section describes how to configure a Standby Pari Master. Each configuration step is briefly described in the step list below, for more detailed information see the corresponding subsection in 4 *Operation* on page 33.

1   Determine the address and access the GUI, see 3.2 *Access the GUI* on page 15

2   Change the default password, see 3.2.2 *Change the Default Password* on page 17.

3   *Note: This step is not needed if the Standby Pari Master is configured as Mirror. In that case, jump to the next step.*
       Configure LDAP replicator, enter the IP address, user name and password to the LDAP server (Pari Master). Alternative LDAP server must not be entered. Select the *Enable* check box, see 4.5.3 *Configure LDAP Replicator* on page 62.

4   Set a static IP address and set DHCP to off, see 4.2.2 *Set a Static IPv4 Address* on page 54.

5   Set the mode to Standby or Mirror, see 4.6.19 *Select Master Mode* on page 77.

6   Perform a reset to restart the IPBS in Standby or Mirror mode, see 4.28 *Reset* on page 125.

7   Enter system name and password, this should be the same system name and password as in the Pari Master, see 4.6.1 *Change System Name and Password* on page 68.

8   Select supplementary services, see 4.6.18 *Configure Supplementary Services* on page 75.

9   Set Master Id, see 4.6.20 *Set Master Id* on page 78.

10   Enable Pari function, see 4.6.21 *Enable PARI Function* on page 78.

11   Enter gatekeeper address, see 4.6.23 *Configure Gatekeeper* on page 79.

12   Connect to a Mobility Master, see 4.6.30 *Connect Master to a Mobility Master* on page 85.

13   Enter CPDM3/WSM3 IP address, see 4.8.1 *Configure Messaging* on page 92.

14   Enter the Time Server address, see 4.1.9 *Configure the NTP Settings* on page 47.

15   Reset in order to make the configuration changes take effect, 4.28 *Reset* on page 125.

3.8 CONFIGURE THE MASTER

This section describes how to configure the Master. Each configuration step is briefly described in the step list below. For more detailed information see the corresponding subsection in 4 *Operation* on page 33.

1   Determine the address and access the GUI, see 3.2 *Access the GUI* on page 15.

2   Change the default password, see 3.2.2 *Change the Default Password* on page 17.

3   *Note: This step is not needed if the Master is configured as Mirror. In that case, jump to the next step.*
       Configure LDAP user name and password, select the *Write Access* check box, see 4.5.1 *Configure LDAP Server* on page 61.

4   Set a static IP address and set DHCP to off, see 4.2.2 *Set a Static IPv4 Address* on page 54.

5   Set the mode to Active or Mirror, see 4.6.19 *Select Master Mode* on page 77.

6   Perform a reset to restart the IPBS in Active or Mirror mode, see 4.28 *Reset* on page 125.

7   Select system name and password, see 4.6.1 *Change System Name and Password* on page 68.

8   Set default language, see 4.6.5 *Set Default Language* on page 69.

9   Select supplementary services, see 4.6.18 *Configure Supplementary Services* on page 75.

10   Set Master id, see 4.6.20 *Set Master Id* on page 78.

11   Enter gatekeeper IP address or ID, see 4.6.23 *Configure Gatekeeper* on page 79.

12   Connect to a Mobility Master, see 4.6.30 *Connect Master to a Mobility Master* on page 85.

13   Enter CPDM3/WSM3 IP address, see 4.8.1 *Configure Messaging* on page 92.

14   Enter the Time Server address, see 4.1.9 *Configure the NTP Settings* on page 47.

15   Reset in order to make the configuration changes take effect, see 4.28 *Reset* on page 125.

3.9 CONFIGURE THE STANDBY MASTER

It is recommended to have a Standby Master in the IP-DECT system. This section describes how to configure a Standby Master. Each configuration step is briefly described in the step list below, for more detailed information see the corresponding subsection in 4 *Operation* on page 33.

1   Determine the address and access the GUI, see 3.2 *Access the GUI* on page 15.

2   Change the default password, see 3.2.2 *Change the Default Password* on page 17.

3   *Note: This step is not needed if the Standby Master is configured as Mirror. In that case, jump to the next step.*
Configure LDAP replicator, enter the IP address, user name and password to the LDAP server. Alternative LDAP server must not be entered. Select the *Enable* check box, see 4.5.3 *Configure LDAP Replicator* on page 62.

4   Set a static IP address and set DHCP to off, see 4.2.2 *Set a Static IPv4 Address* on page 54.

5   Set the mode to Standby or Mirror, see 4.6.19 *Select Master Mode* on page 77.

6   Perform a reset to restart the IPBS in Standby or Mirror mode, see 4.28 *Reset* on page 125.

7   Enter system name and password, this should be the same system name and password as in the Master. See 4.6.1 *Change System Name and Password* on page 68.

8   Select supplementary services, see 4.6.18 *Configure Supplementary Services* on page 75.

9   Set Master Id, see 4.6.20 *Set Master Id* on page 78.

10   Enter gatekeeper address, see 4.6.23 *Configure Gatekeeper* on page 79.

11 Connect to a Mobility Master, see 4.6.30 *Connect Master to a Mobility Master* on page 85.

12 Enter CPDM3/WSM IP address, see 4.8.1 *Configure Messaging* on page 92.

13 Enter the Time Server address, see 4.1.9 *Configure the NTP Settings* on page 47.

14 Reset in order to make the configuration changes take effect, see 4.28 *Reset* on page 125.

3.10 PLUG AND PLAY CONFIGURATION

Radios can be configured from the relevant Pari Master. When a new Radio is connected to the system, it automatically registers itself as an uninitialized registration to all Pari Masters in the system. It is possible to assign the Radio to one Pari Master. See *Add Radios* on page 107.

3.11 CONFIGURE THE RADIO

This section describes how to configure the Radio. Each configuration step is briefly described in the step list below, for more detailed information see the corresponding subsection in 4 *Operation* on page 33.

Note: When one Radio is configured, the configuration can be saved and uploaded to the other Radios in the system.

1 Determine the address and access the GUI, see 3.2 *Access the GUI* on page 15.

2 Change the default password, see 3.2.2 *Change the Default Password* on page 17.

3 Set DHCP mode to "Client", see 4.2.3 *Dynamic IPv4 address via DHCP* on page 54.

4 Enable the Radio in the IPBS, see 4.6.31 *Enable/disable the Radio* on page 85.

5 Select system name and password, see 4.6.1 *Change System Name and Password* on page 68.

6 Enter Pari Master and Alternative Pari Master IP addresses, see 4.6.32 *Enter IP Address to the PARI Master and the Standby PARI Master* on page 85.

7 Configure air synchronization, see 4.6.36 *Configure Air Synchronization* on page 87.

8 Enter the Time Server address, see 4.1.9 *Configure the NTP Settings* on page 47.

9 Reset in order to make the configuration changes take effect, see 4.28 *Reset* on page 125.

10 Save the configuration of the Radio, see 4.14 *Backup* on page 120.

Configure the rest of the IPBSs following the steps below:

Note: Uploading the same configuration to all Radios can only be done if the DHCP is set to client.

1 Determine the address.

2   Select Update > Config and browse to the previously saved configuration. Click "OK".

3   Reset in order to make the configuration changes take effect, see *4.28 Reset* on page 125.

4   Repeat step 1 to 3 for all Radios.

3.12 CONFIGURE DEPLOYMENT

This section describes how to configure an IPBS for deployment used for coverage test of air sync and speech.

NOTE: For coverage test of air sync, two IPBSs must be configured, one as Sync Master and one as Sync Slave.

Each configuration step is briefly described in the step list below. For more detailed information see the corresponding subsection in *4 Operation* on page 33.

3.12.1 CONFIGURE SYNC MASTER IPBS

1   Set the Master mode to Deployment, see 4.5.19 *4.6.19 Select Master Mode* on page 67.

2   In the PARI Master IP Address text field, enter loopback address 127.0.0.1, see 3.3.4 Radio on page 14.

3   Set the sync mode to Master, see *3.12.1 Configure Sync Master IPBS* on page 77.

4   If the IPBS shall be used without a network and a DHCP server, a static IP address must be set, see 4.2.2 *4.2.2 Set a Static IPv4 Address* on page 47.

Do as follows:

Select **LAN** > **DHCP**. In the Mode drop-down list, set the DHCP mode to **disabled.**

Select **LAN** > **IP**. In the **IP Address** text field, enter an IP address, e.g. 192.168.0.1.

5   Reset the IPBS in order to make the configuration changes take effect, see 4.28 Reset on page 127.

6   Select system name and password, see 4.5.1 Change System Name and Password on page 58.

7   Set frequency band, see 4.5.6 Set Frequency Band on page 59.

8   Enter **SARI**, see 4.5.36 Enter SARI on page 76.

9   Perform a reset to restart the IPBS, see 4.28 Reset on page 127.

10   For coverage test of speech sync, register one handset in the IPBS configured as Sync Master, see 3.14 Add Users on page 24.

3.12.2 CONFIGURE SYNC SLAVE IPBS

1   Set the Master mode to **Deployment,** see 4.5.19 Select Master Mode on page 67.

2   In the **PARI Master IP Address text** field, enter loopback address 127.0.0.1, see *3.3.3 Radio* on page 14.

3   Set the sync mode to Slave, see *3.12.2 Configure Sync Slave IPBS* on page 77.

4   If the IPBS shall be used without a network and a DHCP server, a static IP address must be set, see *4.2.2 Set a Static IPv4 Address* on page 47.

Do as follows:

Select **LAN** > DHCP. In the Mode drop-down list, set the DHCP mode to **disabled**.

Select **LAN** > **IP**. In the **IP Address text** field, enter an IP address, e.g. 192.168.0.1.

5   Reset the IPBS in order to make the configuration changes take effect, see 4.28 Reset on page 127.

6   Select system name and password, see *4.6.1 Change System Name and Password* on page 58.

7   Set frequency band, see *4.6.6 Set Frequency Band* on page 59.

8   Enter **SARI**, see *4.6.35 enter sARI* on page 76.

9   Perform a reset to restart the IPBS, see 4.28 Reset on page 127.

3.13 ADD USERS

This section describes how to add users to the IP-DECT system. The IPEI, which is the unique identification number of the handset, can be registered in three ways:

- Anonymous Registration can be used in en existing IP-DECT system. Instead of the administrator collects all the handset, the user of the handset does the registration. The IPEI is automatically associated to the user, see 3.13.1 *Anonymous Registration* on page 29.
- Individual Registration can be used if a few new handsets shall be added to the IP-DECT System. The IPEI is entered manually, see 3.13.2 *Individual Registration* on page 31.
- Easy Registration can be used if many users shall be added to the IP-DECT System. The IPEI is entered with for example a barcode reader to a csv file, see 3.13.3 *Easy Registration* on page 32.

Note: Display Name is only used during Active Directory (AD) replication, see *Attribute Mappings* on page 64.

3.13.1 ANONYMOUS REGISTRATION

Anonymous Registration is done in two steps. First, the user is registered in the IP-DECT System. Second, the handset is assigned to the user from the handset.

Add users in the IP-DECT System

1   Under *Administration*, select "Users".

2   Click "New".

3   Enter the following information in the corresponding text fields, leave the *IPEI / IPDI* text field empty, do not remove the automatically generated *Auth. Code*:

Field name   **Description**   **Max. characters**

Long Name	Mandatory, the name of the user, need to be unique throughout the system.	30
Display Name	Optional (Not used with Mitel call servers).	30
Name	Optional, the user name.	30
Number	Mandatory, the phone number extension, need to be unique throughout the system.	30
Auth Name (SIP)	Auth name is the Authentication name used in SIP authentication. If it is not set the number will be used as authentication name. If SIP authentication is used or not is decided by the configuration in the IP-PBX.	60
Password	Optional, is used for registration towards the gatekeeper. However, in a system with many users where the same password shall be used for all users, instead of setting the password here, it is possible to use the system password for registration towards the gatekeeper. To enable registration with system password, see *4.6.23 Configure Gatekeeper* on page 79.	30
Idle Display	Optional, will be shown in the handset display when the handset is idle.	47

4   Click "OK".

5   Repeat step 2 to 4 for all users.

Assign Handsets to Users

1   Select **DECT** > **System**.

2   In the **Subscriptions** drop-down list, select **With System AC** to enable anonymous registration. Click **OK**.

3   Perform an "over air subscription" using the system Authentication Code. For information on how this is done, see the reference guide of the handset.
The handset IPDI number appears in the Anonymous list. To view the list: Select Users > Anonymous.

4   Assign the handset to any user, subscribed or unsubscribed, on any Master defined in the system by calling the desired Master id & extension & optional individual AC code and hang up.
Example where **0** is the Master id, **200** is the extension and **1234** is the AC code: *0*200*1234#. If **200** is occupied by another handset, the new handset will be assigned this identity and the old handset will be moved to the anonymous list when logging in the new handset.
NOTE: When using AC code, start with * and end with # character. Otherwise skip the *# characters.

5   Repeat step 3 - 4 for all handsets.

Note: For safety reasons, when the Anonymous Registration is finished change the Subscription Method to **Disable** or **With User AC**. See below for more information.

6   Select **DECT** > **System**.

7   Disable anonymous registration by selecting **Disable** or **With User AC** in the **Subscription** drop-down list. Click **OK**.

3.13.2 INDIVIDUAL REGISTRATION

1   Select **DECT** > **System**.

2   In the **Subscriptions** drop-down list, select **With System AC** or **With User AC**. Click **OK**.

      Tip: See also 4.6.2 *Set Subscription Method* on page 68 for more information.

3   Select **Users**.

4   Click **New**.

5   Enter the following information in the corresponding text fields:

Field name	Description	Max. characters
Long Name	Mandatory, the name of the user, need to be unique throughout the system.	30
Display Name	Optional (Not used with Mitel call servers).	30
Name	Optional, the user name.	30
Number	Mandatory, the phone number extension, need to be unique throughout the system.	30
Auth Name (SIP)	Auth name is the Authentication name used in SIP authentication. If it is not set the number will be used as authentication name. If SIP authentication is used or not is decided by the configuration in the IP-PBX.	60
Password	Optional, is used for registration towards the gatekeeper. However, in a system with many users where the same password shall be used for all users, instead of setting the password here, it is possible to use the system password for registration towards the gatekeeper. To enable registration with system password, see *4.6.23 Configure Gatekeeper* on page 79.	30
IPEI / IPDI	The unique identification number of the handset.	
Idle Display	Optional, will be shown in the handset display when the handset is idle.	47
Auth. Code	Optional, the individual authentication code for this user. Automatically created by default. Can be modified manually.	

6   Click **OK**.

7   If "With User AC" have been selected as subscription method, see step 2 above: In the column "IPEI / IPDI", click on the blue text link for the user to allow subscription within 2 minutes.

8   Perform an "over air subscription" using the individual authentication code. For information on how this is done, see the reference guide of the handset.

3.13.3 EASY REGISTRATION

Easy Registration is done in two steps. First, the users are registered in the IP-DECT System through an import of a csv file. Second, the handset is assigned automatically to the user from the handset.

Add users in the IP-DECT System

If many users should be added it is possible to import a csv file with the IPEI / IPDI.

Field name	Description	Max. characters
Long Name	Mandatory, the name of the user, need to be unique throughout the system.	30
Display Name	Optional and only available when using the Ascom VoIP Gateway, the calling or called party name will be shown in the handset (Not used with Mitel call servers).	30
Name	Optional, the user name.	30
Number	Mandatory, the phone number extension, need to be unique throughout the system.	30
Auth Name (SIP)	Auth name is the Authentication name used in SIP authentication. If it is not set the number will be used as authentication name. If SIP authentication is used or not is decided by the configuration in the IP-PBX.	60
Password	Optional, is used for registration towards the gatekeeper. However, in a system with many users where the same password shall be used for all users, instead of setting the password here, it is possible to use the system password for registration towards the gatekeeper. To enable registration with system password, see 4.6.23 *Configure Gatekeeper* on page 79.	15
IPEI / IPDI	The unique identification number of the handset.	
Idle Display	Optional, will be showed in the handset display when the handset is idle.	47

The csv file may have the following format:

Long Name;Name;Number;Display Name;Auth Name (SIP);Idle Display;IPEI/IPDI;Password;

Different separators may be used in a delimiter-separated file. Import of files with the separators semicolon or TAB is supported.

1   Select **Users**.

2   Click **Import**.

3   Click **Browse** to locate the csv file.

4   Click **Open** > **Next**. Ensure the correct number of entries are correct.

5   Click **Next**.

Limitations

- Maximum 1000 rows in the csv file.
- The maximum csv file size is 128 Kb. If the file is to large, divide the file into several files.
- Only the new user data is imported. The old user data is not deleted.
- Existing user data cannot be updated.
- If the separator is wrong an error message will be displayed.
- The Authentication Code (AC) can not be entered in the csv file for safety reasons. The system generates a AC for every user in the list. If the user needs the AC the administrator will have to use Show, see 4.10.1 *Show all Registered Users in the IP-DECT System* on page 103.
- The software in the DECT Handset must have support for Easy Registration.

Assign Handset to Users

1   Select **DECT** > **System**.

2   In the *Subscriptions* drop-down list, select "With User AC" or "With System AC" to enable easy registration. Click "OK".

3   If "With User AC" have been selected as subscription method:
        In the column "IPEI / IPDI", click on the blue text link for the user to allow subscription within 2 minutes.

4   Perform an "over air subscription" by inserting the battery in the handset. The handset automatically connects to the IP-DECT system and assigns to the correct user.

4   OPERATION

This section describes the settings in the Configuration and Administration menu, each subsection represents a sub menu to the Configuration and Administration menu.

Some changes require a reset in order to take effect. It is possible to do several changes before resetting the IPBS.

4.1 GENERAL

This section describes how to do the following configurations and settings.

- Name the equipment
- Change Administrator User Name and Password
- Kerberos
- Display Login Text
- Local Security Policy
- Configure the NTP settings

Figure 2. Assigning an administrator name, username, and password.

4.1.1   NAME THE IPBS

Each IPBS can be assigned a name. It is recommended to assign a descriptive name for example IPBS location.

1   Select **General** > **Admin**.

2   Enter a name in the **Device Name text** field.

3   Click **OK**.

4.1.2   CHANGE USER NAME AND PASSWORD

The user name and password are used to access the IPBS through the web GUI.

1   Select **General** > **Admin.**

2   Write a user name in the **User Name text** field.

3   Enter a new password in the **Password text** field. Repeat the password in the second text field.

4   Click **OK**.

4.1.3   DISPLAY LOGIN TEXT

An informative text or a security warning can be displayed on the login page to inform the user.

1   Select **General** > **Admin**.

2   Enter the desired text in the **Login Banner text** field.

3   Click **OK**.

4.1.4   SET AUTOMATIC LOGOUT

The user will automatically be logged out after being inactive for the time specified here.

The feature is disabled if the field is empty.

1   Select **General** > **Admin**.

2   Enter the idle time in the **Automatic Logout** after field.

3   Click **OK**.

4.1.5 LIMIT SESSIONS

The total number of parallel login sessions can be limited per user or per system. The feature is disabled if the fields are empty.

1   Select **General** > **Admin**.

2   Enter the allowed number of sessions per system and/or per user in the **Limit Sessions to** field.

3   Click **OK**.

4.1.6 DISABLE NATIVE AUTHENTICATION

The use of http authentication can be disabled and the form-based login is used all the time when user authentication is required. Native authentication is disabled by default.

1   Select **General** > **Admin**.

2   Select the **Disable Native Authentication** check box.

3   Click **OK**.

4.1.7 REQUIRE USER CERTIFICATE

If mutual TLS is used to login, the device does not usually check that the trusted client certificate is issued to the user who is trying to login. For enhanced security the device can require that a trusted client certificate issued to the user is available to be able to login.

The following conditions must be met before enabling this feature:

- A trusted client certificate with the associated private key must be available in the web browser's certificate store. The Subject Alternative Name in the certificate must correspond to the User ID entered at login. See "Import Server Certificate in the Web Browser" on page 156. The trusted client certificate issued to the user or the CA certificate that signed client certificate must be added to the trust list in the device. See *Trust List* on page 46.
- Mutual TLS authentication must be enabled. See 4.9.3 *Configure the HTTP settings* on page 96.

IMPORTANT: Ensure that the correct certificate is installed before requiring a user certificate. If the correct certificate is not available, and mutual TLS authentication is enabled, it is not possible to access the device in any other way.

1   Select **General** > **Admin**.

2   Select the **Require Certificate** check box.

3   Click **OK**.

4.1.8   CENTRALIZED MANAGEMENT OF ADMINISTRATOR AND AUDITOR ACCOUNTS USING KERBEROS

In software version 3.X.X, each IPBS had their own set of administrator/auditor accounts. Kerberos is a network authentication protocol that is used when you want to have the same set of user accounts for several IPBSs and then want to administrate these user accounts at one central location (Kerberos server). When an IPBS is setup as a Kerberos server the IPBS act as an authentication server for the rest of the IPBSs that are setup as client devices in the installation. The Kerberos server and the group of client devices constitute a domain called a realm. During Kerberos communication no password is actually sent over the network. Kerberos uses encrypted data packets (tickets) which are time-stamped and expire after a certain period of time. Therefore it is crucial to get the correct time across the system for which a NTP server should be used.

Set up the Kerberos server

It is recommended to set up the Kerberos server on the Master. To configure an IPBS to act as a Kerberos server, do the following:
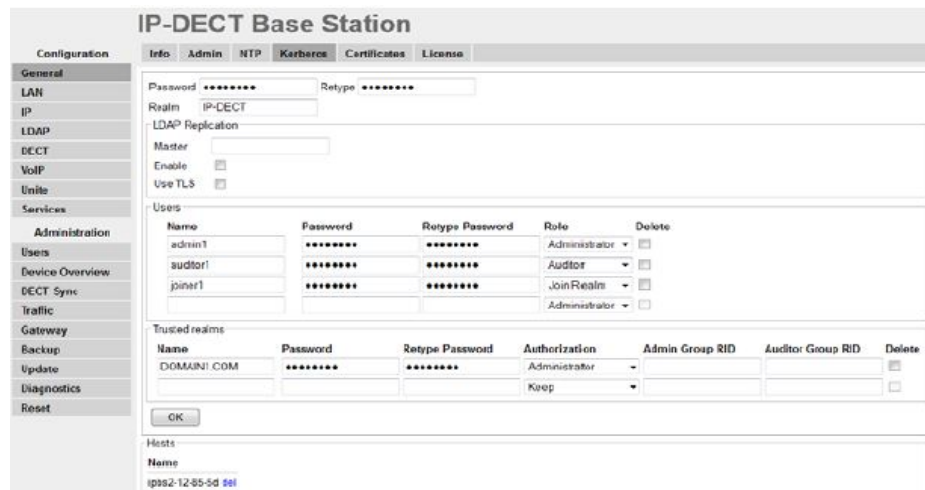
Figure 3. Configure Kerberos server

1   Ensure that the IP address of a NTP time server is specified. Select **General** > **NTP**.

2   Select **General** > **Kerberos**.

3   Enter a root password for the Kerberos server. This password is used to encrypt the information stored on the server.

4   Click **OK**.

5   The Kerberos server is enabled. Enter the realm name of your choice in the Realm field. The Kerberos realms are typically written in upper-case letters.

6   Select/Enter the following information for the users of the realm.

Field Name	Description
Name	Enter a login user name.

Password	Enter a password.
Retype Password	Confirm password.
Role	• Administrator: Write access to all device parameter settings. • Auditor: Read access to device parameter settings. • Join Realm: Add devices to the realm. Is used only to add or remove devices in the realm. This role cannot be used to login to the GUI.

7   Click **OK**.

Set up the client

Depending on the type of system the IPBS can be configured to act as a client in three different ways:

- Configure IPBS as a client in a small existing system (few clients), see *Configure IPBS as a client in a small existing system (few clients)*.
- Configure IPBS as a client in a large existing system (many clients), see *Configure IPBS as a client in a large existing system (many clients)* on page 38.
- Configure IPBS as a client in a new system, see *Configure IPBS as a client in a new system* on page 38.

Configure IPBS as a client in a small existing system (few clients)

The location of the Kerberos server must be configured locally on each client. The server must be configured as a client as well so that it can also join the realm. To configure each IPBS as a client, do the following:

1   Ensure that the IP address of a NTP time server is specified. Select **General** > **NTP**.

2   Select **General** > **Admin**.

3   Go to the **Additional Kerberos encryption types** section.

4   Select the **Enable AES** and **RC4** check box.

5   Go to the **Authentication Servers** section.

6   In the **Realm/Domain** text field, enter the realm name specified in the Kerberos server.

7   In the **Address** text field, enter the IP address of the Kerberos server. In the Kerberos server enter 127.0.0.1 (localhost) as the IP address. The Port and the *Admin Port* text fields are filled out automatically with default ports. Note: If other than default ports are used, in the text fields replace the default ports with the other ports.

8   In the **Secondary Address** text field, enter the IP address of the secondary Kerberos server. In the secondary Kerberos server enter 127.0.0.1 (localhost) as the IP address. The **Secondary Port** and the **Secondary Admin Port** text fields are filled out automatically with default ports. Note: If other than default ports are used, in the text fields replace the default ports with the other ports.

9   Click **OK**.

Join the realm

To enable delegated authentication using the Kerberos server, each client must join the Kerberos realm of the server. To join the realm, do the following:

1   Select **General** > **Admin**.

2   Click on the blue text link **Join realm** in the **Delegated Authentication** section.

3   In the Join Kerberos realm window, enter the following in the text fields:
Realm: Enter the realm name of the Kerberos server.
Host name: The MAC address of the device. Default value is used.
Admin user name and Admin password: Enter the user name and password for a user with administrator account or "join realm" account on the Kerberos server.

4   Click **Join**.

Configure IPBS as a client in a large existing system (many clients)

Requirements for IPBS: Software version 6.1.X is required if Windows 2008 R2 server is used.

1   Setup the update server using the update script described in *Appendix E: Update Script for Configuration of Kerberos Clients*.

2   Select **DECT** > **Radio config**.

3   Go to the **Update** section.

4   In the Command File URL text field, enter the path to the update server and the name of the update script.

5   In the Interval (min) text field, enter the update period.

6   Click **OK**.

After the script is executed and each Radio is restarted, the Kerberos client will join the Kerberos Server and it shall be possible to see all joined Kerberos clients in the bottom of the Kerberos Server tab.

The way the update script is done in *Appendix E: Update Script for Configuration of Kerberos Clients* it will automatically disable the local login possibilities if the joining was successful.

The password used in the script is now possible to change to a more secret password from the Kerberos server page.

It shall now be possible login to the Radio using the Kerberos login credentials, see *Log in using Kerberos* on page 39.

Configure IPBS as a client in a new system

Precondition: The IPBS must have software version 4.1.X or higher.

The idea is to use the Device Overview -> Add to configure the Radios and the Kerberos Client. By using this feature it is not needed to browse into each Radio for configuration.

The Radios are in broadcast mode which means none of them are attached to the Master and configured. If any of the Radios are attached to the master and configured, the Radios must be detached from the Master if this procedure shall work.

1   Select **Device Overview** > **Radios**.

2   Click **Add** to add the Radio to the Master.

3   In the **Add Radio** window, enter a name for the device. You can also add a Standby Master IP Address.

4   Go to the **Kerberos** section and enter the following in the text fields:
Realm: Enter the realm name of the Kerberos server.
Host name: Optional.
User: Enter the same user name defined in the Kerberos server.
Password: Enter the same password defined in the Kerberos server.
Disable local authentication: Select the Disable local authentication check box (recommended).
Enable AES and RC4: Select the *Enable AES and RC4* check box.
Overwrite existing: Select the Overwrite existing check box (optional).

5   Go to the **Authentication Servers** section.

6   In the **Realm/Domain** text field, enter the realm name specified in the Kerberos server.

7   In the **Address** text field, enter the IP address of the Kerberos server. In the Kerberos server enter 127.0.0.1 (localhost) as the IP address. The Port and the *Admin Port* text fields are filled out automatically with default ports. Note: If other than default ports are used, in the text fields replace the default ports with the other ports.

8   In the **Secondary Address** text field, enter the IP address of the secondary Kerberos server. In the secondary Kerberos server enter 127.0.0.1 (localhost) as the IP address. The **Secondary Port** and the **Secondary Admin Port** text fields are filled out automatically with default ports. Note: If other than default ports are used, in the text fields replace the default ports with the other ports.

9   Click **OK**.

Log in using Kerberos

1   Ensure that secure HTTPS protocol is used when logging in.

2   Login on the client using a server account. When prompted for user name, the name of the realm has to be entered in front of the user name, separated by a backslash in the following way: REALM\username or username@REALM.

Note: If mutual TLS authentication is used, the user name is inserted automatically from the client certificate. If a user certificate is required, the Subject Alternative Name in the certificate must include the realm in the following format: **username@REALM** or **username@domain.com** where domain.com equals the realm. See *4.1.7 Require User Certificate*.

Disable local authentication

It is recommended to disable local authentication after Kerberos authentication is configured. It provides additional security and it is much easier to change the password of a user account or delete a compromised user account on the Kerberos server than changing the local user accounts on each IPBS.

IMPORTANT: Make sure that the Kerberos authentication is working properly before disabling local authentication. If the Kerberos authentication is not working and local authentication is disabled it is not possible to access the IPBS in any other way.

1   In the **Delegated Authentication** section select the **Disable local authentication** check box.

2   Click **OK**.

Configure cross-realm authentication

Cross-realm authentication is used to authenticate users from another trusted realm. In this way it is possible for IP-DECT users to login to the IPBS using their Windows user name and password in the Active Directory (AD). Security policies of the AD can then be used in IP-DECT. The trust relationship between the two realms is confirmed by configuring a shared password on both servers in the realms. This password is used to encrypt communication between the realms. To configure cross-realm authentication, do the following:

Requirements for IPBS1 and IPBS2:

*   Software version 6.1.X and later
*   NTP configured
*   Make sure that the device has been configured as a client in the system, see *Set up the client* on page 37.
*   Make sure that the AES and RC4 encryption types are enabled. Select General > Admin and select the *Enable AES and RC4* check box.

AD server configuration for Windows 2008 R2 servers:

The trust relationship must be configured in the AD server.

3   Connect to the Windows 2008 R2 server.

4   In the Windows Start menu select Administrative Tools > Active Directory Domains and Trusts

5   Right-click the realm name you wish to establish a cross realm trust with and select **Properties**.

6   Select the General tab and make a note of the windows realm name.
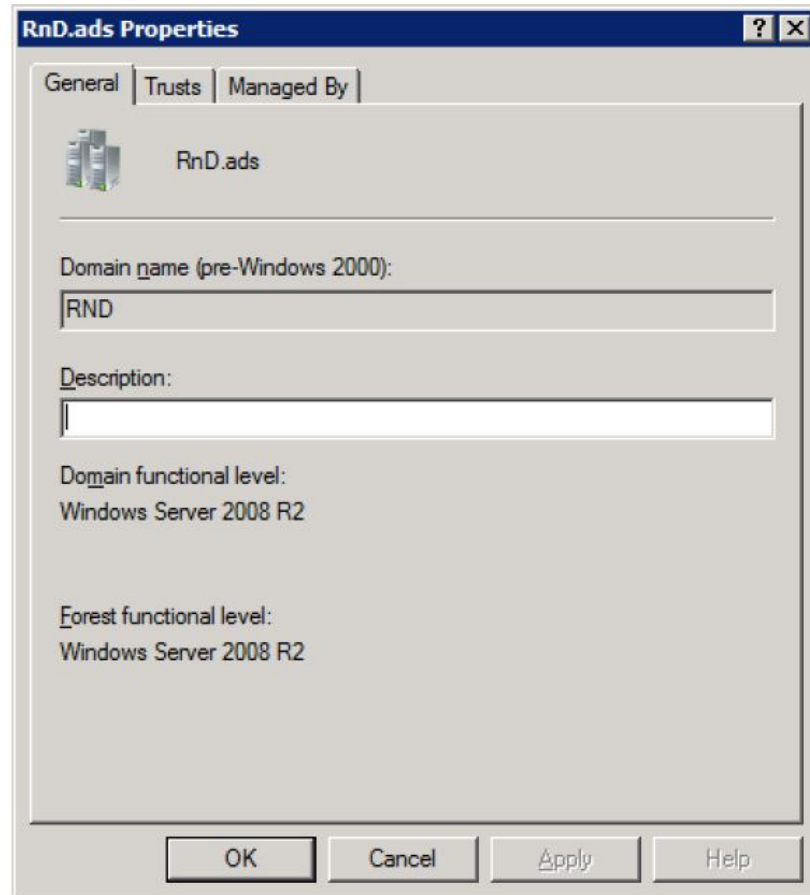
7   Click the Trusts tab and click **New Trust...**.

8   The New Trust Wizard appears. Click **Next.**

9   Enter the name of the Kerberos realm. Must be capital letters. Click **Next**.

10   Select **Realm trust**. Click **Next**.

11   Select **Nontransitive**. Click **Next.**

12   Select **One-way incoming**. Click **Next**.

13   Enter a password that will be a shared secret between the AD server and the Kerberos server. Make a note of the password and click **Next**.

14   Click **Next**.

15   Click **Finish**.

16   Click the **Trusts** tab. Select the realm that you have established a cross realm trust with and click **Properties...**.
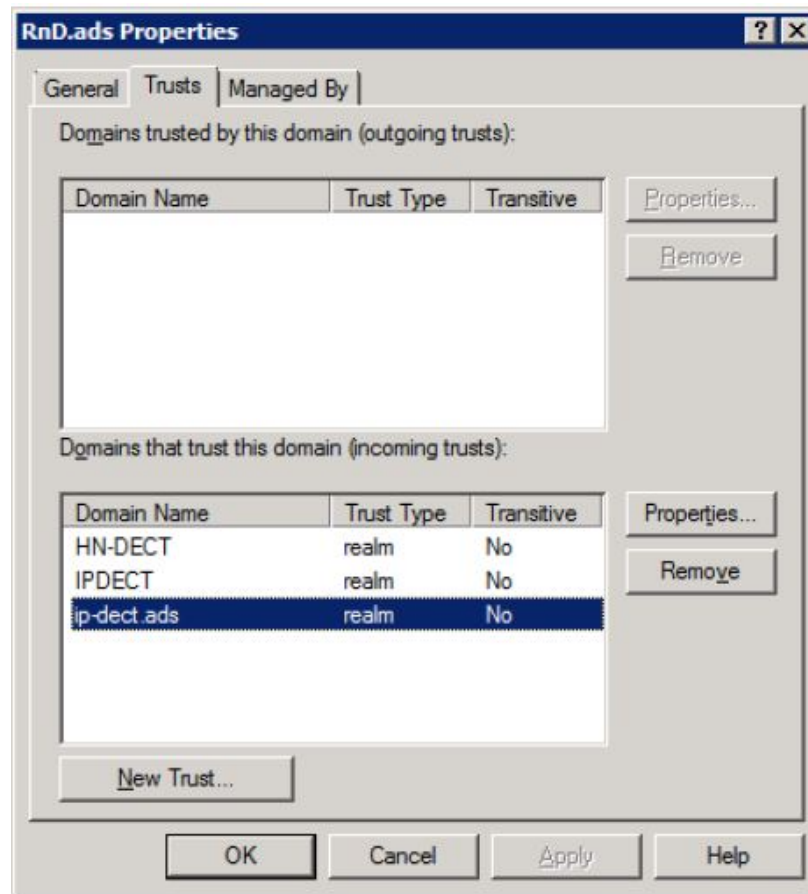
17   Select the **The other domain supports Kerberos AES Encryption** check box.
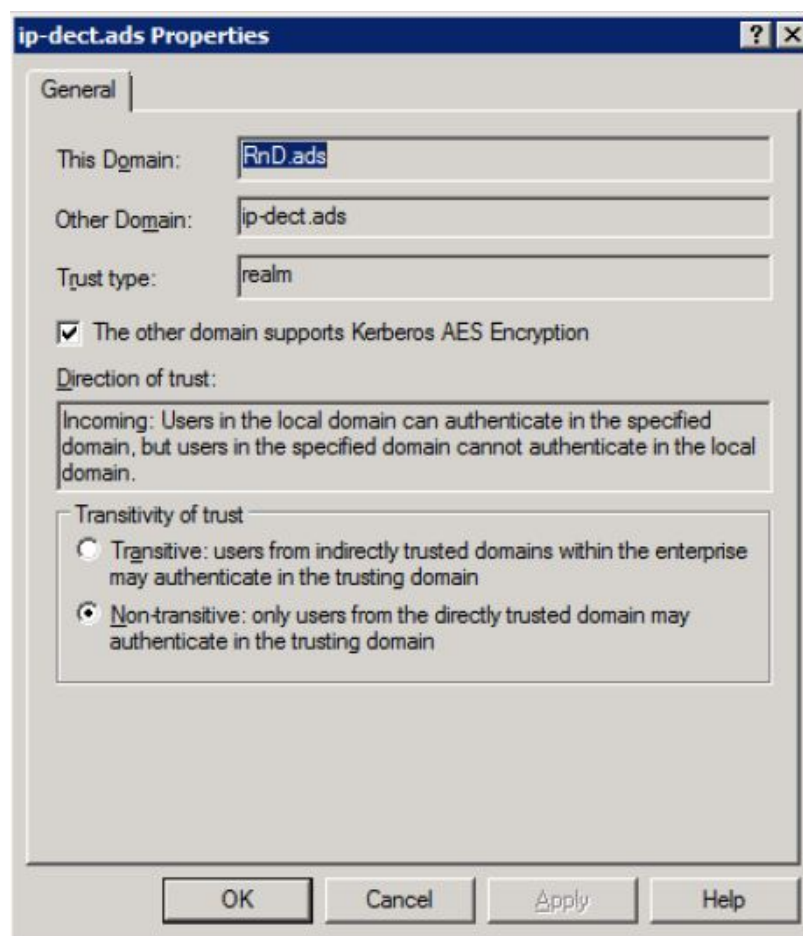
18   Click **OK**.

On IPBS1 and IPBS2 (the Kerberos server):

19   Select **General** > **Kerberos**.

20   In the **Trusted realms** section and the **Name text** field, enter the name of the realm of the AD server (see step 9). Must be capital letters.

21   In the **Password** text field, enter the password entered in step 13.

22   In the **Authorization** drop-down list, select "Use domain group" (recommended).

About "Use domain group", "Administrator" and "Auditor":

• "Use domain group": Only users belonging to a specified AD group will have administrator and auditor access rights.

• "Administrator": All Windows domain users have administrator access rights.

• "Auditor": All Windows domain users have auditor access rights.

23   Note: This step is only applicable if "Use domain group" is selected in the *Authorization* drop-down list, see above.

In the **Admin Group RID** text field, specify the Relative Identifier (RID) of a Windows group with administrator rights.

In the **Auditor Group RID** text field, specify the Relative Identifier (RID) of a Windows group with auditor rights.

The RID is the last part of the Security Identifier (SID) of a group.
Here is an example of a SID where the last five digits (in bold) are the RID: S-1-5-21-4151926548-1272113248-3927039109-**11265**.

To determine the SID of a group, do as follows:
1. Start Windows Command Prompt (cmd.exe). To find Windows Command Prompt, enter "cmd.exe" in Windows Start Menu search field.
2. In Windows Command Prompt, enter "whoami /groups". This command displays the group information of the user logged in to the Windows domain.

24   Click **OK**.

About security groups in AD
Groups are characterized by their scope and their type (security or distribution). Using security groups, you can assign user rights to security groups in AD.
The scope of a security group determines the extent to which the security group is applied within a domain or forest. There are three scopes that can be selected when creating a security group:

- **Universal** - Can contain users/universal groups/global groups from all domains in the forest. Can PARTLY be used in trusted domains, but maybe

makes little sense as only users/groups of the trusted domain will work in IP-DECT.

- makes little sense as only users/groups of the trusted domain will work in IP-DECT.
- **Global** - Can only contain users/global groups from the same domain. Can be used in trusted domains.
- **Domain Local** - Can contain any users/universal groups/global groups of the forest and domain local groups of the same domain. Can NOT be used in trusted domains.

With the above said, it is recommended to select Global as scope for security group.
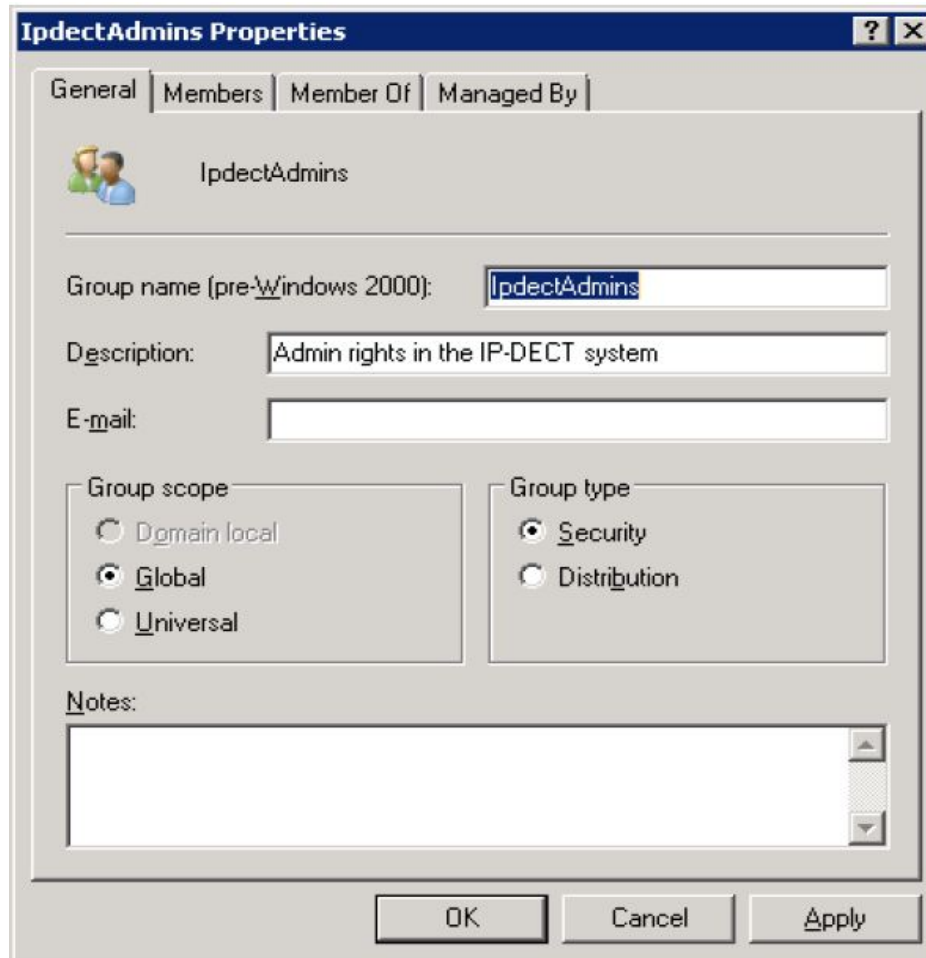
On IPBS1 and IPBS2 (the client):

25   Select **General** > **Admin**.

26   In the **Authentication Servers** section and the **Realm/Domain** text field, enter the realm name of the AD server (see step 9). Must be capital letters.
Note: This has not to be done if a DNS server has been configured to be used in the IP-DECT system. In this case the clients will look up the needed information automatically.

27   In the **Address text** field, enter the IP address of the AD server.

28   Click **OK**.

Log in using Kerberos cross-realm authentication

1   Ensure that secure HTTPS protocol is used when logging in.

2   Login on the client using a Windows server account. When prompted for user name, the name of the Windows domain has to be entered in front of the user name, separated by a backslash in the following way: DOMAIN\username or username@DOMAIN.

Configure secondary Kerberos server

The Kerberos server is crucial when using Kerberos authentication, so it is recommended to have a secondary Kerberos server in the IP-DECT system. The secondary server is used if the primary server is not working properly. It is recommended to set up the secondary Kerberos server on the Standby Master. To configure an IPBS as a secondary Kerberos server, do the following:

1   Ensure that the IP address of a NTP time server is specified. Select General > NTP.

2   Select **General** > **Kerberos**.

3   Enter the root password for the secondary Kerberos server which should be the same as the password used for the primary server. This password is used to encrypt the information stored on the server.

4   Click **OK**.

5   The secondary Kerberos server is enabled. Enter the realm name in the Realm field.

6   LDAP is used to replicate the primary server database. Enter the IP address of the primary Kerberos server in the Master field in the LDAP Replication section. For more information about LDAP, see 4.5 *LDAP* on page 61.

7   Select the **Enable** check box.

8   Select the **TLS** check box.

9   Click **OK**.

10   Click **OK** again to perform the LDAP replication.

Each client must also be configured with the secondary server information.

11   Select **General** > **Admin**.

12   Go to the **Authentication Servers** section.

13   In the *Secondary* Address text field, enter the IP address of the secondary Kerberos server. In the secondary Kerberos server enter 127.0.0.1 (localhost) as the IP address. The *Secondary* Port and the *Secondary Admin Port* text fields are filled out automatically with default ports. Note: If other than default ports are used, in the text fields replace the default ports with the other ports.

14   Click **OK**.

Delete a user or trusted realm

To delete a user account from the Kerberos server do the following:

1   Select **General** > **Kerberos**.

2   In the Users section select the Delete check box for the user to be deleted.

3   Click **OK**.

To delete a trusted realm relationship from the Kerberos server do the following:

1   Select General > Kerberos.

2   In the Trusted Realms section select the Delete check box for the realm to be deleted.

3   Click **OK**.

Deactivate Kerberos realm membership

IMPORTANT: Make sure that local authentication is enabled and working properly before leaving the Kerberos realm. If local authentication is still disabled and the IPBS is no longer a member of the realm it is not possible to access the IPBS in any other way.

1   Select **General** > **Admin**.

2   In the **Delegated Authentication** section clear the Disable local authentication check box.

3   Click **OK**.

To deactivate the Kerberos membership for a client, do the following:

1   Select **General** > **Admin**.

2   Go to the **Kerberos** section and click on the blue text link **Leave realm**.

3   It is possible to deactivate Kerberos realm membership in two ways:

- Deregister: The client is removed from the server database.
  In the *Leave Kerberos realm* window, enter the user name and password for a user with administrator or join the realm account in the *Deregister with Kerberos server* section.
  Click **Deregister**.

- Delete: Leave the realm without removing data from the server.
  Click **Delete**.

4.1.9   CONFIGURE THE NTP SETTINGS

Since the IPBS does not have a battery-backed real-time clock, the internal time will be set to 0:00 hrs, 1.1.1970 in the case of a restart.

In order to get the correct time in the system, specify the IP address of a NTP time server. The IPBS will synchronize its internal clock to the time server at startup and at the specified intervals. The clock is, for example, used by the handsets and log files.

Figure 4. Configure NTP settings

1   Select **General** > **NTP**.

2   Enter the IP address or the fully qualified domain name (FQDN) to the primary NTP server in the Time Server text field.

3   Enter a time interval in the Interval (min) text field.

4   Select time zone in **Time zone** drop-down list. If the desired time zone is not in the list, select **Other** and edit the String text field following the instructions in the next step.

5   Enter the timezone string if automatically updates summer/winter is desired.

     <String: StdOffset [Dst[Offset], Date/Time, Date/Time]>

     • Std: Time zone (for example EST for Eastern Standard Time).
     • Offset: time difference between the timezone and the UTC (Universal Time Coordinator).
     • Dst: summertime zone (for example EDT for Eastern Daylight Time).
     • Second Offset : time difference between the summer time and the UTC.
     • Date/ Time, Date/ Time: beginning and end of summertime.
         - date format: Mm.n.d (d day of n week in the m month)
         - time format: hh:mm:ss in 24-hour format.

     Note that a week always starts on a Sunday and the number for Sunday is 0.

     Example:
     North Carolina is located in the Eastern Time Zone. Eastern Standard Time (EST) is 5 hours behind UTC (StdOffset: EST5), the Eastern Daylight Time (EDT) is 4 hours behind UTC (DstOffset: EDT4). Summertime for the year 2013 begins at two a clock, on a Sunday, the second week in March (M3.2.0/2). The summertime ends at two a clock, on a Sunday, the first week in November (M11.1.0/2).

     <String: EST5EDT4,M3.2.0/2,M11.1.0/2>

6   Click **OK**.

4.1.10 CERTIFICATES

The Certificates tab is part of IP Security in IP-DECT. For more information on IP Security, see chapter *2 IP Security* on page 11.

Select **General** > **Certificates**.

Trust List

A trust list is set up when the device must know which third parties (for example IP-PBX) it shall trust in. The list contains the certificates to be accepted by the device for TLS secured connections (for example HTTPS, SIPS).

Trust list

	Subject	Issuer	Not before	Not after	Download
☑	ccmutv	ccmutv	04.03.2010	04.03.2015	PEM DER
☐	00-01-3e-00-b6-b4	00-01-3e-00-b6-b4	07.03.2011	07.03.2012	PEM DER

[Remove] [Clear]

Download all

File: [   ] [Browse...]

[Upload]

The following table describes the different functions.

Field name	Description
Subject	Click the hyperlink (under the Subject header) to display certificate details in a window.
PEM	Click the PEM hyperlink (under the Download header) to download the certificate in PEM format.
DER	Click the DER hyperlink (under the Download header) to download the certificate in DER format.
Remove	To remove a certificate: Select the check box for the certificate and click the Remove button.
Clear	To remove all certificates from the trust list: Click the Clear button.
Download all	Click the Download all hyperlink (under the Remove button) to download the complete trust list as a PEM encoded text file.
Upload	Use the Upload function to upload a certificate file to the device.
	1 Click the Browse button
	2 Select a certificate file
	3 Click the Upload button to upload the file to the device.

Rejected Certificates

This list contains the certificate chains that were rejected before, while trying to establish a secure TLS connection. This happens for example if the certificate is expired or neither the certificate nor any of the issuing CAs is trusted. If one of that certificates should be trusted for future connections you can select and add it to the trust list, directly.

The following table describes the different functions.

Field name	Description

Subject	Click the name of a certificate to display its details in a window.
Clear	Discard all rejected certificate chains.
Trust	Click this button to add the selected certificates to the trust list and remove the corresponding chains from the rejected certificates..

Device Certificate

As described in *2. Certificate Handling Options with Device Certificates* on page 13, there are four possible certificate options:

1   Default device certificate, see *Default Device Certificate* on page 50.

2   Self-signed certificates, see *Self-signed Certificates* on page 51.

3   Certificates signed by a Certificate Authority (CA), see *Certificate Signing Request (CSR)* on page 52.

4   Import of Certificate Including Private Key (PKCS #12 file), see *Import of Certificate Including Private Key (PKCS #12 file)* on page 53

The following table describes the different functions.

Field name	Description
Subject	Click the hyperlink (under the Subject header) to display certificate details in a window.
PEM	Click the PEM hyperlink (under the Download header) to download the certificate in PEM format.
DER	Click the DER hyperlink (under the Download header) to download the certificate in DER format.
Trust	Click this button to add the selected certificates to the trust list.
Clear	This button is only displayed if a certificate was installed by the user, before. Click this button to discard the current device certificate and restore the standard certificate.
Create New	The Create New hyperlink is used for two purposes: • *Self-signed Certificates* on page 51 • *Certificate Signing Request (CSR)* on page 52
Upload	Use the Upload function to upload a certificate file to the device. 1 Click the Browse button 2 Select a certificate file 3 Click the Upload button to upload the file to the device. NOTE: The Upload function requires a previously issued CSR to exist.

Default Device Certificate

This section corresponds to option 1 in *2. Certificate Handling Options with Device Certificates* on page 13.

If the default device certificate is missing for the device it will be generated, together with a key pair, when the IPBS is upgraded to version R3. The default certificate contains the MAC address of the device and will be valid for 10 years.

If the self-signed certificate is deleted and the device is restarted, a new certificate and key pair will be generated.

HTTPS is deactivated during the generation (creation) of the certificate.

The default certificate is a self-signed certificate. This means that certificates cannot be verified and thus the user/administrator will be prompted by the web browser to accept the certificate before it can be used. From this point on within the browser session (as long as the certificate is not changed) communication between the browser and the device is possible without further accept operations from the user/administrator.

If the device certificate is replaced or regenerated the user/administrator has to manually accept the new certificate.

Self-signed Certificates

This section corresponds to option 2 in 2.2.2 *TLS Certificates* on page 12.

1	Select **Configuration** > **General** > **Certificates**.

2	Click the **Create New** hyperlink in the **Device Certificate** section. A **New Certificate** window opens.

3	Select **Self-signed** certificate in the **Type** drop-down list.

4	Select/Enter the following settings:

Field name	Description
Key	Select either the desired key strength (1024-bit, 2048-bit, 4096-bit) or select to reuse the old key pair (this is not recommended).
Signature	Select which signature that shall be used for the certificate. Following signatures can be selected: SHA1, SHA256, SHA384, SHA512. The last three ones are SHA2 variants.
Validity	Enter the default validity in years. This is a mandatory field.
Common Name	Enter the domain name or IP address for the device. This is the same value as entered in the web browser when accessing the device.

| | DNS Name | If the device has got a DNS name it should be entered here. It will be stored as a subjectAltName (SAN) in the certificate. The format of this field is a FQDN (e.g. host.domain.com). |

5   Click "OK".

6   A new key pair and a certificate will be created. This may take up to one hour depending on the key strength selected. During this time the device will be fully operational with the exception of https not working and the certificate tab pane not being visible.

Certificate Signing Request (CSR)

This section corresponds to option 3A & 3B in 2.2.2 *TLS Certificates* on page 12. This will be the most common options for IP-DECT systems. For more information on CSRs see *Certificate Authorities* on page 11.

1   Select Configuration > General > Certificates.

2   Click the "Create New" hyperlink in the Device Certificate section. A New Certificate window will open.

3   Select "Signing Request" in the Type drop-down list.

4   Select/Enter the following settings:

Field name	Description
Key	Select the desired key strength (1024-bit, 2048-bit, 4096-bit) or select to reuse the old key pair (this is not recommended).
Signature	Select which signature that shall be used for the certificate. Following signatures can be selected: SHA1, SHA256, SHA384, SHA512. The last three ones are SHA2 variants.
Validity	This is an read-only information field indicating a default mandatory validity of 1 year. The time length of the validity is defined by the CA.
Common Name	Enter the domain name or IP address for the device. This is the same value as entered in the web browser when accessing the device.
DNS Name	If the device has got a DNS name it should be entered here. It will be stored as a subjectAltName (SAN) in the certificate. The format of this field is a FQDN (e.g. host.domain.com).

5   Click **OK**. The windows closes.

A key pair and a CSR file will be created. This may take up to one hour depending on the key strength selected. During this time the device will be fully operational with the exception of https not working and the certificate tab pane not being visible.

When the CSR file has been generated it is visible in the Signing Request section of the Certificates page.

6   Download the CSR file by clicking the "PEM" or "DER" link in the Signing Request section.

7   Send the CSR file to your CA.

8   If successful your CA will send back a digitally signed certificate file. This file should now be uploaded.

9   Select the certificate file.

10   Click **Upload**.

Note: If the CSR file generated in step 5 is deleted before receiving the reply from the CA (in step 8) it will not be possible to upload the signed certificate file in step 10. The system will automatically delete the CSR file when step 10 has completed.

Import of Certificate Including Private Key (PKCS #12 file)

This section corresponds to option 4 in 2.2.2 TLS Certificates on page 6.

1   Select **Configuration** > **General** > **Certificates**.

2   In the Device Certificate section, click **Browse** to locate the PKCS #12 file. If the file is password protected, enter a password in the **Password** field.

3   Click **Upload**.

4.2 LAN

This section describes how to do the following configurations and settings in the IPBS:

- Set DHCP mode
- Set IP static address
- Set dynamic IP address
- Set link type
- Configure VLAN
- Set 802.1X
- View LAN statistics
- Disable LLDP

The IP-DECT system supports dual-stack, so both IPv4 and IPv6 addresses can be used simultaneously

Some of the above configurations and settings plus additional ones can be set by a DHCP server via DHCP options. For more information about DHCP options, see Appendix I: *Configure DHCP Options* on page 166.

4.2.1 SET DHCP MODE FOR IPV4

The IPBS can have different DHCP modes for IPv4, see the table below.

Disabled	Used if the IPBS should have a static IP address.
Client	The IPBS acts as a DHCP Client, if there is a DHCP server in the network it will be assigned an IP address
Automatic	In automatic DHCP mode the IPBS will act as a DHCP client on power up. If the IPBS is restarted by shortly pressing the reset button it will get the IP address 192.168.0.1 and the netmask 255.255.255.0 for the LAN1 port.

Change DCHP mode following the steps below.

1   Select **LAN** > **DHCP4.**

2   Select **DCHP mode** in the **Mode** drop-down list.

3   Click **OK**.

4   If "Client" or "Automatic" is set, reset to make the changes take effect. See

4.2.2 SET A STATIC IPV4 ADDRESS

It is necessary for the Master and the Standby Master to have static IP addresses. The Radios can have dynamic IP4 addresses retrieved from the network DHCP server.

Ask the network administrator to reserve an IPv4 address for the Master and Standby Master.

1   On the IPBS: Select **LAN** > **DHCP4**.

2   Select **Disabled** in the Mode drop-down list.

3   Click **OK**.

4   Do NOT reset the device yet. Set a static IP address first.

5   On the IBPS: Select **LAN** > **IPv4.**

6   Enter "IP Address", "Network Mask", "Default Gateway" and "DNS Server" addresses provided by the network administrator in the text fields.

       You can also enter an alternative DNS Server in the Alt. DNS Server text field and select the Check ARP check box to detect and prevent ARP poisoning attacks.

       You can also configure an alternative gateway under Static IP Routes if a specific IP address should use another gateway instead of the default one.

7   Click **OK**.

8   Reset in order to make the changes take effect, see

9   Start the web-based configuration, using the static IP address.

4.2.3 DYNAMIC IPV4 ADDRESS VIA DHCP

The Radios can have dynamic IPv4 address allocation if the network has an DHCP server.

1   On the IBPS: Select **LAN** > **DHCP4**.

2   Select **Client** in the Mode drop-down list.

3   Select **Selected Server only** if the device should accept a lease only from a selected DHCP server.

4   Enter the number of seconds the device waits for a lease from the selected DHCP server before accepting a lease from another server in the **Wait for selected Server** field.

5   If several DHCP servers are available, enter the object identifier (DHCP vendor option 250 value) of the selected DHCP server in the **Server Identifier** field. For example, 1.3.6.1.4.1.27614.1.1.

6   The device sends a default hostname to the server. Enter an alternative hostname in the **Hostname** field to change the default name. Up to 63 alphanumeric characters are allowed.

7   Click **OK**.

8   Reset in order to make the changes take effect, see 4.28 *Reset* on page 125.

Note: If the DHCP lease time is shorter than the time-to-live of the name/IP address association in the Windows Internet Name Service (WINS) server, it may cause a mismatch, and a wrong device may be reached if its WINS name is used.

4.2.4   SET DHCP MODE FOR IPV6

The device can have different DHCP modes for IPv6, see the table below.

Diabled	Used if the device should have a static IP address
Inform	The device can receive DHCP options, but it will use its automatically assigned IP addresses.
Client	The device acts as a DHCP client. If there is a DHCP server in the network, it will be assigned an IP address.

Change DCHP mode following the steps below.

1   Select **LAN** > **DHCP6.**

2   Select **DCHP mode** in the Mode drop-down list.

3   Click **OK**.

4   If **Client** is set, reset to make the changes take effect. See 4.28 *Reset* on page 125.

4.2.5   DYNAMIC IPV6 ADDRESS VIA DHCP

The Radios can have dynamic IPv6 address allocation if the network has an DHCPv6 server.

1   Select **LAN** > **DHCP6.**

2   Select **Client** in the Mode drop-down list.

3   Select **Selected Server only** if the device should accept a lease only from a selected DHCP server.

4   Enter the number of seconds the device waits for a lease from the selected DHCP server before accepting a lease from another server in the **Wait for selected Server** field.

5   If several DHCP servers are available, enter the object identifier (DHCP vendor option 250 value) of the selected DHCP server in the **Server Identifier** field. For example, 1.3.6.1.4.1.27614.1.1.

6   The device sends a default hostname to the server. Enter an alternative hostname in the **Hostname** field to change the default name. Up to 63 alphanumeric characters are allowed.

7   Click **OK**.

8   Reset in order to make the changes take effect, see 4.28 *Reset* on page 125.

4.2.6 SET AN AUTOMATIC IPV6 ADDRESS

The IPv6 protocol supports stateless address autoconfiguration. It means that the device gets a link-local IPv6 address and a default gateway automatically. For IPv6 configuration, automatic address assignment is the default setting.

To view the assigned IPv6 address:

1   Select **LAN** > **IPv6**.

2   The address is shown under **Addresses**.

You can also configure an alternative gateway under Static IP Routes if a specific IP address should use another gateway instead of the default one.

4.2.7 SET A STATIC IPV6 ADDRESS

It is necessary for the Master and the Standby Master to have static IP addresses. The Radios can have dynamic IP addresses retrieved from the network DHCP server.

Ask the network administrator to reserve an IPv6 address for the Master and Standby Master.

1   Select **LAN** > **DHCP6**.

2   Select **Disabled** in the Mode drop-down list.

3   Click **OK**.

4   Do NOT reset the device yet. Set a static IP address first.

5   Select **LAN** > **IPv6**.

6   Select **Static** in the Mode drop-down list.

7   Enter the **IP Address**, **Prefix** and **Default Gateway** addresses provided by the network administrator in the text fields.

You can also configure an alternative gateway under Static IP Routes if a specific IP address should use another gateway instead of the default one.

8   Click **OK**.

9   Reset in order to make the changes take effect, see 4.28 *Reset* on page 125.

10   Start the web-based configuration, using the static IP address.

4.2.8 LINK

1   On the IBPS: Select **LAN** >**Link**.

The link setting should be set to "auto" under all normal circumstances.

4.2.9 CONFIGURE VLAN

Identity and priority settings for VLAN are done in the "LAN > VLAN" sub menu.

Note: It is necessary to have a VLAN with the same ID as configured in the IPBS, otherwise it will not be possible to access the IPBS.

Note: If "VLAN = 0", the Quality of Service (QoS) is inactive according to 802.1q. It is also recommended to avoid "VLAN = 1" as it often is used as a default VLAN setting.

4.2.10 SET 802.1X

The 802.1X standard is used for authentication when connecting to the LAN. EAP-MD5 and EAP-TLS are supported. The EAP-MD5 fields must be filled out even if EAP-TLS is used.

If EAP-TLS is used, a certificate must be available at **General** > **Certificates** > **Device Certificate**.

1   Select **LAN** > **802.1X**

2   Enter the user name for the authentication in the **User text** field.

3   Enter the corresponding password for EAP-MD5 or an arbitrary text for EAP-TLS in the **Password text** field.

4   Click **OK**.

4.2.11 VIEW LAN STATISTICS

To view statistics of LAN events:

1   On the IBPS: Select **LAN** > **Statistics**.

To reset the Ethernet statistics counters, click **Clear**.

4.2.12 DISABLE LLDP

LLDP (Link Layer Discovery Protocol) is a vendor-neutral link layer protocol used by network devices for advertising their identity, capabilities, and neighbours on an IEEE 802 local area network.

LLDP is enabled by default and can be disabled in order to prevent the IP-DECT device to get VLAN settings through the LLDP protcol. To disable LLPD, do as follows:

1   Select **LAN** > **LLDP**.

2   Select the **Disable** check box.

3   Click **OK**.

4.3 IPV4

4.3.1 CONFIGURE IPV4 SETTINGS

The following settings can be done in the IPv4 settings sub menu:

ToS priority, RTP Data and VoIP Signaling:	Determines the priority from the ToS field in the IP header. This function can be used if the router can use ToS priority control. Hexadecimal, octal or decimal values can be used; 0x10, 020 and 16 are all equivalent. There are two fields for ToS priority, one for RTP Data and one for VoIP Signaling[a]. Other types of traffic (for example http and ldap) are not prioritized and use 0x00. **Note:** Remember that the same value should be set in the ToS field for all devices.
RTP ports:	If the ports fields are left blank, the ports 16384 to 65535 will be used.

    a. VoIP Signaling includes roaming, handover, registrations towards the IP-PBX etc.

Note: These settings are also valid for IPv6.

1   Select **IPv4** > **Settings**.

2   Enter the ToS priority value (recommended value is "0xb8") in the **ToS Priority - RTP Data text** field.

3   Enter the ToS priority value (recommended value is "0x68") in the **ToS Priority - VoIP Signaling text** field.

4   Select which ports to use for RTP traffic by entering the first port in the **First UDP-RTP Port text** field.

5   Enter the number of ports to use in the **Number of Ports text** field.

6   Click **OK**.

4.3.2 ROUTING

View the IPv4 routing by **Select IPv4** > **Routing**.

4.3.3 TLS

The following TLS versions are supported:

- TLS 1.0
- TLS 1.1
- TLS 1.2

The following TLS versions and cipher suits can be configured:

Normal	Enables all supported versions and ciphers. Most recent versions and most secure ciphers have priority.
Fast	Enables all supported versions and ciphers. The fastest ciphers have priority, but they provide less security.
Highest security	Only the most recent supported TLS version and secure ciphers are enabled. This setting might cause compatibility issues.

To set the TLS profile, do the following:

1   Select **IPv4** > **TLS**.

2   Select the TLS profile in the **Profile** drop-down list.

3   Click **OK**

4.3.4   STUN

The ICE (Interactive Connectivity Establishment) protocol can use STUN or TURN servers for NAT traversal of media. NAT traversal allows data traffic to get to a specified destination when a device does not have a public IP address.

The following settings are available for NAT traversal:

Field Name	Description
STUN Servers	Defines the STUN server to use for NAT traversal. Up to two STUN servers can be configured. The STUN server addresses to the different servers should be separated by a semi-colon (;). The server address must be entered in one of the following formats: • a single DNS name (a domain or a fully qualified domain name (FQDN)) and an optional port (for example, stun.example.com:1234) When a domain is used, a DNS SRV lookup is made to discover up to two STUN servers. • an IP address and an optional port. If an IP address is used, an alternative address can be specified for each server, separated by a comma (for example, 172.16.13.1:1234, 172.16.13.2)

Field Name	Description
TURN Server	Defines the TURN server to use for NAT traversal. One TURN server can be configured and the server address must be entered in one of the following formats:
	• a single DNS name (a domain or a fully qualified domain name (FQDN)) and an optional port (for example, turn.example.com:1234)
	• an IP address and an optional port. If an IP address is used, an alternative address can be specified, separated by a comma (for example, 172.16.13.1:1234, 172.16.13.2)
	A TURN server configuration can optionally be followed by a protocol specification such as "turn.example.com?protocol=prot" where prot can be either tcp or udp.
TURN User Name	Defines the user name for accessing the TURN server.
TURN Password	Defines the password for accessing the TURN server.
Slow STUN/TURN Server	If the turnaround time to the STUN/TURN server is long, extra time can be given before timeout.
NAT Detection Interval	Specifies in minutes how often the NAT detection procedure is initiated.

To configure NAT traversal, do the following:

1   Select **IPv4** > **STUN**.

2   Enter the **STUN** or **TURN** server information.

3   Click **OK**.

4.4 IPV6

4.4.1 ROUTING

View the IPv6 routing by **Select IPv6** > **Routing**.

4.4.2 TLS

The following TLS versions are supported:

• TLS 1.0
• TLS 1.1
• TLS 1.2

The following TLS versions and cipher suits can be configured:

Normal	Enables all supported versions and ciphers. Most recent versions and most secure ciphers have priority.
Fast	Enables all supported versions and ciphers. The fastest ciphers have priority, but they provide less security.
Highest security	Only the most recent supported TLS version and secure ciphers are enabled. This setting might cause compatibility issues.

To set the TLS profile, do the following:

1   Select **IPv6** > **TLS**.

2   Select the TLS profile in the **Profile** drop-down list.

3   Click **OK**

4.5 LDAP

The Lightweight Directory Access Protocol (LDAP) protocol is required for systems in which the server and a replicating client access a joint user database. All IPBSs in the system have access to the database, one of the IPBSs can be configured to be the LDAP server.

The joint user database contains information about the users registered in the system. It also contains the system configuration, that is the configurations made under the DECT menu.

This section describes how to do the following configurations and settings.

• Configure LDAP Server
• Check LDAP Server Status
• Configure LDAP Replicator
• Check LDAP Replicator Status

4.5.1 CONFIGURE LDAP SERVER

The IP-DECT system needs an LDAP server in some configurations. If the VoIP gateway is set up as an LDAP server, the Master should be set up as an LDAP replicator, see 4.5.3 *Configure LDAP Replicator* on page 62.

Setup the IPBS as an LDAP server

Note: The selected user name and password must be the same in both the Master and the Standby Master. If a Multi Master system is used, the Masters must also have the same user name and password.

1   Select **LDAP** > **Server**.

2   Add a user, for example ldap-user, in the User text field.

3   Enter a password in the **Password** text field.

4   Select the **Write Access** check box.

5   Click **OK**.

4.5.2   CHECK LDAP SERVER STATUS

Select **LDAP** > **Server Status**

The following information is displayed:

- connections - Total number of active connections to the LDAP server
- write connections - Number of write-enabled connections
- rx search - Number of received search requests
- rx modify - Number of received change requests
- rx add - Number of added objects
- rx del - Number of deleted objects
- rx abandon - Number of lost connections
- tx notify - Number of sent change notifications
- tx error - Number of sent error notifications
- tx error 49 - Number of sent error notifications due to invalid credentials
- tx error 50 - Number of sent error notifications due to insufficient access rights

4.5.3   CONFIGURE LDAP REPLICATOR

LDAP Replicators are usually configured in the following cases:

- User data is replicated from the Master to the Standby Master. The replicator is configured on the Standby Master (Full Directory Replication)
- User data is replicated from the Active Directory (AD) to the Master. The replicator is configured on the Master
- User data is replicated from the PBX to the Master. The replicator is configured on the Master (Full Directory Replication)

Configure Full Directory Replication

1   Select **LDAP** > **Replicator.**

2   Select **Full Replication** in the **Type** drop-down list.

3   Select the **Enable** check box.

4   Enter the IP address to the LDAP server in the **Server** text field.

5   Enter the IP address to the alternative LDAP server in the **Alt. Server** text field.

6   NOTE: If this IPBS is configured as an alternative/standby LDAP server, leave the Alt. Server text field empty. Select a filter method from the Filter Type drop-down list

- Dect Gateway Name - Enter the name of the DECT gateway to limit the replication to users of a certain group
- LDAP Filter - Enter an LDAP filter to limit replication to certain LDAP objects

7   Enter the LDAP User name and Password in the **User** and **Password** text fields.

8   Click **OK**.

Note: In the case of Master to Standby Master Full Directory Replication, do not register new handsets when the LDAP Server is down even if there is a Standby LDAP Server in the system.

Configure Active Directory Replication

During Active Directory (AD) replication the configured LDAP replicator retrieves only relevant data.

AD replication is a one-way replication where data is only transferred from the AD to the IP-DECT but not from the IP-DECT to the AD. Data originating from the AD cannot be modified in the IP-DECT system, but it is possible to change or add those user attributes locally that are not replicated.

Note: If AD replication is enabled, existing local users are replaced with corresponding users in the AD, and some local attributes may be deleted. Contact Technical Support if you would like to enable AD replication with existing local users.

For AD Server configuration settings, see *Configure AD Server* on page 66.

1   Select **LDAP** > **Replicator.**

2   Select **Active Directory Replication** in the **Type** drop-down list.

3   Select the **Enable** check box.

4   Enter the IP address to the AD in the **Server** text field.

5   Enter a Distinguished Name (DN) to configure a search base for AD users.

The user information is usually replicated so It is recommended to write "CN=Users, DC=DomainName" where "DomainName" is the name of the domain on the AD server.

You can also click **Show Options...** to see some naming contexts on the configured server.

6   Enter an LDAP filter to retrieve only the relevant LDAP objects from the AD.

A default (objectclass=user) filter is offered, but it is recommended to assign all IP-DECT users to a group within the AD. For example, the following filter can be entered to retrieve only IP-DECT users.

"(&(objectClass=user)(memberOf=CN=grp_ipdect,CN=Users,DC=DomainName))"

where "grp_ipdect" is the group created for IP-DECT users, "Users" is the default folder for users and "DomainName" is the name of the domain on the AD server.

7   Enter the user name and the password of a user who has read access to the AD in the **User** and the **Password** text fields. It is recommended to choose a user with Enterprise Administrator rights.

8   Configure In Maps and Out Maps for Attribute mapping. Attribute mapping describes how the obtained information from the AD is handled within the IP-DECT system. For more information see *Attribute Mappings* on page 64.

9   Click **OK**.

10   After proper configuration check the Replicator Status by selecting **LDAP** > **Replicator Status**. The state of the Active Directory Replication should be **Up** and the state of the remote directory should be **Completed**.

Attribute Mappings

The following attributes are generally used to configure attribute mappings:

IP-DECT designator	IP-DECT attribute name	AD attribute name	Description
Long Name	cn	cn	Mandatory, the name of the user, need to be unique throughout the system.
Display Name Idle Display	dn	displayName, givenName, sn	Display Name: Is not used in Mitel system. Idle Display: Optional, will be shown in the handset display (Not used with Mitel call servers).
Name	h323	userPrincipalName	User name

Number	e164	telephoneNumber, ipPhone, mobile	Business or mobile phone number, mandatory and must be unique
Auth. Name (SIP)	auth		Auth name is the Authentication name used in SIP authentication. If it is not set the number will be used as authentication name. If SIP authentication is used or not is decided by the configuration in the IP-PBX.
Password	password		Optional, is used for registration towards the gatekeeper.
IPEI / IPDI	ipei		The unique identification number of the handset.
Auth. Code	authCode		Optional, the individual authentication code for this user. Automatically created by default. Can be modified manually.

Note: If IPEI is replicated shared phone does not work, i.e. login/logout is blocked. If password is replicated it is stored as clear text in config.

In Maps

In Maps define which attributes of the incoming objects are replicated and how the attributes are used in the IP-DECT system. In Maps can be configured with the following text fields:

- Source Attribute - The name of the AD attribute to be replicated. Only those users are replicated who have the defined source attributes. See *AD attribute name* on page 64 for examples.
- Assignment Pattern - A regular expression that assigns AD attributes to local temporary variables. A local temporary variable can have any name starting with a % sign, for example %tel. Regular expressions are written in a formal language that is widely used in Unix environments. For more information, see regular expression manuals on the internet.
- Description - Short explanation of what is configured with regular expressions

If there are several in maps for one attribute, all maps are handled in the order of appearance. To change the order of appearance click the "Move Up" or "Move Down" icons on the left side of the In Maps window.

Out Maps

Out Maps define how the local temporary variables configured for In Maps are assigned to the internal IP-DECT attributes. Out Maps can be configured with the following text fields:

- Dest. Attribute - The name of the IP-DECT attribute. See *IP-DECT attribute name* on page 64 for examples.
- Destination Value - The name of the local temporary variable.

Example

In the example above regular expressions are used to remove non-numerical characters from the phone number (second line of In Maps). The third line of In Maps defines a local temporary variable (dsp) which stores all numbers starting with 031 with "Gbg" added before them. This is shown in the Display attribute as assigned in the Out Maps.

It is recommended to configure a default value for some attributes to avoid the retention of old information in the IP-DECT database. In the example below the display attribute is assigned an empty string if that attribute is not defined in the AD. The Source Attribute in the third line of In Maps is cn because it should be an attribute that is always present in the AD.

Example

Configure AD Server

The IP-DECT system supports only simple binding authentication. However, the default registry setting for Microsoft Active Directory 2003 does not allow simple binds, so it may be necessary to change Windows Registry settings to use AD replication.

1 In Windows, select **Run...** in the **Start** menu.

2 Enter **regedit** and click **OK** to start the Windows Registry Editor.

3 In the Editor navigate to the "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Param eters\ LDAPServerIntegrity" key.

4 Click on the key with the right mouse button and click **Modify**.

5 Change the key value of 2 to the value of 1.

6 Click **OK**.

4.5.4 CHECK LDAP REPLICATOR STATUS

1 Select **LDAP** > **Replicator-Status**.

The following information is displayed:

- Server - The IP address and port of the LDAP server.
- Active Directory Replication - Current state of replication. Four states are possible: Stopped, Starting, Up, Down
- Remote - State of replication in the source directory. Three states are possible: Stopped, Active, Completed
- Notify - Number of change notifications received from the server
- Paged - Number of objects received from AD server in response to paged search requests
- No match - Number of objects received that are not matching the configured LDAP filter condition
- Discarded - Number of objects discarded because no suitable map is found
- Local - State of replication in the destination directory. Three states are possible: Stopped, Active, Completed
- Notify - Number of change notifications sent to the server
- Add - Number of locally added objects
- Del - Number of locally deleted objects
- Modify - Number of locally modified objects
- Pending - Number of local objects waiting to be sent to the server

4.5.5 EXPERT TOOL

The Expert function should only be used after consultation with Technical Support.

4.6 DECT

This section describes how to do the following configurations and settings.

- Change System Name and password
- Set Subscription Method
- Configure Authentication Code
- Select Tones
- Set Default Language
- Set Frequency Band
- Enable/Disable Carriers
- Enable/Disable Local R-Key Handling
- Enable/Disable No Transfer on Hangup
- Enable/Disable No On-Hold Display

- Enable/Disable Display Original Called
- Disable ICE Support
- Wideband Audio
- Enable/Disable Early Encryption
- Configure Coder
- Secure RTP
- Configure Supplementary Services
- Select Master Mode
- Set Master Id
- Enable PARI Function
- Set Region Code
- Configure Gatekeeper
- Registration for Anonymous Devices
- Conferencing Unit
- Select Crypto Master mode
- Select Mobility Master mode
- Connect Mobility Master to other Mobility Master(s)
- Disconnect Mobility Master to other Mobility Master(s)
- Connect Mobility Master to a Crypto Master
- Connect Master to a Mobility Master
- Enable/Disable Radio
- Enter IP address to the PARI Master and the Standby PARI Master
- Multiple Radio Configuration
- Assign PARI
- Enter SARI
- Configure Air Synchronization

4.6.1 CHANGE SYSTEM NAME AND PASSWORD

Note: This is only applicable for a Master, never on a Slave.

The system name and password must be the same for all IPBS throughout the system. Reset in order to make the changes take effect, see 4.28 *Reset* on page 125.

1   Select DECT > System.

Note: To access the System tab, the Master mode has to be activated, see 4.6.19 *Select Master Mode* on page 77.

2   Write a system name in the **System Name** text field.

3   Enter a new password in the **Password** text field. Repeat the password.

4   Click **OK**.

Note: It is recommended to create a backup of the IPBS configuration when the password has been changed, see 4.14 *Backup* on page 120.

4.6.2 SET SUBSCRIPTION METHOD

The IP-DECT system can be set to use the following subscription methods:

- With User AC - Individual Registration and Auto Registration is possible.

- With System AC - Anonymous Registration and Individual Registration is possible.
- Disable - Registration is not possible.

Select subscription method:

1   Select DECT > System.

   Note: To access the System tab, the Master mode has to be activated, see 4.6.19 *Select Master Mode* on page 77.

2   Select subscription method in the Subscriptions drop-down list.

3   Click **OK**.

Note: When"With System AC" is enabled anyone could register to the IP-DECT System.

4.6.3   CONFIGURE AUTHENTICATION CODE

If "allow anonymous subscription" method is selected it is needed for the IP-DECT system to have an authentication code configured. The authentication code is generated automatically but can be modified manually by selecting a code consisting of 4 to 8 numbers (0-9).

1   Select DECT > System.

   Note: To access the System tab, the Master mode has to be activated, see 4.6.19 *Select Master Mode* on page 77.

2   Enter an authentication code in the Authentication Code text field.

3   Click **OK**.

4.6.4   SELECT TONES

1   Select **DECT** > **System**.

   NOTE: To access the System tab, the Master mode has to be activated, see 4.6.19 *Select Master Mode* on page 77.

2   Choose tones in the **Tones** drop-down list.

3   Click **OK**.

4.6.5   SET DEFAULT LANGUAGE

If the handset does not send language information to the system, this setting determine which language that is displayed for some text messages (for example hung-up and disconnected).

1   Select **DECT** > **System**.

   Note: To access the System tab, the Master mode has to be activated, see 4.6.19 *Select Master Mode* on page 77.

2   Choose language in the **Default Language** drop-down list.

3   Click **OK**.

4.6.6   SET FREQUENCY BAND

The IPBS can operate in the following frequency bands:

- 1880 - 1900 MHz, Europe, Africa, Middle East, Australia, New Zealand and parts of Asia
- 1900–1906 MHz (Thailand)
- 1910-1930 MHz, South America
- 1920-1930 MHz, North America

1 Select **DECT** > **System**.

   NOTE: To access the System tab, the Master mode has to be activated, see 4.6.19 *Select Master Mode* on page 77.

2 Select frequency area in the Frequency drop-down list.

3 Click **OK**.

Note: All calls will be disconnected and all handsets will temporarily lose contact with the system.

4.6.7 ENABLE/DISABLE CARRIERS

The device has 5 carriers for the North American frequency band, 4 carriers for the Thai frequency band and 10 carriers for the other frequency bands. Under all normal circumstances all carriers should be enabled.

To enable or disable carriers:

1 Select **DECT** > **System**.

   NOTE: To access the System tab, the Master mode has to be activated, see 4.6.19 *Select Master Mode* on page 77.

2 Select/clear the **Enabled Carriers** check boxes.

   Note: For Brazil, the following carriers shall be selected only: 18, 19, 20 and 21.

3 Click **OK**.

4.6.8 ENABLE/DISABLE LOCAL R-KEY HANDLING

With this option enabled keypad information is handled locally. If this option is disabled keypad information is sent transparently to the IP-PBX. Local R-key handling is further described in *Appendix B*.

1 Select **DECT** > **System**.

   NOTE: To access the System tab, the Master mode has to be activated, see 4.6.19 *Select Master Mode* on page 77.

2 To enable, select the **Local R-Key Handling** check box.

   NOTE: To access the Local R-Key Handling check box, the SIP protocol has to be selected on the Master, see 4.6.23 *Configure Gatekeeper* on page 79.

3 Click **OK**.

4.6.9 ENABLE/DISABLE NO TRANSFER ON HANGUP

If enabled it will not be possible to do a transfer by hanging up the handset. R4 must be pressed (see *Appendix B*).

1   Select **DECT** > **System**.

NOTE: To access the System tab, the Master mode has to be activated, see .

2   To enable, select the **No Transfer on Hangup** check box.

3   Click **OK**.

4.6.10 ENABLE/DISABLE NO ON-HOLD DISPLAY

If enabled, no On-Hold indication will be displayed in the handsets.

When one party in a call put the other party on-hold, the existing information in the other party's handset display will be replaced with an on-hold message. To prevent this the "No On-Hold Display" option must be enabled. Do as follows:

1   Select **DECT** > **System**.

NOTE: To access the System tab, the Master mode has to be activated, see .

2   To enable, select the **No On-Hold Display** check box.

3   Click **OK**.

4.6.11 ENABLE/DISABLE DISPLAY ORIGINAL CALLED

If enabled, the original called party, instead of the diverted party, is shown to the called party if the call is diverted.

Example: Handset B is diverted to handset C which in turn is diverted to handset D. When handset A is calling handset B the following extension number or name will be shown in handset D's display depending on if the feature "Display Original Called" is enabled or not.

- Display Original Called is **enabled**: The extension number or name of handset B will be shown in handset D.
- Display Original Called is **not enabled**: The extension number or name of handset C will be shown in handset D.

Note: In both cases the extension number or name of handset A will be shown as well.

To enable Original Called Display, do as follows:

1   Select **DECT** > **System**.

NOTE: To access the System tab, the Master mode has to be activated, see .

2   To enable, select the **Display Original Called** check box.

3   Click **OK**.

4.6.12 ENABLE/DISABLE EARLY ENCRYPTION

With this option enabled the early encryption feature will be activated in the IP-DECT system.

Note: Activating early encryption will cause a restart of all RFPs.

Note: For the early encryption feature to function in the system, the DECT handset must also support early encryption.

Note: Handsets already registered will continue to function without early encryption.

Note: Only the handsets registered after enabling the early encryption feature will have support for this feature.

For more information on early encryption, see about Enhanced DECT Security in the System Description documentation for IP-DECT.

1   Select **DECT** > **System**.

NOTE: To access the System tab, the Master mode has to be activated, see 4.6.19 *Select Master Mode* on page 77.

2   To enable, select the **Early Encryption** check box.

Note: To access the Early Encryption check box, the Pari Master mode has to be activated, see 4.6.21 *Enable PARI Function* on page 78.

3   Click **OK**.

4   In a system with several PARI Masters, it is recommended to repeat step 1 to 3 for all PARI Master.

Note: It is possible to have a system with different Pari domains where early encryption is enabled in some and disabled in other. However, all IPBSs must have software support for early encryption even though it is not enabled.

5   To enable the early encryption feature in a system with Mobility Master(s), connect the Mobility Master(s) to a Crypto Master, see 4.6.29 *Connect Mobility Master to a Crypto Master* on page 84.

6   To view a list of DECT handsets where early encryption is in use: Select Users > Users and then click **Show**. Those DECT handsets where early encryption is in use is indicated with a dot in the column EE (Early Encryption).

4.6.13 ENABLE/DISABLE RFP LOCATION

Note: Activating RFP Location will cause a restart of all RFPs.

With this option enabled the RFP Location feature will be activated in the IP-DECT system. This will however increase the load on the system and should only be enabled when the location information is required by an external application. For information on developing applications based on RFP location, contact the support about how to use the XML API.

The Masters in a distributed IP-DECT system keeps track of where handsets are located to be able to know where to reach the handset with different kinds of messages, like phone calls and messaging.

To enable RFP Location, do as follows:

1   Select **DECT** > **System**.

NOTE: To access the System tab, the Master mode has to be activated, see 4.5.19 Select Master Mode on page 67.

2   To enable, select the **RFP Location** check box.

Note: To access the RFP Location check box, the Pari Master mode has to be activated, see 4.5.21 Enable PARI Function on page 68.

3   Click **OK**.

4.6.14 DISABLE ICE SUPPORT

ICE (Interactive Connectivity Establishment) is a protocol for finding and selecting a working network path between two media endpoints. The basic idea is that each endpoint discovers all its addresses that could be used to receive media. Those candidates are sent to the other endpoint. Then all combinations of local and remote candidates are tested. The best working combination is used for the actual media stream. If there is no working combination, the call will be disconnected.

ICE is default enabled. To be sure to not run into interoperability problems during media negotiation, ICE can be disabled, as follows:

1   Select **DECT** > **System**.

2   To disable, select the **Disable ICE** check box.

3   Click **OK**.

4.6.15 WIDEBAND AUDIO

Note: Wideband Audio media is supported by IPBS2/IPBS4x2 only (software version 9.1.X or later). The support for Wideband Audio is also dependent on what model of handset that is used and the type of PBX, presently supported on MX-ONE, that is used in the system and if handsets from other manufacturers supports the same wideband coder. For more information, see the data sheet for the handset.

Wideband audio is high definition voice quality for telephony audio. It extends the frequency range of audio signals, resulting in higher quality speech. For more information about wideband audio, see the System Description for IP-DECT.

To enable wideband audio, do as follows:

1   In the PARI Master, select **DECT** > **System**.

Note: To access the System tab, the Master mode has to be activated, see 4.5.19 Select Master Mode on page 67.

2   In the Coder drop-down list, choose either the G722.2/G711A or G722.2/G711u coder. Depending on the support for wideband audio in the system (see the note text in the beginning of this section), then the G722.2 coder will be offered as the preferred choice which enables wideband audio. Otherwise, the G711A or G711u coder will be preferred instead. If it for some reason is necessary to disable the use of G722.2 coder in the system avoid these two coder options.

3   Enter the sample time in milliseconds in the Frame text field. Note: The sample time will be used only for the G711A or G711u coder.

4   Choose Exclusive enabled or disabled by selecting/clearing the Exclusive check box. The Exclusive check box will be used only for the G711A or G711u coder. If exclusive is selected for the coder the IPBS is forced to use that coder.

Note: When exclusive is enabled for a coder it might be impossible to make calls outside the IP-DECT system.

5   Choose Silence Compression enabled or disabled by selecting/clearing the SC check box. The Exclusive check box will be used only for the G711A or G711u coder. With Silence Compression enabled no information is sent during pauses in the conversation, this is used to save bandwidth.

6   Click **OK**.

4.6.16 CONFIGURE CODER

Select the preferred coder, and enter the desired frame length. If exclusive is selected for the coder the IPBS (Not used with Mitel call servers) is forced to use that coder. With Silence Compression enabled no information is sent during pauses in the conversation, this is used to save bandwidth.

Note: When exclusive is enabled for a coder it might be impossible to make calls outside the IP-DECT system.

1   Select **DECT** > **System**.

Note: To access the System tab, the Master mode has to be activated, see 4.6.19 *Select Master Mode* on page 77.

2   Choose the applicable coder in the Coder drop-down list.

NOTE: The G726-32 coder is not supported by SIP.

3   Enter the sample time in milliseconds in the Frame text field.

4   Choose **Exclusive enabled** or **disabled** by selecting/clearing the **Exclusive** check box.

5   Choose **Silence Compression enabled** or **disabled** by selecting/clearing the **SC** check box.

6   Click **OK**.

4.6.17 SECURE RTP

This option makes it possible to encrypt media streams. The encryption is activated if the SRTP is also enabled in the IP-PBX. For additional privacy it is recommended to use the encrypted signaling protocol (SIPS) as well to hide the exchange of the SRTP keys when this is done through the signaling.

Note: If SRTP is enabled one Radio can handle maximum 5 calls for each IPBS1/ IPBS4x0 and 20 for each IPBS2/IPBS4x2 at the same time. For this reason and because of the high load on the CPU when SRTP is used, it is recommended to deactivate the Radio in the Master.

Two different key exchange methods for SRTP can be selected. SDES is inside the signaling which is encrypted hop-by-hop. DTLS-SRTP is inband and encrypted end-to-end. DTLSSRTP is more secure but adds a small delay to the beginning of phone calls. In the text below here, "DTLS" means "DTLS-SRTP".

1   Select **DECT** > System.

Note: To access the System tab, the Master mode has to be activated, see 4.6.19 *Select Master Mode* on page 77.

2   Select in the Secure RTP Key Exchange drop-down list what key exchange method(s) are offered and what method is selected from received offers, as follows:

SDES-DTLS (Both SDES and DTLS are offered. SDES is selected, if possible)

DTLS-SDES (Both are offered. DTLS is selected, if possible)

SDES (Only SDES is offered. SDES is selected, if possible)

DTLS (Only DTLS is offered. DTLS is selected, if possible)

No encryption (Is set by default. No SRTP is offered. No SRTP is selected)

3   Select in the Secure RTP drop-down list a cryptographic suite. The numbers in the list refer to key-length/sha1 hash-length.

Note: The Secure RTP Cipher drop-down list will not be visible if "No encryption" has been selected in the Secure RTP Key Exchange drop-down list.

4   Click **OK**.

If a call is successfully encrypted a lock icon appears next to the ongoing call description in the Traffic > Master Calls section.

The maximum amount of media streams are as follows depending on if SRTP is enabled or not:

• IPBS1/IPBS4x0: 20 RTP
• IPBS1/IPBS4x0: 5 SRTP
• IPBS2/IPBS4x2: 20 RTP
• IPBS2/IPBS4x2: 20 SRTP

4.6.18 CONFIGURE SUPPLEMENTARY SERVICES

The supplementary services determine how to handle a call if for example busy or not answered by the user.

1   Select **DECT** > **Suppl. Serv**.

NOTE: To access the Suppl. Serv. tab, the Master mode has to be activated, see

2   Select the **Enable Supplementary Services** check box to activate the supplementary services below. The default Activate and Deactivate feature codes are preset.

Explanation of feature code syntax:
$ - Placeholder for user provided digits, e.g. a phone number
$# - Number of digits decided by end indicator #
$(N) – Number of digits decided by N

Example: Default feature code for Logout User is #11*$#

Feature	Description
Call Forwarding Unconditional	Forwards incoming calls to a given number in all cases
Call Forwarding Busy	Forwards incoming calls to a given number if the handset is busy
Call Forwarding No Reply	Forwards incoming calls to a given number if the call is not answered or there is no coverage
Do Not Disturb	Sets the handset in busy mode
Call Waiting	A second incoming call during a call is indicated with a call waiting tone
Call Completion	Notifies the caller when a busy number or no answering user becomes available and re-initiates the call.

Feature	Description
Call Park	Allow users to place a call on hold so it can be retrieved from another phone.
Interception	Allow users to enter absent information in a presence system to inform the calling person why the called person is not available. For information on how to configure an IP-DECT presence system, see 4.8.7 Configure IP-DECT to Connect to a Presence System Using ICP on page 88.
Call Service URI	Not used by Mitel call servers.
Call Service URI (Argument)	Not used by Mitel call servers.
Logout User	Logs out the user and the handset becomes anonymously subscribed.
Clear Local Settings	Clears all locally stored feature settings and all features are deactivated.
MWI Mode	MWI (Message Waiting Indication) enables the receiving of a notification from an IP-PBX when, for example, a voice mail is available for listening. There are four modes that can be selected to enable MWI: Fixed interrogate and fixed notify number User dependent interrogate number User dependent notify number Both numbers users dependent "Fixed" means that a common call number is used for all users. "User dependent" means that the user's own call number is used. **Note:** This option should be selected when the site is configured with resilient MiVoice Business, whether MiVoice Business resiliency is used alone or in conjunction with IP-DECT resiliency. If IP-DECT Resiliency is configured, and MiVoice Business Resiliency is not configured, this option should be deselected. Enable SIP check-box for "IP-PBX Supports Redirection Of Registration When Registered To Alternative Proxy" if site is configured with resilient MiVoice Business and MWI is required.
MWI Interrogate Number	The number used by the handset when it checks with the IP-PBX if there are any message waiting indications to be notified about.
MWI Notify Number	A call number shown in the handset display when receiving a MWI notification. To receive the stored message the user dial the number.

Feature	Description
Local Clear of MWI	If necessary, enter the number of the message center in this field to clear the message waiting indication locally when dialling the number.
External Idle Display	Depending on type of IP-PBX, absence and call forwarding texts will be displayed on the handset when idle. Note: If call forwarding is handled by the IP-PBX, the following options must be disabled: Call Forwarding Unconditional Call Forwarding Busy Call Forwarding No Reply

Note: To disable a specific service, select the Disable check box to the right. Disable services in order to allow the MiVoice call server to control these features. Some exceptions apply to MWI (see note below) and Logout User. Do not disable Logout User.

3   Click **OK**.

4   Reset in order to make the changes take effect, see .

Figure 5. Supplementary services

4.6.19 SELECT MASTER MODE

1   Select **DECT** > **Master**.

Note: The Master can be set to be inactive or active or for redundancy purposes, the Master can be set to act in two other ways: As Standby or Mirror.

2 Select in the *Mode* drop-down list one of the following:

- **Off**, if this IPBS is not a Master.
- **Active,** if this IPBS is the Master.
- **Standby**, if this IPBS is the Standby Master.
- **Deployment** is used for coverage test only. The speech from the handset is looped back to the handset.
- **Mirror**, if this IPBS is the Mirror. For information about Mirror devices, see the system description for IP-DECT.

3 If you have selected the "Standby" mode enter the primary Master IP address in its text field.

4 If you have selected the **Mirror** mode, do the following:

- Configure NTP settings, see 4.1.9 *Configure the NTP Settings* on page 47
- Enter the IP address to the other Mirror Master in the **Mirror Master IP address text** field

For the Master that initially shall be the active Mirror, click on the text link **Activate mirror**. Any user and handset data in the inactive Mirror will be replaced with the user and handset data stored in the active Mirror.

To switch the active role between the Mirror Masters, click on the text link Switch active mirror.

Note: This should be done within a maintenance window as all active calls will be lost.

5 Click **OK**.

6 Reset in order to make the changes take effect, see 4.28 *Reset* on page 125.

4.6.20 SET MASTER ID

1 Select **DECT** > **Master**.

2 Enter a Master id in the **Master Id** field. The id must be unique for each Master in a multiple Master system. The Standby Master must have the same id as the Master.

3 Reset in order to make the changes take effect, see 4.28 *Reset* on page 125.

4.6.21 ENABLE PARI FUNCTION

The PARI Master is responsible for assigning PARIs, being part of the same external handover domain, to the Radios associated. A Radio will always be given the same PARI, based on the PARI-mac-address-association.

1 Select **DECT** > **Master**.

2 If this is the Pari Master or standby Pari Master, select the **Enable Pari function** check box.

Note: Only one Master per handover and sync domain can have the Pari function enabled.

3 Reset in order to make the changes take effect, see 4.28 *Reset* on page 125.

4.6.22 SET REGION CODE

When placing calls from IP-DECT in a multiple site installation, the IP-PBX has no way of knowing in which site the user is located because the call is always sent from that user's Master. Knowing the location becomes especially important for emergency calls.

For more information on region codes, see about *Call Localization* in the System Description documentation for IP-DECT.

1   Select **DECT** > **Master**.

2   Enter a region code in the **Region Code** field. The region code can consist of numbers **0-9**, ***** and **#**.

4.6.23 CONFIGURE GATEKEEPER

Note: Use the following settings for MiVoice Business:

•   Protocol = SIP

•   Proxy = IP address of the MiVoice Business RTC

•   Alt. Proxy = IP Address of the secondary MiVoice Business RTC used for resiliency

•   Enter the Max. Internal Number Length

•   Enable Enbloc Dialing

•   Enable Enbloc Send-Key

•   Enable Allow DTMF Through RTP

•   In the SIP interoperability Settings: Registration Time To Live should reflect the settings in MiVoice Business SIP Capabilities settings, normally 300 seconds

•   Hold Signalling = Send Only

•   Hold Before Transfer is disabled

•   Accept Inbound Calls not Routed through Home Proxy is disabled

•   Register with number is disabled

•   KPML support is disabled

The Master need to know the address to the system gatekeeper.

1   Select **DECT** > **Master.**

2   Select **H.323**, **H.323/TCP**, **H.323/TLS**, **SIP/UDP**, **SIP/TCP** or **SIP/TLS** protocol in the Protocol drop-down list.

If **H.323**, **H.323/TCP**, **H.323/TLS** protocol is selected, continue with step 3 and 4. Otherwise, jump to step 5.

3   Enter the address to the gatekeeper in the Gatekeeper IP address text field.

4   Enter the address to the alternative gatekeeper in the Alt-Gatekeeper IP address text field.

NOTE: As an alternative to the Gatekeeper IP Address, the Gatekeeper ID can be used.

NOTE: Unless you have a fully qualified domain name (FQDN) in your certificate when using SIPS with an alternative gatekeeper, please make sure that the parameter "No Server Certificate Subject Check For TLS Connections" under VOIP/SIP has been set to avoid connection problems with the PBX.

5   **NOTE:** Step 5 to 7 applies to the SIP/UDP, SIP/TCP or SIP/TLS protocols.

Enter the IP address, domain name or host name and optionally port of proxy (e.g. proxy1.example.com:5060) to the SIP proxy (registrar) in the Proxy text field.

6   Depending on how many alternative SIP proxys that are used, do as follows:

In the Alt. Proxy 1 text field: Enter the IP address, domain name or host name and optionally port of proxy (e.g. proxy2.example.com:5060) to the alternative SIP proxy (registrar).

In the Alt. Proxy 2 text field: Enter the IP address or host name and optionally port of proxy (e.g. proxy3.example.com:5060) to the alternative SIP proxy (registrar).
NOTE: The Alt. Proxy 2 text field cannot be used if the Proxy and the Alt. Proxy 1 text fields contain domain names.

In the Alt. Proxy 3 text field: Enter the IP address or host name and optionally port of proxy (e.g. proxy4.example.com:5060) to the alternative SIP proxy (registrar).
NOTE: The Alt. Proxy 3 text field cannot be used if the Proxy and the Alt. Proxy 1 text fields contain domain names.

NOTE: Unless you have a fully qualified domain name (FQDN) in your certificate when using SIPS with an alternative proxy, please make sure that the parameter "No Server Certificate Subject Check For TLS Connections" under VOIP/SIP has been set to avoid connection problems with the PBX.

7   If used, enter the domain address in the **Domain** text field.

8   Enter the maximum internal number length in the Max. internal number length text field.

9   To handle calls of international format: Depending on the type of IP-PBX and handsets that are used in the IP-DECT system, it can be necessary to enter an international CPN prefix in the IPBS. Do as follows:
Enter in the *International CPN Prefix* text field the international CPN prefix for the country in which the IPBS is used.

Following will happen: When the IP-DECT system is receiving a call of international format, the IPBS will convert the plus sign (+) to the international CPN prefix that has been entered in the *International CPN Prefix* text field. The international CPN prefix will be shown in the handset display of the called party and when the called party calls back, the international CPN prefix will be used.

10   To use the system password for registration, select the *Registration with system password* check box.
In a system with many users where the same password shall be used for all users, it is possible to use the system password for registration towards the gatekeeper. About how to set the system password, see 4.6.1 *Change System Name and Password* on page 68.
NOTE: When changing the system password you also need to change the password in all Radios and all other Masters, Pari Masters including standby devices. After this you need to restart all the devices where you made changes (i.e. probably the whole system).

11   To enable "Enbloc Dialing", select the **Enbloc Dialing** check box.

With this option enabled the keystrokes on the handsets are buffered in the IPBS for a short period of time before sent to the IP-PBX (use this when the IP-PBX does not support overlap sending). If disabled the keystrokes are immediately sent to the IP-PBX.

12   To enable "DTMF through RTP Channel", select the **DTMF through RTP channel** check box.

If enabled DTMF is negotiated according to RFC2833/4733, resulting in DTMF digits being sent as RTP payload directly to the other endpoint. If the other party does not support RFC2833/4733, there will be fallback to DTMF over the signaling channel (SIP INFO or H.245)

If disabled, the DTMF is always sent in the signaling channel.

13   To enable "Short disconnect tone", select the **Short disconnect tone** check box.

With this option enabled, a short tone (i.e. busy tone) is received when the other party hangs up. If this option is not enabled, busy tones will be received for a longer period of time.

14   To determine how calls that are rejected by the user should be handled: Select **Busy, Rejected**, or **No user responding** in the **Treat rejected calls as** drop-down list.

15   If you in step 2 selected "SIP" protocol, enable or disable the following options in the SIP Interoperability Settings section:

Registration time-to-live
This is the Expires-header in the REGISTER message. The default is 120 seconds.

To enable this option, enter a value specified in seconds in the **Registration time-to-live** field.

NOTE: Depending on the number of users, the entered value may have to be increased. For example, for 500 users it is recommended to enter 300 seconds and for 1000 users it is recommended to enter 600 seconds. The SIP proxy might respond to the REGISTER with a different value. Then the responded value will be used for REGISTER refresh.

When secondary SIP proxy is in use, for example when the primary SIP proxy is down, the configured time-to-live value is used to decide how often the Master will try to reconnect to the primary SIP proxy.

STUN

If the SIP server is outside the private network and a STUN server is used for NAT traversal, enter the STUN server address in one of the following formats:

•   a DNS name (a domain or a fully qualified domain name (FQDN)) and an optional port (for example, stun.example.com:1234)
When a domain is used, a DNS SRV lookup is made to discover up to two STUN servers.

•   an IP address and an optional port. If an IP address is used, an alternative address can be specified for each server, separated by a comma (for example, 172.16.13.1:1234, 172.16.13.2)

Hold Signaling
Some IP-PBXs require special way of hold signaling. In the "Hold Signaling" list field, select one of the following:
inactive: No media stream is sent or received.
sendonly: Media stream is sent only and not received.
sendonly with 0.0.0.0: Special case of sendonly where also the media IP address is set to 0.0.0.0.

Hold before Transfer
If this option is enabled, the consultation call is put on hold before transfer. Some IP-PBXs require this option so that both called parties are put on hold before the

transfer is carried out.
To enable this option, select the "Hold before Transfer" check box.

Accept Inbound Calls not Routed via Home Proxy

If this option is enabled it could be possible for inbound calls to bypass call restrictions configured in the IP-PBX. If it is disabled a 305 Use Proxy response will be sent.
To enable this option, select the "Accept inbound calls not routed via home proxy" check box.

Register with number

If this option is enabled, number will be used for registrations towards the IP-PBX instead of name. Name will be used for authentication.
To enable this option, select the "Register with number" check box.

KPML support

If this option is enabled, the DTMF digits are sent with the SIP signaling using the Keypad Markup Language (KPML) method. With this method single DTMF digits can also be sent during call setup to add digits to the callend number (overlap sending). Enbloc dialing can then be unchecked. The IP-PBX must also support KPML.
To enable this option, select the KPML support check box.

Make sure that the Allow DTMF through RTP and the Send inband DTMF check boxes are cleared.

16   Click **OK**.

17   Reset in order to make the changes take effect, see 4.28 *Reset* on page 125.

If you in step 2 selected the "SIPS" protocol the IPBS downloads a certificate from the IP-PBX to ensure a secure transaction. The IPBS does not initially trust the certificate so it must be added manually to the trust list of the IPBS. It is also possible that more than one certificate is downloaded creating a certificate chain. The root CA certificate is at the end of the chain which contains a self-signed signature and it is able to approve other certificate requests. It is recommended to add the root CA certificate to the IPBS trust list.

Note: The connection to the IP-PBX will only be established after the certificate is acknowledged.

If the certificate expires, the ongoing connection is maintained but it will not be possible to start a new connection until the certificate is renewed.

To add a certificate to the trust list do the following:

1   Select **General** > **Certificates**.

2   In the Rejected certificates section select the check box of the certificate you want to trust.

3   Click **Trust.**

To ensure two-way authentication the IP-PBX also downloads a certificate from the IPBS. The trust list must also be manually updated with this certificate in the IP-PBX similarly to the IPBS.

For more information about certificate handling, see 4.1.10 *Certificates* on page 48.

4.6.24 REGISTRATION FOR ANONYMOUS DEVICES

Handsets registered anonymously can make emergency calls through an extension reserved for anonymous users.

Note: Call restrictions must be configured in the PBX to allow for emergency calls only.

Note: When SRTP is enabled on base stations and on MiVoice Business, extensions used to make emergency calls from the base station must be programmed in MiVoice Business to use one of the SIP device profiles for IP-DECT. The profiles are programmed in the SIP Device Capabilities form and are numbered 65 (5603 SIP), 66 (5604 SIP) and 67 (5607 SIP). Other profiles cannot be used because they don't have the special SAVP handling in the MiVoice Business that is only enabled for profiles 65 through 67.

This option also provides a solution for the case when the Master, running on an IPBS with local power, loses IP connectivity without the local host Radio losing its connection to the Master. The handsets locked to this Radio become isolated from the system without any notification.

1   Select **DECT** > **Master.**

2   Enter the registration name and number to the PBX in the **Registration Name / Number** text fields.

3   Select the **Deactivate Master if no connection** check box to make the Master deactivate itself if the anonymous registration to the PBX fails. As a result the local host Radio will fail to register to the Master, and handsets, depending on their type, can move to another Radio that is operable.

Note: It is not recommended to use this option for a Master without a Standby Master.

4   Click **OK**.

Note: A simpler and reliable way to handle this case is to deactivate the local host Radio on the Master.

4.6.25 SELECT CRYPTO MASTER MODE

In a system with Mobility Master(s), a Crypto Master must be configured to enable the early encryption feature.

1   Select **DECT** > **Crypto Master.**

2   Select **Active** in the **Mode** drop-down list.

3   Write a login name in the **Name** text field.

4   Enter a password in the **Password** text field.

5   Click **OK**.

6   Connect Mobility Master(s) to the Crypto Master, see

4.6.26 SELECT MOBILITY MASTER MODE

In a system with two or more Masters (Multiple Master system), a Mobility Master must be configured. For more information on Multiple Master Systems, see the System Planning documentation for IP-DECT.

1   Select **DECT** > **Mobility Master**.

2   Select in the Mode drop-down list:
- "Active", if this IPBS is the Mobility Master.
- "Standby", if this IPBS is the Standby Mobility Master.

3   If you have selected the "Standby" mode: Enter the primary Mobility Master IP address in its text field.

4   Write a login name in the **Name** text field.

5   Enter a password in the **Password** text field.

6   Click **OK**.

4.6.27 CONNECT MOBILITY MASTER TO OTHER MOBILITY MASTER(S)

1   Select **DECT** > **Mobility Master**.

2   In the **Other Mobility Masters** section, enter a name in the **Name** text field

3   Enter a password in the **Password** text field.

4   Enter the address to the other Mobility Master in the IP Address text field.

5   Enter the address to the Standby Mobility Master for the other Mobility Master in the **Alt. IP Address** text field.

6   Click **OK**.

7   Repeat the above steps to connect to additional Mobility Masters.

4.6.28 DISCONNECT MOBILITY MASTER FROM OTHER MOBILITY MASTER(S)

1   Select **DECT** > **Mobility Master**.

2   Delete the name in the **Name** text field.

3   Delete the password in the **Password** text field.

4   Delete the address to the other Mobility Master in the IP Address text field.

5   Delete the address to the Standby Mobility Master for the other Mobility Master in the Alt. IP Address text field.

6   Click **OK**.

7   Repeat the above steps to disconnect from additional Mobility Masters.

Note: When disconnecting from other Mobility Master(s) the password field might have to be re-entered.

4.6.29 CONNECT MOBILITY MASTER TO A CRYPTO MASTER

In a system with Mobility Master(s), all Mobility Master(s) must be connected to a Crypto Master to enable the early encryption feature.
For information on how to configure a Crypto Master, see 4.6.25 *Select Crypto Master Mode* on page 83.

1   Select **DECT** > **Mobility Master**.

2   In the **Crypto Master** section: Enter the name for the Crypto Master in the **Name** text field.

3   Enter the password for the Crypto Master in the **Password** text field.

4 Enter the address to the Crypto Master in the **IP Address** text field.

5 Click **OK**.

6 Repeat the above steps to connect additional Mobility Masters to the Crypto Master.

7 To view a list of Mobility Masters connected to the Crypto Master: Select **Device Overview** > **Crypto Master**. The Mobility Masters sync status is shown in the list with a green, yellow or red dot in the column Sync. Green dot means that the Mobility Master is connected to the Crypto Master. Yellow dot means that the Mobility Master is disconnected from the Crypto Master. Red dot means that the Mobility Master must connect to the Crypto Master before the Crypto Master is operable.

4.6.30 CONNECT MASTER TO A MOBILITY MASTER

In a system with several Masters, all Masters must be connected to the Mobility Master.

1 Select **DECT** > **Master**.

2 Enter the name for the Mobility Master in the **Name** text field.

3 Enter the password for the Mobility Master in the **Password** text field.

4 Enter the address to the Mobility Master in the **IP Address** text field.

5 Enter the address to the Standby Mobility Master in the **Alt. IP Address** text field.

6 Click **OK**.

7 Reset in order to make the changes take effect, see 4.28 *Reset* on page 125.

4.6.31 ENABLE/DISABLE THE RADIO

If the IPBS shall not be used as a radio, for example only be used as a PARI Master, it can be disabled by marking the Disable check box.

Tip: To assign a PARI Master, see 4.6.32 *Enter IP Address to the PARI Master and the Standby PARI Master* on page 85.

1 Select **DECT** > **Radio**.

2 Clear the **Disable** check box.

4.6.32 ENTER IP ADDRESS TO THE PARI MASTER AND THE STANDBY PARI MASTER

All IPBS need to know the IP address of the PARI Master and the Standby PARI Master.

1 Select **DECT** > **Radio**.

2 Enter the name for the PARI Master in the **Name** text field.

3 Enter the password for the PARI Master in the **Password** text field.

4 Enter the address to the PARI Master in the PARI Master **IP Address** text field. If this is the PARI Master, enter 127.0.0.1.
   NOTE: The PARI Master can be configured as Active or Mirror.

5 Enter the address to the Standby PARI Master in the **Alt. PARI Master IP Address** text field. If this is the Standby PARI Master, enter 127.0.0.1.
   NOTE: The Standby PARI Master can be configured as Standby or Mirror.

6   Click **OK**.

7   Reset in order to make the changes take effect, see 4.28 *Reset* on page 125.

4.6.33 MULTIPLE RADIO CONFIGURATION

The PARI Master can configure the same Radio settings for all Radios in the system. All settings configured in the Radio Config page replace the local Radio settings. This means that all settings in the Radio Config menu will have precedence over values configured locally or received via DHCP options.

1   Select **DECT** > **Radio Config**.

        NOTE: To access the Radio Config. tab, the PARI function has to be enabled, see 4.6.21 *Enable PARI Function* on page 78.

2   Configure alarm and event forwarding, see *Forward Alarms and Events* on page 95.

3   Configure automatic firmware update, see 4.9.1 *Configure Automatic Firmware Update* on page 94.

4   Configure NTP settings, see 4.1.9 *Configure the NTP Settings* on page 47.

5   Configure IP settings, see 4.3.1 *Configure IPv4 Settings* on page 58.

6   Click **OK**.

4.6.34 ASSIGN PARI

The PARI is a part of the broadcast identity, which uniquely identifies an IPBS. This PARI is automatically assigned to each IPBS in the system. But if more than one Mitel IP-DECT system operates within the same coverage area, the systems need to have a unique system identity in the PARI assigned in order to differentiate the systems.

To see the occupied system IDs of other Mitel IP-DECT systems within the coverage area, perform an RFP scan, see 4.27.9 *RFP Scan* on page 125.

1   Select **DECT** > **PARI**.

        NOTE: To access the PARI tab, the PARI function has to be enabled, see 4.6.21 *Enable PARI Function* on page 78.

2   Select a number between 1 and 296, see below. If this is not done, the IPBS will randomly select a number.

        NOTE: The number of system IDs will affect how many IPBSs that can be used per PARI Master in an installation, as shown below:

        In large systems with system ID 293 to 296, the Radio should be disabled in the Pari Master. Also, with the exception for the Pari Master role, no other roles (for example Crypto Master, Kerberos server, etc.) should be activated in the Pari Master.

        System ID = 1 to 36:
        Max. 1023 IPBS per Pari Master

        System ID = 37 to 292:
        Max. 127 IPBS per Pari Master

        System ID = 293 to 296:
        Max. 2047 IPBS per Pari Master

3   Click **OK**.

4 Reset in order to make the changes take effect, see 4.28 *Reset* on page 125.

Note: The RFPI, which the PARI is a part of, can be used for localization of a handset making a personal alarm. To ensure that RFPIs are system unique, use different System ID's for each PARI Master.

4.6.35 ENTER SARI

The SARI is the broadcast identity, which uniquely identifies an IP-DECT system. The SARI is added in the PARI Master. It is possible to add more than one SARI (guest SARIs). This is necessary if you want to join two separate IP-DECT systems and allow handsets to roam into each other's system. The advantage is that the handsets in the two different IP-DECT systems need not be re-registered to a common SARI.

Note: Up to 10 SARIs can be added in the PARI Master. It will take approx. 1 s to broadcast 2 SARIs and approx. 6 s to broadcast 10 SARIs. The impact this has on roaming areas will be more significant for a user moving fast.

1 Select **DECT** > **SARI**.

  NOTE: To access the SARI tab, the PARI function has to be enabled, see 4.6.21 *Enable PARI Function* on page 78.

2 Enter the SARI number in the SARI text field.

3 Click **OK**.

4 You can add optional guest SARI numbers in the empty field.

5 Click **OK**. All RFPs are reinitialized to broadcast also the added guest SARI.

4.6.36 CONFIGURE AIR SYNCHRONIZATION

IPBS System

The IPBSs use the DECT air interface to synchronize to each other. For an individual IPBS it is not needed to configure which IPBS to synchronize to. It is needed to manually select one or several IPBS as synchronization master candidate. ThePARI Master assigns one of these IPBS as an active sync master. The remaining candidates will act as sync slaves and can be new sync masters in case the active sync master will fail/break. When using one sync region it is recommended to configure at least two base stations in the middle of the building as synchronization masters.
All IPBSs in sync slave mode sends its list over received sync candidates to thePARI Master. ThePARI Master informs the IPBS sync slaves which sync candidate it shall synchronize to.

Sync Regions

Sync regions are used when, for example, several buildings are located in the same coverage area and all radios are using samePARI Master but where the synchronization coverage between buildings is not good enough for a stable synchronization.

A solution may be to use separate synchronization regions for the buildings and have reference synchronization between the regions. Each region has its own Sync Master but can take reference sync from another region and handover between the buildings is possible. If a region should lose the reference synchronization with another region, the internal synchronization in respective region will still work but there can be no handover between the regions.

Note: For the synchronization to work, it is not allowed to configure reference sync in a ring.

Configure Sync Slave IPBS

All IPBSs in sync slave mode sends its list of sync candidates to the PARI Master. The PARI Masters informs the IPBS sync slave which sync candidate it shall synchronize to.

In addition to the above automatic synchronization procedure it is also possible to use static synchronization, that is, manually lock on to a specific RFPI. When specifying a specific RFPI, it must be within the same synchronization region.

Configure Sync Slave as follows:

1   Select **DECT** > **Air Sync**.

2   Select **Slave** in the **Sync Mode** drop-down list.

3   To lock the sync slave to a specific RFPI, enter the sync RFPI in the Sync RFPI text field. Enter an alternative sync RFPI in the Alternative Sync RFPI text field (optional).

4   Enter a region ID between 0 and 249 in the **Sync Region** text field.

5   Click **OK**.

Configure Restricted Slave IPBS

The restricted slave mode gives the possibility to disable air synchronization sources that are not reliable. IPBSs configured in restricted slave mode cannot be used as a synchronization source so they can only retrieve synchronization from other radios.

Configure restricted slave mode as follows:

1   Select **DECT** > **Air Sync**.

2   Select **Restricted Slave** in the Sync Mode drop-down list.

3   To lock the restricted slave to a specific RFPI, enter the sync RFPI in the **Sync RFPI** text field. Enter an alternative sync RFPI in the **Alternative Sync RFPI** text field (optional)

4   Enter a region ID between 0 and 249 in the **Sync Region** text field.

5   Click **OK**.

Configure Sync Master IPBS

Radios configured as sync master will report to the PARI Master that it wants to be a sync master. The PARI Master will select one of them to be the active sync master.

When a sync master has been assigned to be active it searches for other IPBSs within the same region during 30 seconds. If any IPBS is found the values for slot, frame, multi frame and PSCN are received and applied to the Sync Master. After receiving all these values or after the time-out of 30 seconds the Sync Master enters the master state.

With this method it will be possible to restart only the Master in the region. The remaining slaves will be able to maintain synchronization for a few minutes during restart of the Master. The Master will adjust itself to the other IPBSs at startup. The slaves will notice that the Master is back and the synchronization will be received from the Master.

In master state the values are updated locally during all further operation of the Master IPBS and no synchronization to other IPBSs in the same region is done.

It is possible to configure the Sync Master to synchronize to a reference base station (another or same DECT system). In this case the Sync Master will try to synchronize to the reference system if the reference system is found but it will not require the reference system to be available. The Sync Master will operate even though the reference system is not available. During startup the Master will prefer to synchronize to a slave base in the same system before synchronizing to the reference base station.

Configure Sync Master as follows:

1   Select **DECT** > **Air Sync**.

2   Select **Master** in the **Sync Mode** drop-down list.

3   To synchronize the sync master to a reference base station, enter the reference base station in the Reference RFPI text field. Enter an alternative reference base station in the Alternative reference RFPI text field (optional).

4   Enter a region ID between 0 and 249 in the **Sync Region** text field.

5   Select type of resynchronization action to perform at reference sync failure, a manual or an automatic (scheduled) one.

6   Click **OK**.

4.7 VOIP

This section only applies if the SIP protocol is used in the system.

4.7.1 ADD INSTANCE ID TO THE USER REGISTRATION WITH THE IP-PBX

This might simplify administration with some IP-PBXs.

1   Select **VoIP** > **SIP**.

2   To enable, select the **Add instance id to the user registration with the IP-PBX** check box corresponding to the SIP protocol that is used.

3   Click **OK**.

4.7.2 IP-PBX SUPPORTS REDIRECTION OF REGISTRATION WHEN REGISTERED TO ALTERNATIVE PROXY

When the primary proxy is down and an alternative proxy is in use, the IP-PBX will redirect the registration to the primary proxy when available again. IP-DECT will not make any attempts to contact the primary proxy as long as the alternative proxy is available.

1   Select **VoIP** > **SIP**.

2   To enable, select the **IP-PBX supports redirection of registration when registered to alternative proxy** check box corresponding to the SIP protocol that is used.

3   Click **OK**.

4.7.3 USE LOCAL CONTACT PORT AS SOURCE PORT FOR TCP AND TLS CONNECTIONS

Instead of having a dynamic/ephemeral source port for the persistent TCP/TLS connection, the local contact port of the corresponding phone can be used instead (required by some IP-PBXs.).

1   Select **VoIP** > **SIP**.

2   Select the **SIPS** check box.

3   Click **OK**.

4.7.4 PREFER P-ASSERTED-IDENTITY AS CALLING PARTY IDENTITY

Enable this option if the P-Asserted-Identity-header is preferred instead of the Fromheader as calling party identity, received in the INVITE message.

1   Select **VoIP** > **SIP**.

2   To enable, select the **Prefer P-Asserted-Identity As Calling Party Identity** check box corresponding to the SIP protocol that is used.

3   Click **OK**.

4.7.5 USE SBC FOR NAT TRAVERSAL

If a Session Border Controller (SBC) is used which handles NAT traversal between IP-DECT and the IP-PBX, it might be needed to enable this option. By enabling this option the Contact address will not be updated with the external address when NAT is detected by IP-DECT.

1   Select **VoIP** > **SIP**.

2   To enable, select the **Use SBC for NAT traversal** check box corresponding to the SIP protocol that is used.

3   Click **OK**.

4.7.6 NO SERVER CERTIFICATE SUBJECT CHECK FOR TLS CONNECTIONS

Normally the server certificate subject (CN/SAN) will be checked against what has been configured in IP-DECT. If there is no match, the TLS connection will fail. By selecting this option the check will not be made.

1   Select **VoIP** > **SIP**.

2   To enable, select the "No Server Certificate Subject Check For TLS Connections" check box corresponding to the SIP protocol that is used.

3   Click **OK**.

4.7.7 ACCEPT HOLD SIGNALING USING REMOTE MEDIA ADDRESS 0.0.0.0

This option is used when a media re-negotiation returns a remote media address 'c=IN IP4 0.0.0.0' and the purpose is to put the local handset on hold without media, but the media attribute 'a=inactive' is not used.

1   Select **VoIP** > **SIP**.

2   To enable, select the **Accept Hold Signaling Using Remote Media Address 0.0.0.0** check box corresponding to the SIP protocol that is used.

3   Click **OK**.

4.7.8 REMOVE SRTP LIFETIME IN SDP

This option is used to disable SRTP crypto key lifetime in SDP. The purpose is to make the SRTP negotiation compatible with PBXs that does not support SRTP crypto key lifetime in SDP (e.g. Cisco UCM).

1   Select **VoIP** > **SIP**.

2   To enable, select the **Remove SRTP Lifetime in SDP** check box corresponding to the SIP protocol that is used.

3   Click **OK**.

4.7.9 ALLOW MULTIPLE CODECS IN ANSWER SDP

If a received SDP answer includes multiple voice codec choices, a re-negotiation is started to pinpoint the preferred codec and avoid potential asymmetric media problems. By selecting this option the re-negotiation will not be made.

1   Select **VoIP** > **SIP**.

2   To enable, select the Allow Multiple Codecs in Answer SDP check box corresponding to the SIP protocol that is used.

3   Click **OK**.

4.7.10 SESSION TIMER (INITIAL VALUE)

If set, a keep-alive mechanism will be used to detect if a call is still valid as defined by rfc 4028. This is normally handled by the IP-PBX and then not necessary to be defined here.

1   Select **VoIP** > **SIP**.

2   To enable, enter a time (sec.) in the **(Session Timer initial value)** field.

3   Click **OK**.

4.7.11 AASTRA USER AGENT

For backward compatibility in systems with MX-ONE, do as follows:

1   Select **VoIP** > **SIP**.

2   Select the **Aastra User Agent** check box.

3   Click **OK**.

4   Perform a reset to restart the IPBS, see

4.8 UNITE (CPDM3/WSM3)

4.8.1 CONFIGURE MESSAGING

If an CPDM3/WSM3 is to be used in the IP-DECT system, enter the IP address following the steps below.

1   Select **UNITE** > **SMS**.

      NOTE: To access the SMS tab, the Master mode has to be activated, see

2   Enter the address to the CPDM3/WSM3 in the **IP Address** text field.

3   Click **OK**.

The communication between the Master and the CPDM3/WSM3 should be encrypted, do as follows:

1   Select **UNITE** > **SMS**.

      Note: To access the SMS tab, the Master mode has to be activated, see

2   Deselect the **Encryption** check box.

Note: a) When selecting or clearing the Encryption check box, it may take up to a couple of minutes until the CPDM3/WSM3 is fully operational.

      b) The CPDM3/WSM3 support for encryption is depending on the CPDM3/WSM3 software version.

3   Click **OK**.

4.8.2 DEVICE MANAGEMENT

NOTE: To access the Device Management tab, the Master mode has to be activated, see

If a specific Device Manager is to be used in the IP-DECT system, enter the IP address to the Device Manager following the steps below. To set the Master to search for an existing Device Manager on the network, go to

The PARI Master setting is distributed to all Radios automatically.

For Portable Devices, do as follows:

1   Select **UNITE** > **Device Management**.

2   In the **Portable Devices** section: Enter the address to the Device Manager in the **IP Address** text field.

      The IP address for the Device Manager that the Master is currently connected to is shown under Active Settings.

3   Click **OK**.

For IP-DECT Devices, do as follows:

1   Select **UNITE** > **Device Management**.

2   In the **IP-DECT Devices** section: Enter the address to the Device Manager in the **IP Address** text field.

Note: The IP address for the Device Manager that the Master is currently connected to is shown under Active Settings.

The IP address for the Device Manager that the PARI Master is currently connected to is shown under Active Settings.

3   Enter the Resource Identity/Service in the **Resource Identity** text field. The default is **IPDECT**.

4   Click **OK**.

4.8.3   SERVICE DISCOVERY

Note: In this section, the word "device" means both PARI Master and other devices where the Radio is not activated.

If no Device Manager has been selected to be used in the IP-DECT system, see 4.8.2 *Device Management* on page 92, then the Master will automatically search for an existing Device Manager on the network. To set the Master to search in a specific domain on the network or to stop the search, follow the steps below.

1   Select **UNITE** > **Service Discovery**.

Note: The **Service Discovery** tab is accessible only for PARI Master and for devices where the Radio is not activated.

2   Do one of the following:

- To stop the Master to search for a Device Manager, select the **Disable** check box.
- To set the Master to search for a Device Manager in a specific domain on the network, enter the domain id in the **Domain ID** text field. The domain id must be the same as the one entered in the Device Manager.

3   Click **OK**.

When the Master is connected to a Device Manager, the IP address for the Device Manager is shown in the Unite Address text field under UNITE > Device Management.

4.8.4   SEND STATUS LOG

It is possible to send alarm and event reports to the Unite system. For example directly to the ESS fault handler or to the UNA (Unite Node Assistant) which in turn forwards the alarm event according to distribution lists.

1   Select **UNITE** > **Status Log**.

2   Enter the address to the server where the Status Log should be sent in the Unite IP Address text field.

3   Enter the Resource Identity/Service in the **Unite Resource Identity** text field. If this field is left empty then the default will be UNA (Unite Node Assistant).

4.8.5   MODULE FAULT LIST

It is possible to change the severity level on alarms and events generated in the IP-DECT system.

1   Select **UNITE** > **Module Fault List.** A list of alarms and events generated in the
      IP-DECT system is shown with their fault codes (IP-DECT code and Unite code).
      Alarms are listed with a Yes and events are listed with a No in the column
      Persistant.

2   To change the severity level on an alarm/event: Select in the Seriousness drop-
      down list one of the following:

   • Disabled (The alarm/event will not be sent to the Unite system.)
   • Information
   • Warning
   • Error
   • Critical

3   Click **OK**.

      Except for severity level Disabled, the alarm/event will be sent to the Unite
      system with changed severity level.

4.9 SERVICES

4.9.1 CONFIGURE AUTOMATIC FIRMWARE UPDATE

The IPBS can be configured to automatically update its firmware. A script file must be
uploaded to a suitable directory on an internal web server. For information on the script
file syntax, see Appendix A: *How to Configure and Use the Update Server* on page
137.

1   Select **Services** > **Update**

2   Enter the URL of the script file in the URL text field.

3   Enter the poll interval, in minutes, in the Interval (min) text field

4   Click **OK**.

The Current Update Serials section shows the values of the variables set after the last
execution of the associated command.

4.9.2 CONFIGURE LOGGING

There are three ways to collect logs, see the table below.

TCP	The syslog entries are transmitted using a TCP connection.
SYSLOG	The entries are reported to a "syslogd" server in the network, which is responsible for further evaluation or storage of the entries.
HTTP	The syslog entries are transferred to a web server where they can be further processed. Each individual syslog entry is transmitted as form data to the web server in HTTP GET format.
HTTPS	The syslog entries are transferred to a web server where they can be further processed. Each individual syslog entry is transmitted as form data to the web server in HTTPS GET format.

Store the Syslog Entries using a TCP Connection

1   Select Services > Logging

2   Select "TCP" in the Type drop-down list.

3   Enter the "IP address" of the logging server in the Address text field.

4   Enter the "Port" of the logging server in the Port text field.

5   Click "OK".

Store the Syslog Entries in a Syslogd

1   Select Services > Logging.

2   Select "SYSLOG" in the Type drop-down list.

3   Enter the "IP address" of the syslogd in the Address text field.

4   Enter the desired syslogd message class in the Class text field.

5   Click "OK".

Store the Syslog Entries on a Web Server

1   Select Services > Logging.

2   Select "HTTP" or "HTTPS" in the Type drop-down list.

3   Enter the IP address in the IP Address text field.

4   Enter the port in the Port text field.

5   Enter the relative URL of the form program on your web server in the Path text field.

6   Click "OK".

Note: The IPBS will make an HTTP GET request or HTTPS GET request to the web server on the registered URL followed by the URL-encoded log entry.

Example:

Enter the value "/cdr/ cdrwrite.asp" in the "URL-Path" field if a page is on the web server with the name "/cdr/cdrwrite.asp" with a form that expects the log message in the "msg" parameter. In this example, the IPBS will make a GET /cdr/ cdrwrite.asp?event=syslog&msg=logmsg request to the server.

Forward Alarms and Events

It is possible to forward alarms and events to a HTTP server destination. Typically this can be a Master base station. This programming can be done in the PARI Master (DECT > Radio config) or locally as described below.

1   Select Services > Logging.

2   If the HTTP server destination requires HTTPS then select "HTTPS" in the Type drop-down list.

3   Enter the IP Address of the IPBS where you want to have an overview of all faults in the External HTTP Server Address text field.

4   Enter the HTTP server port in the External HTTP Server Port text field. The default value is 80.

4.9.3 CONFIGURE THE HTTP SETTINGS

Traditionally IPBS has been administered over the network via the http protocol (default port 80).

In a secure system (see the IP Security chapter) IPBS should be administered via the https protocol (default port 443). If for some reason port 443 is not to be used, you can use another port for the local https server and then access the IPBS via this port.

Http and https traffic, respectively, would be disabled if their port values were to be set to zero (0). Therefore:

- To disable http traffic set "Port" to 0 (which is recommended in a secure system). Attempts to contact the device using the http protocol will result in an Unable to connect message.
- To disable https traffic set "HTTPS Port" to 0 (not recommended).

Any other port values would enable http and https traffic, respectively, for the port specified.
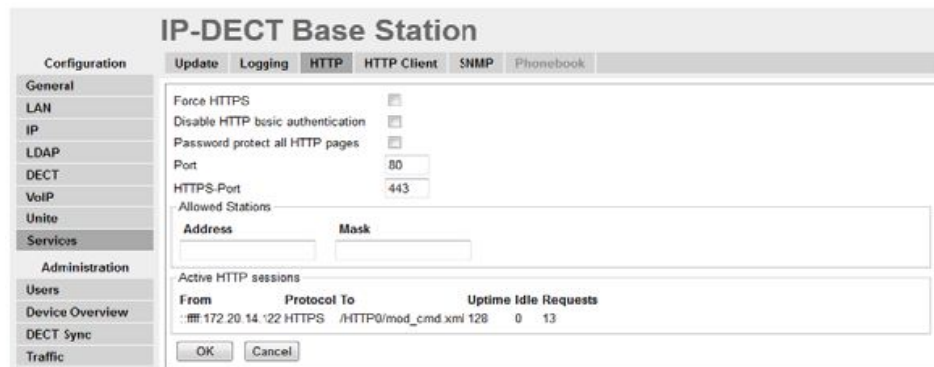
Figure 6. Configure the HTTP Settings

1   Select **Services** > **HTTP**

- Select the **Force HTTPS** check box to allow only HTTPS sessions and all HTTP requests are redirected as HTTPS requests.
- Select the **Disable HTTP basic authentication** check box to require all administrative and programmatic clients to support HTTP digest authentication.
- Select the **Password protect all HTTP pages** check box to password protect all HTTP pages.
- Select the **Mutual TLS (MTLS)** check box to enable mutual TLS for client certificate authentication.

IMPORTANT: A trusted client certificate with the associated private key must be installed in the web browser's certificate store. See Appendix G: *Import Client Certificate in the Web Browser* on page 160. The trusted client certificate or the CA certificate that signed the client certificate must also be added to the trust list in the device. See *Trust List* on page 49. If the correct certificate is not available, and mutual TLS authentication is enabled, it is not possible to access the device in any other way.

- Select the **No Cache** check box to request the web browser not to store any data in the cache.
- Enter **Port number** in the **Port** text field. The IPBS is by default administered over the network via the TCP port 80 (http). If port 80 is not to be used

another port can be set up for access. Set this value to 0 to disable http traffic (recommended). Attempts to contact the device using the http protocol will result in an Unable to connect message.

- Enter **HTTPS Port** in the **HTTPS Port** text field. To access IPBS securely, use the TCP port 443 (https). Set this value to anything except zero (0) to enable https traffic. The default value is 443. The value zero (0) disables https traffic which is not recommended.
- Enter **Network Base Address/ Network Base Mask** in the **Allowed stations** text fields to only allow access only from matching network, for example:172.16.0.0 / 255.255.0.0
- In the **Active HTTP sessions** field all ongoing HTTP traffic is displayed.

2   Click **OK**.

4.9.4   CONFIGURE THE HTTP CLIENT SETTINGS

A list of URL that require authentication can be specified.

1   Select Services > HTTP Client.

2   Enter the "URL" in the URL text field.

3   Enter "User" and "Password" in the User and Password text fields.

4   Click "OK".

A new row will be shown and more URLs can be added.

4.9.5   SNMP

Faults can be reported in the IP-DECT system via the Simple Network Management Protocol (SNMP). The SNMP framework has three parts:

- An SNMP manager: the system used to control and monitor the activities of network hosts using SNMP.
- An SNMP agent: the software component within the managed device that maintains data for the device and reports data, as needed, to managing systems.
- A MIB: The Management Information Base (MIB) is a virtual information storage area for network management information.

The agent and MIB reside on a network device (for example, router, access server, or switch). To enable the SNMP agent on the IPBS, the relationship between the manager and the agent must be defined.

The MIB file is available in the IPBS software package zip file.

Figure 7. Configure SNMP Settings

1   Select Services > SNMP

2   Enter a name in the Community field if you are not using the standard community name (public). The community text string acts like a password to regulate access to the agent on the Base Station.

3   Enter a device name in the Device Name field. This field is optional and serves only informational purposes.

4   Enter the name and phone number of the contact person in the Contact field. This field is optional and serves only informational purposes.

5   Enter a location in the Location field. This field is optional and serves only informational purposes.

6   Select the Authentification Trap check box to enable the sending of authentification traps. Access via SNMP is only possible if the correct Community Name is entered. If enabled a trap will be generated in the event of access with an incorrect Community Name.

7   Enter the IP address of the desired trap destinations in the Trap Destinations field. SNMP traps will be sent to all destinations.

8   Enter the IP address and mask of the networks that are allowed to send SNMP requests. All networks are allowed if the field is empty.

9   Click "OK".

4.9.6 PHONEBOOK

This section describes how to import entries to the central phonebook (see *Import Entries to the Central Phonebook* on page 99) and how to export the central phonebook to csv file (see *Export the Central Phonebook to a csv file* on page 100 and how to configure LDAP directories).

Central phonebook is a feature that when enabled in the Master allow DECT handset users to search for telephone numbers in a database stored locally on a Master. If enabled, the central phonebook can also be accessed through a PBX or an external LDAP server.

If the same central phonebook shall be used in a multiple Master system and/or Standby Master functionality is used, the central phonebook must be stored in all masters. This is done by using LDAP replication where the central phonebook in one Master (LDAP server) is replicated to the masters configured as LDAP replicators. See *Import Entries to the Central Phonebook by Replication from other Master* on page 99.

Note: If the phonebook functionality in the IPBS is enabled, then the SMS feature in the CPDM3/WSM3 is disabled. If a CPDM3/WSM3 is connected, the central phonebook should be located in the CPDM3/WSM3 instead of the IPBS.

Import Entries to the Central Phonebook

There are two ways to import entries to the central phonebook:

- from a csv file
- by replication from other Master

Import Entries to the Central Phonebook from a csv file

Note: A csv file can contain max 1000 users.

The csv file to be imported to the phonebook shall have the following format:

First name 1;Last name 1;Telephone number 1
First name 2;Last name 2;Telephone number 2

or

First name 1,Last name 1,Telephone number 1
First name 2,Last name 2,Telephone number 2

Note: When importing a central phonebook file in csv format, existing entries are deleted.

1   Select **Services** > **Phonebook**.

2   Select **Local** in the Current view drop-down list

3   Select **File upload** in the **Data Source** drop-down list.

4   Select file type for the csv file in the **File Type** drop-down list.

5   If so needed, select separator for the csv file in the **Delimeter** drop-down list.

6   Click **OK**. The options **Import** and **Export** are displayed.

7   Select **Import** > **Choose File**.

8   Locate the csv file in the system and select **Open** > **Next**. Ensure the correct number of entries are correct.

9   Click **Close**

Import Entries to the Central Phonebook by Replication from other Master

Note: An LDAP server and LDAP replicator(s) must first be configured. See *4.5 LDAP* on page 61.

1   Select **Services** > **Phonebook**.

2   Select **Local** in the Current view drop-down list

3   Select **Replication from other Master** in the **Data Source** drop-down list.

4   Enter the IP address to the LDAP server in the **Master IP Address** text field.

5   Enter the LDAP user name and password in the **Name and Password** text fields.

6   Click **OK**.

To check the replicator status, select **LDAP** > **Replicator-Status**. See also 4.5.4 *Check LDAP Replicator Status* on page 67.

Export the Central Phonebook to a csv file

The complete phonebook can be exported to a csv file for example for editing or backup reasons.

1   Select **Services** > **Phonebook**.

2   Click **Export**.

3   Click **Download file** in the window that appears.

4   Click **Save** in the dialog window that appears.

5   Enter a name of the file and select in which folder the file should be saved.

6   Click **Save**.

Configure the Central Phonebook in the PBX

DECT handset users can search the central phonebook through an Innovaphone PBX LDAP directory.

1   Select **Services** > **Phonebook**.

2   Select **LDAP** in the **Current view** drop-down list.

3   Select the **Enable** check box under PBX.

4   Enter the IP address and port number of the LDAP server in the following format: **IP address:port**, for example: 176.14.12.1:1234.

5   Select the **Use TLS** check box to use a secure LDAP connection through port 636.

6   Enter the user name for the LDAP server authentication in the **User** field.

7   Enter the password for the LDAP server authentication in the **Password** field.

8   Click **OK**.

Configure the Central Phonebook in the External LDAP Server

DECT handset users can search the central phonebook through an external LDAP server.

1   Select **Services** > **Phonebook**.

2   Select **LDAP** in the **Current view** drop-down list.

3   Select the **Enable** check box under PBX.

4   Enter the IP address and port number of the LDAP server in the following format: **IP address:port**, for example: 176.14.12.1:1234.

5   Select the **Use TLS** check box to use a secure LDAP connection through port 636.

6   Enter the user name for the LDAP server authentication in the **User** field.

7   Enter the password for the LDAP server authentication in the **Password** field

8   Enter the search root for the LDAP search in the **Search Base** field.

For example, if an Active Directory (AD) is used, the search base can be "CN=Users, DC=DomainName" where "DomainName" is the name of the domain on the AD server.

9   Enter an LDAP filter in the **Search Filter** field if you want to retrieve only certain LDAP objects. This field can usually be left blank for searching in the phonebook.

10   Enter the attributes to search for in the **Search Attributes** field. For example, "cn".

11   Enter the requested LDAP number attributes in the **Number Attributes** field. Each attribute name can be followed by a tag used to identify the type of number.

For example, ipphone:office, homephone:home.

12   Enter the attribute used to sort the search result in the **Display/Sort Attributes** field. For example, "cn".

13   Click **OK**.

Configure Dialing Location

If the telephone numbers are stored in an international format in the directory, the prefixes can be configured to convert the phone number into the correct format.

1   Select **Services** > **Phonebook**.

2   Select LDAP in the Current view drop-down list.

3   Enter the required prefixes under Dialing Location.

The following prefixes can be configured:

Country code	The country code used to convert a phone number to an international number, for example 46.
Area code	The area code used to convert a phone number to a national number, for example 30.
National prefix	The national trunk prefix used to mark a number as national, for example 0.
International prefix	The international trunk prefix used to mark a number as international, for example 00.
External line	The prefix needed to access a trunk line. Usually 0 in most PBX configurations.
Subscriber numbers	The prefix used to convert an extension to a subscriber number, for example 4322.

4   Click **OK**.

4.9.7   REFORMATTING MIVOICE 250 USER INFORMATION FOR THE PHONEBOOK

When you export users from the MiVoice 250 into a.csv file, you cannot chose the specific columns that you want. Therefore, the .csv file contains more columns of information than needed.

Re-format the.csv file to contain only the three columns described above in the csv file to be imported to the phonebook shall have the following format: on page 75. You will then be able to import this newly-formatted .csv file into the Central Phonebook.

Note: When importing a central phonebook file in csv format, existing entries are deleted.

1   Select **Services** > **Phonebook**.

2   Select the **Enable** check box.

3   Select **File upload** in the **Data Source** drop-down list.

4   Select file typer for the csv file in the **File Type** drop-down list.

5   If so needed, select separator for the csv file in the **Delimeter** drop-down list.

6   Click **OK**. The options Import and Export are displayed.

7   Select **Import** > **Choose File**.

8   Locate the csv file in the system and select Open > Next. Make sure the correct number of entries are correct.

9   Click **Close**.

4.9.8   CONFIGURE IP-DECT TO CONNECT TO A PRESENCE SYSTEM USING ICP

With a presence system users will be able to enter absent information to inform the calling person why the called person is not available.

The IP-DECT system can be configured to connect to a presence system via the ICP protocol as follows:

1   Select **Services** > **ICP**.

Note: To access the ICP tab, the Master mode has to be activated, see 4.5.19 Select Master Mode on page 67.

2   Select the **Enable** check box.

3   In the **Presence System** text field, enter the IP address to the presence system to connect to.

Note: Leave this field empty if connection is established from other side.

4   In the **Port** text field, enter the port over which presence information are sent/ received.

5   In the **Deactivation Type** drop-down list, select which type of deactivation message to use.

6   In the **Terminal ID Len** drop-down list, select the maximal length of a terminal id (operator desk).

7   In the **Directory Number Len** drop-down list, select the maximal length of a directory number (user number).

8   In the **Fill Character** text field, enter a character that will be used to fill shorter directory/terminal numbers. Recommended is to use "@".

9   Select the **Send Heartbeat** check box if the IP-DECT system should send heartbeat signals towards the presence system.

10   In the **Heartbeat Interval (s)** text field, enter in seconds the interval between two heartbeats.

11   In the **Server reconnection interval (s)** text field, enter in seconds the time between reconnection attempts if acting as server.

12   In the **Code** text fields, enter new display texts if other than the default ones (max 12 characters). For each code, set if time (HHMM) or date (MMDD) input is required.

13   In the month text fields, enter new display texts if other than the default ones (max three characters).

14   Click **OK**.

To activate presence

Presence can be activated from a DECT handset or from an operator desk. To activate from a DECT handset the user is entering key pad data for activation of presence, for example *23*3*1500#, where "3" is the reason code and "1500" is the back time. Depending on what has been configured for reason code 3 (see step 12 above), the back time is entered in format HHMM (hour and minutes) or MMDD (month and day).

Note: To configure the key pad data for activation and deactivation of presence, select DECT > Suppl. Serv. Set the Interception parameter.

For more information, see 4.5.18 Configure Supplementary Services on page 65.

To deactivate presence

To deactivate from a DECT handset the user is entering key pad data for deactivation of presence, for example #23#.

4.10 Users

This section describes the Users sub menu and how to do the following:

- Show all registered users in the IP-DECT system.
- Search for user information.
- Add a user.
- Add a user administrator.
- Import a csv file with user information.
- Export a csv file with user information.
- Show all anonymous registered handsets in the IP-DECT system.
- Add an anonymous handset.
- Import a csv file with IPEI numbers for anonymous handsets
- Export a csv file with IPEI numbers for anonymous handsets.

4.10.1 SHOW ALL REGISTERED USERS IN THE IP-DECT SYSTEM

Shows both User Administrator and Users.

1   Select **Users** > **Users**.

2   Click **show**.

It is possible to change the order of the list by clicking on the headings.

4.10.2 SEARCH FOR USER INFORMATION

It is possible to search for users registered in the system by name or extension number. Search for a user following the steps below:

1   Select **Users** > **Users**.

2   Enter the long name to search for in the text field, either by entering the whole long name or by entering the beginning of the long name.

3   Click **show**.

4.10.3 ADD A USER

For information on how to add users to the IP-DECT system, see 3.13 *Add Users* on page 29.

Add a User to Another IP-DECT System

To allow handsets to identify the system to which the subscription shall be directed (e.g. the same physical area may be covered by different systems), it may be necessary to enter an initial PARK into a handset.

To view the PARK and the PARK 3rd pty code:

1   Select **Users** > **Users**.

PARK: Must be used for DTxx/5600 handsets. Can also be used for other handsets if they support a PARK that matches the SARI.

PARK 3rd pty: Must be used for handsets that do not support a PARK that matches the SARI.

For information on how to subscribe the user's handset to the other IP-DECT system, see the reference guide for the handset.

4.10.4 ADD A USER ADMINISTRATOR

For information on how to add user administrator to the IP-DECT system, see *Managing User Administrators* on page 21.

4.10.5 IMPORT USERS FROM A CSV FILE

For information on how to add users with import a csv file to the IP-DECT system, see

3.14.3 Easy Registration on page 28.

4.10.6 EXPORT THE USERS TO A CSV FILE

The Users can be exported to a csv file, for example for editing or backup reasons.

1   Click **Export**.

2   Click **Save** in the dialog window that appears.

3   Enter a name of the file and select in which folder the file should be saved.

4   Click **Save**.

Note: For safety reasons, the Auth. Code and Password will not be included in the csv file.

4.10.7 SHOW ALL ANONYMOUS REGISTERED HANDSETS

The IPEI / IPDI number is displayed on anonymous registered handsets.

1   Select **Users** > **Anonymous**.

4.10.8 4.9.8ADD AN ANONYMOUS HANDSET

1   Select **Users** > **Anonymous**.

2   Click **new**.

3   Enter the IPEI for the anonymous handset.

4   Click **OK**.

For information on how to assign the anonymous handset to a user, see 3.14.1 Anonymous Registration on page 25.

4.10.9 IMPORT ANONYMOUS HANDSETS FROM A CSV FILE

The anonymous handsets IPEI can be imported from a csv file. The csv file may have the following format with one IPEI per line:

IPEI

IPEI

IPEI

IPEI

1   Select **Users** > **Anonymous**.

2   Click **import**.

3   Click **Browse** to locate the csv file.

4   Click **Open** > **Next.** Make sure the correct number of entries are correct.

5   Click **Next.**

Limitations

• Maximum 1000 rows in the csv file.
• The maximum csv file size is 128 Kb. If the file is too large, divide the file into several files.
• Only the new IPEIs are imported. The old IPEIs are not deleted.
• Existing IPEIs cannot be updated.

4.10.10 EXPORT ANONYMOUS HANDSETS TO A CSV FILE

The anonymous registered handsets IPEI can be exported to a csv file, for example for editing or backup reasons.

1   Select **Users** > **Anonymous**.

2   Click **export**.

3   Click **Save** in the dialog window that appears.

4   Enter a name of the file and select in which folder the file should be saved.

5   Click **Save**.

4.11 DEVICE OVERVIEW

4.11.1 RADIOS

Information about the devices in the IP-DECT system.

1   Select **Device Overview** > **Radios**.

Name	The unique identification name. The name syntax is ipbs-xx-xx-xx (IPBS1/IPBS4x0), ipbs2-xx-xx-xx (IPBS2/IPBS4X2), where xx-xx-xx should be replaced with the last 6 hexadecimal digits of the MAC address.
RFPI	Radio Fixed Part Identity.
IP Address	The IP address, click on the IP address to access the configuration GUI of that IPBS.
Sync	The current synchronization status. Should be "Master OK", "Slave OK" or "Standby OK" if synchronized. "Standby" is a Radio configured as a Sync Master but it is active.
Region	The sync region which the Radio belongs to.
Device Name	The name entered in the general menu.
LDAP	The LDAP status, can be "" (blank), "-", "up", "server" or "down". Should be "-", "up" or "server".
Version	The current software version.
Connected Time	The elapsed time since connected to the Master.

Add Radios

In the Uninitalized Registrations section, uninitialized Radios not registered to a PARI Master are shown.

1   Select **Device Overview** > **Radios**

2   Click **Add** to add the Radio to the Master.

3   In the **Add Radio** window enter a name for the device. You can also add a Standby Master IP Address and a Sync Region.

4   Click **OK**.

5   The Radio restarts and it establishes a connection to the PARI Master only.

Delete Radios

In the Static Registrations section, initialized Radios no longer registered to the PARI Master are shown.

1   Select **Device Overview** > **Radios**

2   In the **Static Registrations** section, click **Delete** to delete the Radio.

     The Radio's RFPI is now released and can be reused. All other RFPIs in use are not affected.

Move RFPIs

In the Static Registrations section, initialized Radios no longer registered to the PARI Master are shown. If it is vital that the new device keeps the RFPI for the broken device e.g. alarm localization purposes, move the RFPI for the broken device to the new device registered to the PARI Master.

1   Connect the replacing device.

2   Add the Radio to the PARI Master, see *Add Radios* on page 107.

3   Select **Device Overview** > **Radios**.

4   In the Static Registrations section, click **Move** for the Radio that is broken.

5   In the **Move RFPI** window, select in the Destination section the new Radio that you want to move the broken Radio's RFPI to.

6   Click **Move**.

     Existing RFPI on the new Radio is replaced by the broken Radio's RFPI. The new Radio's RFPI is now released and can be reused. All other RFPIs in use are not affected. The broken Radio will be deleted from the Static Registrations section.

4.11.2 AIR SYNC

Air Sync status is displayed in the Device Overview > Air Sync menu. For explanation on the information shown for the active and the alternative sync bearers, see the table below.

RFPI	Radio Fixed Part Identity is the Id number of the sync bearer.
Carrier	The carrier used for air synchronization
Slot	The slot used for air synchronization

Hop	The number of hops from the Sync Master to the sync bearer
RSSI	Received Signal Strength Indication
FER	Frame Error Rate, a value between 0 and 100%. For a good synchronization the FER should be 0. It is OK to occasionally have a high FER, but only for short periods (up to one minute).

4.11.3 SYNC LOST COUNTER IN IPBS

This section will describe briefly the different situations when the "sync lost counter" is incremented and what impact it has for the users.

Sync Lost Counter

When an IPBS increments the sync lost counter it means that the IPBS stops to handle all radio traffic for a while and after that restarts the synchronization procedure. The radio part is not really restarted but out of service for a short time period. The IP-part of the IPBS is not affected by this but is in service all the time.

There are five reasons for when the sync lost counter is incremented:

- The IPBS has not been able to find a synchronization source within 9 minutes.
- The PSCN value is changed.
- The value for frame number is changed.
- The value for multi frame number is changed.
- The number of enabled carriers is changed.

If the PSCN, frame number, multi frame number and/or the number of enabled carriers is changed, then the radio stops to handle traffic immediately.

Impact for the Users

During speech

If the radio stops to handle traffic as described in *Sync Lost Counter* on page 108, it does not necessarily mean a disconnected call. In a system with good overlapping coverage it might be possible to make a handover to another IPBS without disconnecting the call. If the handset does not quickly find any other IPBS the call will be disconnected and the handset will indicate "No System". As soon as the IPBS is synchronized it is available again for handset communication. The handset will then connect to the system in the same way as for a normal power on.

In idle mode

In idle mode the user will most likely not discover any problem. Since the handsets have a short delay before showing "No System" the handset has time to roam to another IPBS. This requires a good overlap between radio cells to make it possible for the handset to roam to another IPBS. If no other IPBS is available the handset(s) will indicate "No System". As soon as the IPBS is synchronized it is available again for handset communication. The handset will then connect to the system in the same way as for a normal power on.

4.12 DECT SYNC

4.12.1 AIR SYNC OVERVIEW

This section only applies to the PARI Master.

To see a graphic presentation of the air synchronization in a system, select **DECT Sync** > **Air Sync Overview**.

The internal synchronization for each region is shown separately by an expandable tree view, see Figure 8. The green, yellow and red dots in the sync tree show the following sync status for the Radios:

• Green: Synchronized
• Yellow: Synchronized but poor received signal strength (RSSI < -83 dBm)
• Red: Unsynchronized

The grey dot at top in the sync tree shows that it is a reference sync RFPI.

The FER value in the Sync tree is a long term calculation based on the active sync bearer.
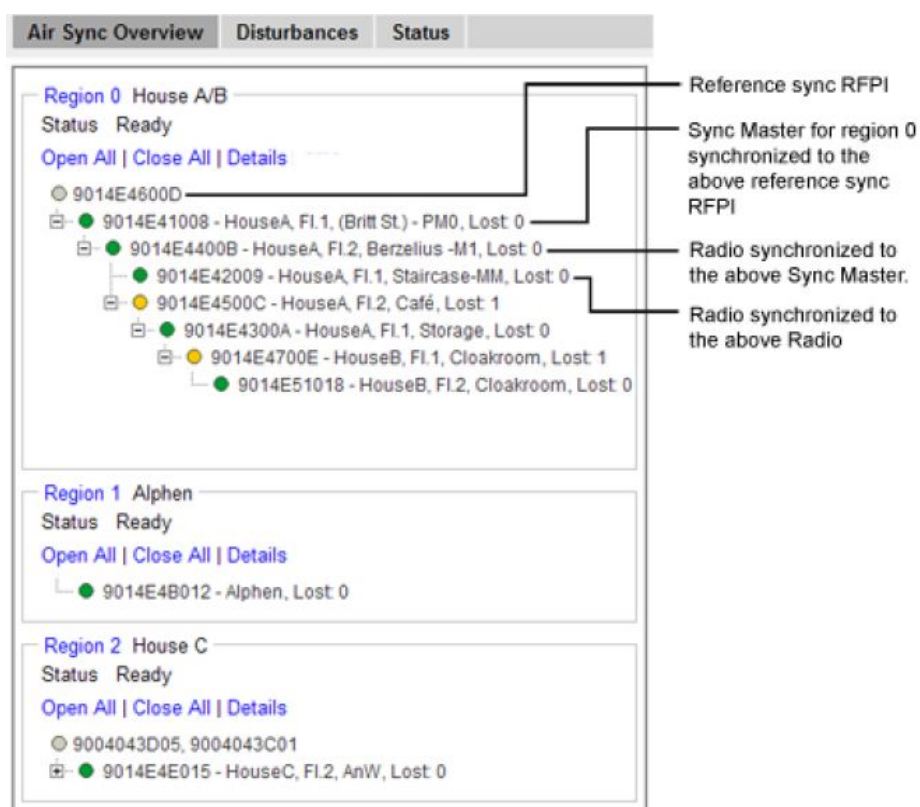
Figure 8. The sync trees for region 0, 1 and 2 where region 0 is fully expanded.

Region Details

1   Select **DECT Sync** > **Air Sync Overview**.

2   Click on the region ID text at top above the sync tree.

3   If this has not already been done: In the Region Details window, enter a name for the region.

4   In section Statistics, there are three counters:
- Calculations: Is incremented each time the sync tree is calculated.
- Configurations: Is incremented when an IPBS has received a new sync instruction.
- *Sync Lost*: Is incremented when an IPBS stops to handle radio traffic for a while and after that restarts the synchronization procedure.

5   Click **Clear** to clear the counters.

Reference Synchronization

To get the Sync Master to resynchronize to the reference sync, do as follows:

1   Select **DECT Sync** > **Air Sync Overview**.

2   Click on the region ID text at top above the sync tree.

3   In the Region Details window, click **Start.** When resynchronizing, all ongoing calls in the region will be disconnected.

IPBS Details

1   Select **DECT Sync** > **Air Sync Overview**.

2   Click on the **Details** text link above the sync tree. The sync tree will now display name and sync lost counter for the IPBSs in the region. The sync lost counter is a counter that is incremented when the IPBS stops to handle radio traffic for a while and after that restarts the synchronization procedure.

3   Hover over an IPBS with the mouse pointer for the pop-up mouse-over window. The pop-up window shows a list of sync candidates with corresponding RSSI and FER values.

The FER value in the pop-up window is a long term calculation based on the average of all the alternative sync bearers of the candidate.

4.12.2 DISTURBANCES

This section only applies to the PARI Master.

1   Select **DECT Sync** > **Disturbances**.

2   Click **Start.**

A list of potential disturbances is shown, that is, alien DECT systems that have a higher signal strength than the current sync signal.

4.12.3 STATUS

Air Sync status is displayed in the DECT Sync > Status menu. For explanation on the information shown for the active and the alternative sync bearers, see the table below.

Sync offset	Adjustment of frequency in progress performed by the current IPBS so it can be in synchronization with the synch source.
Drift	The time difference between the current IPBS and its sync source.

Sync lost counter	A counter that is incremented when the IPBS stops to handle radio traffic for a while and after that restarts the synchronization procedure.
RFPI	Radio Fixed Part Identity is the Id number of the sync bearer.
Carrier	The carrier used for air synchronization
Slot	The slot used for air synchronization
Hop	The number of hops from the Sync Master to the sync bearer
RSSI	Received Signal Strength Indication
FER	Frame Error Rate, a value between 0 and 100%. For a good synchronization the FER should be 0. It is OK to occasionally have a high FER, but only for short periods (up to one minute).

4.13 TRAFFIC

Traffic information is displayed in the Traffic sub menu. For the Master the traffic information for the IP-DECT system is displayed as well as traffic information for the Radio itself (if this Radio is enabled).

4.13.1 DISPLAY ALL ONGOING CALLS IN THE SYSTEM

All ongoing calls in the IP-DECT system can be displayed by selecting Traffic > Master Calls in the Master. See the table below for information about the different statistics fields.

Master	
Calls In	The total number of incoming calls to the Master.
Calls In Delivered	The number of connected incoming calls in the Master.
Calls Out	The number of outgoing calls from the Master.
Handover	The number of handovers in the Master.
Handover Cancelled	The number of cancelled handovers in the Master. Occurs when the handset decides to stay on the original Base Station.
Abnormal Call Release	The number of abnormal call terminations. A call release can occur if for example the user leaves the system's coverage area. To analyze the events, select Diagnostics > Events. To analyze how calls are connected and disconnected, select Diagnostics > Logging and select the *DECT Master* check box.
Busy Hour Call Attempts	The number of calls under the busiest hour counting from when pressing the Clear button.
Busiest hour start time	The start time of the busiest hour counter which was started when pressing the Clear button.

4.13.2 DISPLAY CALLS

All calls on an IPBS can be displayed by selecting Traffic > Radio Calls. See the table below for information about the different statistics fields.

Radio	
Calls In	The number of incoming calls to the Radio.
Calls Out	The number of outgoing calls from the Radio.
Handover	The number of handovers in the Radio.
Handover Cancelled	The number of failed handovers in the Radio. NOTE: There can be several reasons for uncompleted handovers occurring. This will in most cases not cause dropped or disconnected calls.

4.13.3 HANDOVER

During call, all ongoing handovers in the IP-DECT system can be displayed by selecting **Traffic** > **Handover in the Master**.

4.14 SOFTWARE UPGRADE

The RFP version information is not displayed in the IPBS2 GUI. RFP software is more integrated now and this information becomes obsolete. In IPBS1 the RFP software has a separate flash memory, but this is not the case for IPBS2. On the IPBS1 the RFP version is still displayed.]

4.14.1 BEFORE UPGRADING

1   For safety, take a backup of the configuration parameters for the Master and Standby Master.

2   Make a note of the Master and Standby Master IP address. On the device configured as Master, continue with step 3 to 5 below.

3   When upgrading from software version 2.X.X to later: Select **DECT** > **SMS** and make a note of the CPDM3/WSM3 IP address.

4   When upgrading from software version 2.X.X to later, select **DECT** > **Master** and make a note of the SIP proxy (registrar) IP address, found in the **Gatekeeper IP Address** text field.

5   When upgrading from software version 2.X.X to later: Select **DECT** > **Master** and make a note of the alternative SIP proxy (registrar) IP address, found in the **Alt. Gatekeeper IP Address** text field.

4.14.2 UPGRADING SEQUENCE

1   Upgrade firmware and boot file of Standby Mobility Master, see 4.14.3 *Software Upgrade from 2.X.X* on page 113 and 4.14.4 *Software Upgrade* on page 113.

2   Upgrade firmware and boot file of Mobility Master, see 4.14.3 *Software Upgrade from 2.X.X* on page 113 and 4.14.4 *Software Upgrade* on page 113

3   Upgrade firmware and boot file of Radios, see 4.14.3 *Software Upgrade from 2.X.X* on page 113 and 4.14.4 *Software Upgrade* on page 113

When upgrading from software version 2.X.X to later: Update configuration of Radios, 4.14.5 *Configuration After Updating the Firmware From Software Version 2.X.X to Later* on page 114.

4   Upgrade firmware and boot file of Standby Master, see 4.14.3 *Software Upgrade from 2.X.X* on page 113 and 4.14.4 *Software Upgrade* on page 113.

When upgrading from software version 2.X.X to later: Update configuration of Standby Master, see 4.14.5 *Configuration After Updating the Firmware From Software Version 2.X.X to Later* on page 114.

When upgrading from software version 3.X.X to later: Update configuration of Standby Master, see 4.14.6 *Configuration After Updating the Firmware From Software Version 3.X.X to Later* on page 114.

5   Upgrade firmware and boot file of Master, see 4.14.3 *Software Upgrade from 2.X.X* on page 113 and 4.14.4 *Software Upgrade* on page 113.

When upgrading from software version 2.X.X to later: Update configuration of Master, see 4.14.5 *Configuration After Updating the Firmware From Software Version 2.X.X to Later* on page 114.

When upgrading from software version 3.X.X to later: Update configuration of Master, see 4.14.6 *Configuration After Updating the Firmware From Software Version 3.X.X to Later* on page 114.

4.14.3 SOFTWARE UPGRADE FROM 2.X.X

1   When upgrading from software version 2.X.X to later: Disable LDAP replication for all Radios except in the case of Standby Master to Master Replication. Select **LDAP** > **Replicator** and make sure that the Enable check box is not selected.

2   When upgrading from software version 2.X.X to later: Update the firmware to 2.4.0 or later 2.X.X. See 4.22.2 *Update Firmware* on page 118 for more information on how to update the firmware.

3   Reset in order to make the changes take effect, see 4.29 Reset.

4   Update the firmware to 3.4.12. See 4.22.2 *Update Firmware* on page 118 for more information on how to update the firmware.

5   Reset in order to make the changes take effect, see 4.29 Reset.

6   Update the boot file to 3.0.26. See 4.23.3 Update the Boot File for more information on how to update the boot file.

7   Reset in order to make the changes take effect, see 4.29 Reset.

8   To update the IPBS Web GUI, press CTRL+F5 on the keyboard or close the IPBS Web GUI and start it again in order to update the GUI.

9   Continue with 4.14.4 *Software Upgrade* on page 113.

4.14.4 SOFTWARE UPGRADE

1   Update the firmware to the latest. See 4.22.2 *Update Firmware* on page 118 for more information on how to update the firmware.

2   Update the boot file to the latest. See 4.22.3 *Update the Boot File* on page 118 for more information on how to update the boot file.

3   Reset in order to make the changes take effect, see 4.28 *Reset* on page 125.

4   To update the IPBS Web GUI, press **CTRL+F5** on the keyboard or close the
       IPBS Web GUI and start it again in order to update the GUI.

4.14.5 CONFIGURATION AFTER UPDATING THE FIRMWARE FROM SOFTWARE VERSION 2.X.X TO LATER

The following configuration settings should be changed in the Web GUI after updating
the firmware from version 2.X.X to later.

Radio Configuration

1   Select **DECT** > Radio and enter the name and password for the Pari Master.

2   Reset in order to make the changes take effect, see 4.28 *Reset* on page 125.

Master/Standby Master Configuration

For both Master and Standby Master, do as follows:

1   If the Radio is activated, select **DECT** > **Radio** and enter the name and
       password for the Pari Master in the **Name** and **Password** text fields.

2   For Standby Master only: Enter the address to the Master in the **Primary Master
       IP Address** text field.

3   Select **UNITE** > **SMS** and enter the address to the CPDM3/WSM3 in the **IP
       Address** text field.

4   Select **DECT** > **Master**.

5   Select the **Enable Pari function** check box.

       If SIP/UDP, SIP/TCP or SIP/TLS protocol is used, continue with step 6 to 11
       below.

6   Enter the IP address to the SIP proxy (registrar) in the **Proxy** text field.

7   Enter the IP address to the alternative SIP proxy (registrar) in the **Alt. Proxy** text
       field.

8   Select the **Enbloc Dialing** check box.

9   Select the **Allow DTMF through RTP** check box.

10   Select the **Register with number** check box.

11   To update the Web GUI, press **CTRL+F5** on the keyboard or close the Web GUI
       and start it again in order to make the new menu to appear.

12   If H.323 protocol is used: Enter the address to the gatekeeper in the **Gatekeeper
       IP Address** text field.

13   Reset in order to make the changes take effect, see see 4.28 *Reset* on page
       125.

4.14.6 CONFIGURATION AFTER UPDATING THE FIRMWARE FROM SOFTWARE VERSION 3.X.X TO LATER

Master/Standby Master Configuration

When upgrading from version 3.X.X to later the MWI will automatically be set to Off. If
the MWI was enabled prior to the upgrade: Select **DECT** > **Suppl. Serv**. and select an
MWI mode in the **MWI Mode** drop-down list.

When upgrading a system from software version 3.X.X to later, existing system administration accounts remain configured locally in the IPBS(s). However, it is recommended that the system administration accounts are configured centrally instead by moving them to the Kerberos server. To have the system administration accounts configured locally is a potential security risk. For information on how to configure Kerberos, see 4.1.8 *Centralized Management of Administrator and Auditor Accounts Using Kerberos* on page 36.

To move the system administration accounts to the Kerberos server, do as follows:

1   For each IPBS where system administration accounts have been configured locally, do as follows:

   • Select **General** > **Admin**.
   • Go to the **Additional Administrator and Auditor Accounts** section.
   • Write down each accounts configuration data such as the user name, password (when known) and role.

2   On the Kerberos server, do as follows:

   • Select **General** > **Kerberos** Server.
   • Go to the **Users** section and enter the configuration data for each account that was written down in step 1 above.
   • Click **OK**.

3   For each IPBS where system administration accounts have been configured locally, do as follows to delete the local system administration accounts:

   • Select **General** > **Admin**.
   • Go to the **Additional Administrator and Auditor Accounts** section.
   • For each account row, select the **Delete** check box.
   • Click **OK**.

All local system administration accounts are deleted and the Additional Administrator and the Auditor Accounts section is no longer visible. The system administration accounts are now instead configured centrally on the Kerberos server.

4.15 SYSTEM UPGRADE FROM SOFTWARE VERSION 4.X.X TO 7.0.X

Radios with software version 4.X.X will not be able to connect to a Pari Master with software version 7.0.X. It is therefore recommended when doing a manual upgrade (i.e. when not using an update server) to upgrade Radios first and then the Pari Master.

4.16 SYSTEM UPGRADE FROM SOFTWARE VERSION 6.0.X TO 6.1.X - 7.0.X

When upgrading, the supplementary service codes *23* and #23 will be captured by the IP-DECT supplementary services and will not be forwarded to a PBX unless "OK" is pressed on the supplementary services page after upgrade.

After upgrade, do as follows.

1   Select **DECT** > **Supp. Serv**.

2   Click **OK**.

4.17 SYSTEM UPGRADE FROM SOFTWARE VERSION 7.0.X OR EARLIER TO 7.1.X

When upgrading an IP-DECT Base Station that have no LLDP (Link Layer Discovery Protocol) support to a version with LLDP support, extra care has to be taken in an IP network which sends VLAN configuration through LLDP. A Base Station which is upgraded to a version with an active LLDP support will change its VLAN configuration upon upgrade and might become unreachable.

LLDP functionality has been gradually introduced for certain hardware in IP-DECT 6.1.X to 7.0.X and has been activated for all hardware combinations in 7.1.X. To see if a Base Station have LLDP support, search for "LLDP" under "Diagnostics > Config show". If "LLDP" is found, then there is LLDP support. To see if LLDP is activated or not, look for the "/disable" flag on this configuration line.

4.17.1 UPGRADING

When upgrading an IP-DECT Base Station from a version without LLDP support to a version with LLDP support in a network that propagates VLAN settings, follow one of the two instructions below depending on which version the Base Station is upgraded to.

Upgrading to 7.X.X

1   Disable VLAN configuration over LLDP for the network or move the Base Station to a network without VLAN configuration over LLDP.

2   Upgrade the Base Station.

3   Disable LLDP for the Base Station with these HTTP commands:
!config add LLDP0 /disable
!config write
!reset

4   Enable VLAN configuration on the network again or move the Base Station back.

Note: If there is a need to activate LLDP for the Base Station again, use the following HTTP command: **!config rem LLDP0 /disable.**

Upgrading to 8.0.X or later

1   Disable VLAN configuration over LLDP for the network or move the Base Station to a network without VLAN configuration over LLDP.

2   Upgrade the Base Station.

3   Select **LAN** > **LLDP**.

4   Select the **Disable** check box.

5   Click **OK**.

6   Enable VLAN configuration on the network again or move the Base Station back.

7   If there is a need to activate LLDP for the Base Station again, deselect the **Disable** check box (**LAN** > **LLDP**).

4.18 SYSTEM DOWNGRADE FOR IPBS2/IPBS4X2

This section applies only to IPBS2 with the following article numbers that can be found on the label on the backside of the device:

- **IPBS2-**A**

Note: When downloading, minimum version of the software that runs on IPBS2 is 7.2.11.

4.19 SYSTEM DOWNGRADE FROM SOFTWARE VERSION 7.0.X

Downgrade has to be done in several steps:

1   Take a configuration backup of at least all the central modules, e.g. Master, Mobility Master, Crypto Master etc. For information about how to backup, see 4.14 *Backup* on page 120.

2   Downgrade complete system to version "ToPreV7". This firmware will convert the database. The conversion only takes a few seconds and it is ready when the message "VARS compression completed" is shown on the General > Info page.

3   Downgrade to desired version.

4.20 SYSTEM DOWNGRADE TO SOFTWARE VERSION 2.X.X

After downgrading: The LDAP replication must be activated again.

1   Select **LDAP** > **Replicator.**
2   Select the **Enable** check box to activate LDAP replication.
3   Check the MWI settings.

4.21 SYSTEM DOWNGRADE TO SOFTWARE VERSION 4.X.X AND 3.X.X

After downgrading: Check the MWI settings.

4.22 UPDATE

This section describes how to do the following configurations and settings.

- Update Configuration
- Update Firmware
- Update the Boot File

4.22.1 UPDATE CONFIGURATION

A previously saved configuration can be loaded and activated on the IPBS. See
4.14 *Backup* on page 120 for information on how to save a configuration.

1   Select **Update** > **Config**.

2   Click **Browse...** and browse to the saved configuration.

3   Click **Upload**.

4   Reset in order to make the changes take effect, see 4.28 *Reset* on page 125.

Considerations when updating of configuration

Configuration files are only fully compatible if the backup and restore are done on
products that have CPUs with the same endianess. IPBS1/IPBS4x0 has "big-endian"
CPUs compared to IPBS2/IPBS4x2 which have "little-endian" CPU. Hence, IPBS1/
IPBS4x0 and IPBS2/IPBS4x2 configurations are not compatible.

If a device (e.g. IPBS2/IPBS4x2) is configured and the configuration is taken from
another type of device (e.g. IPBS1/IPBS4x0), some lines in the configuration will be
skipped by the configured device (IPBS2/IPBS4x2). This is because devices of
different types do not have the same hardware and some configuration lines are
therefore not applicable in the configured device (IPBS2/IPBS4x2).

When upgrading an IP-DECT system where IPBS1/IPBS4x0 is replaced with IPBS2/
IPBS4x2s and the backup file of the IPBS1/IPBS4x0 configuration is installed on the
IPBS2/IPBS4x2, the severity level on alarms and events listed in the configuration file
will be changed in the IPBS2/IPBS4x2. For information on how to change the severity
level on alarms and events, see 4.8.5 *Module Fault List* on page 93.

4.22.2 UPDATE FIRMWARE

Updated software files are distributed by your supplier.

There are three ways to update the firmware:

*   Using an update server, see Appendix A: *How to Configure and Use the Update
    Server* on page 137.
*   Using a Device Manager.
    To setup a connection to a Device Manager, see 4.8.2 *Device Management* on page
    92. To update the firmware using a Device Manager, see the Installation and
    Operation Manual for CPDM3/WSM3.
*   Manual update, see below.

To update manually:

1   Select **Update** > **Firmware**.

2   Click **Browse...** and browse to the firmware file.

3   Click **Upload**

4   Reset in order to make the changes take effect, see 4.28 *Reset* on page 125.

4.22.3 UPDATE THE BOOT FILE

Updated software files are distributed by your supplier.

There are three ways to update the boot file:

- Using an update server, see Appendix A: *How to Configure and Use the Update Server* on page 137.
- Using a Device Manager.
  To setup a connection to a Device Manager, see 4.8.2 *Device Management* on page 92. To update the boot file using a Device Manager, see the Installation and Operation Manual for CPDM3/WSM3.
- Manual update, see below.

To update manually:

1   Select **Update** > **Boot**.

2   Click **Browse...** and browse to the boot file.

3   Click **Upload**.

4   Reset in order to make the changes take effect, see 4.28 *Reset* on page 125.

4.23 SYSTEM UPGRADE IN SYSTEM WITH MOBILITY MASTERS

Upgrade in the following order:

1   Upgrade all Standby Mobility Masters.

2   Upgrade all Mobility Masters.

3   Upgrade all of the remaining devices for each site by following the upgrade sequence under 4.15.2 *Upgrading Sequence* on page 120.
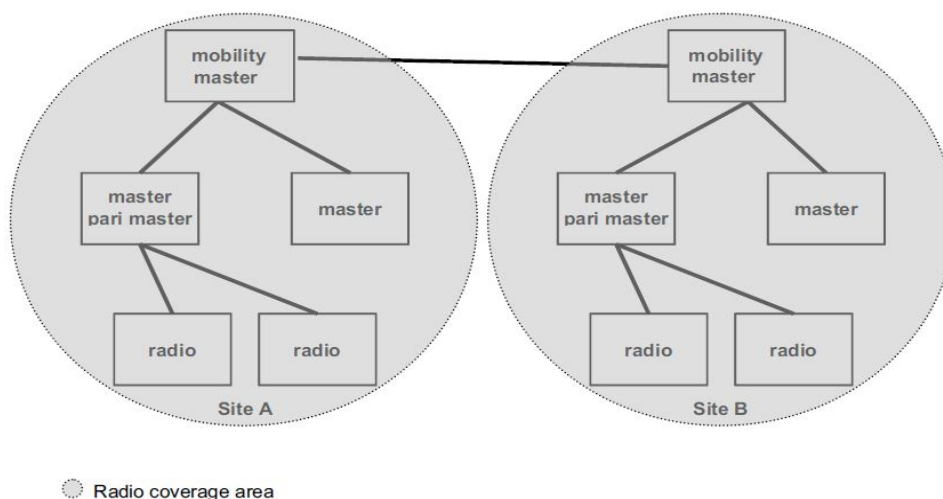
Figure 9. System with several Mobility Masters

Note: Roaming between sites is only possible when the sites have the same software version.

4.24 REPLACING MASTER HARDWARE IN MULTIPLE MASTER SYSTEM

If a faulty Master IPBS is replaced with a new one, then the faulty Master must have been disconnected from the system more than 2 minutes before the new Master is connected, otherwise all the subscription data will be lost when connecting the new Master:

1   Disconnect the faulty Master.

2   Wait at least 2 minutes.

3   On the Mobility Master, select Device Overview > Masters and delete the faulty Master.

4   Connect the new Master and upload the configuration from the faulty Master. For information on how to upload a configuration on the new Master, see 4.22.1 *Update Configuration* on page 118.

4.25 REPLACING MASTER HARDWARE IN A SYSTEM WITH A CRYPTO MASTER ACTIVE

If a faulty Master is replaced with a new one, then the faulty Master must be deleted in the Mobility Master. The reason for deleting the replaced Master is that the Crypto Master is operable only if all Masters, part of the Crypto Master hierarchy, are connected.

4.26 REPLACING MOBILITY MASTER HARDWARE IN A SYSTEM WITH A CRYPTO MASTER ACTIVE

If a faulty Mobility Master is replaced with a new one, then the faulty Mobility Master must be deleted in the Crypto Master. The reason for deleting the replaced Mobility Master is that the Crypto Master is operable only if all Mobility Masters, part of the Crypto Master hierarchy, are connected.

4.27 DIAGNOSTICS

4.27.1 LOGGING

The IPBS can generate a number of logs which can be useful when supervising and troubleshooting the IP-DECT system. For information on how to collect the log files, see 4.9.2 *Configure Logging* on page 94. For a description of each log, see the table below.

Setting	Description
TCP	Logs generated upon TCP connection set-ups in the H.225 / H.245 protocol.
Gateway Calls	Logs generated by calls that go through the gateway interface.

Gateway Routing	Logs generated by calls that are routed through the gateway interface.
H.323 Registrations	Logs generated upon RAS registration.
H.323/TCP Registrations	Logs generated upon RAS registration.
H.323/TLS Registrations	Logs generated upon RAS registration
SIP/UDP Registrations	Logs generated upon SIP registration.
SIP/TCP Registrations	Logs generated upon SIP registration.
SIP/TLS Registrations	Logs generated upon SIP registration.
DECT Master	Logs generated by the Master software component in the IPBS.
DECT Radio	Logs generated by the Radio software component in the IPBS.
DECT Stack	A low level DECT log, intended for support departments.
Config Changes	Logs generated upon configuration changes in the IPBS or the IP-DECT system.
Radio is busy for speech	Enable if a fault event should be sent when all speech resources are busy.

1   Select Diagnostics > Logging.

2   Select which logs to generate by selecting the check box next to the log name.

3   Click "OK".

4   View the logs by clicking the "syslog" link. The logs are updated in real-time.

4.27.2 TRACING

The information gathered from the trace functionality is mainly used for troubleshooting in case of failure in the system. The trace information is intended for the support departments.

It is possible to trace traffic information on the LAN for troubleshooting purposes.

1   Select **Diagnostics** > **Tracing**.

2   Select the **Enable** check box in the **Remote PCAP** section to enable the use of a network protocol analyzer program, for example Wireshark.

  The **Trace** check box in the **Remote PCAP** section is mainly used by the R&D department to follow the desired network attributes.

3   Select the **TCP/UDP Traffic** check box in the IP section to capture traffic information.

4   Click **OK**.

4.27.3 ALARMS

Under Diagnostics > Alarms are all active alarms displayed.

An alarm is a fault that affects the normal service of the IP-DECT system and may require action from personnel to correct it. An IP-DECT Master can collect alarms from Radios and it can display all active alarms in the system. If an object is removed from the system, object-related alarms are automatically cleared after a timeout period of 30 minutes. Active alarms are also cleared if the related object is restarted.

For a description of the attributes, see the table below.

Attribute	Description
Time	The date and time when the alarm is issued.
Code	A unique number that identifies the alarm. Click the code to get more detailed information about the alarm. For a list of possible codes and their descriptions, see 6.2 *Fault Code Descriptions* on page 129.
Severity	It has three possible states: • Critical - Immediate action is required. It is displayed, for example, if a managed object goes out of service. • Major - Urgent action is required. It is displayed, for example, if the capability of the managed object is severely degraded. • Indeterminate - Level of severity cannot be determined
Remote	The IP Address of the object that reported the alarm. Click the IP address to access the object.
Source	The software module that reported the alarm. Together with the code it uniquely identifies an alarm.
Description	A textual description of the alarm.

4.27.4 EVENTS

Under Diagnostics > Events is history of alarms and errors displayed including active alarms. Click "Clear" in the top-right corner to clear the list of alarms and errors.

For a description of the attributes, see the table below.

Attribute	Description
Time	The date and time when the alarm, error is issued or cleared.
Type	The status of the fault. It has four possible states: • Alarm - Alarms displayed in red are active alarms • Alarm cleared - The alarm is already cleared • Alarm timeout - The alarm exceeded the timeout period • Error - Refers to faults that are not active for a specific time.
Code	A unique number that identifies the alarm. Click the code to get more detailed information about the alarm. For a list of possible codes and their descriptions, see 6.2 *Fault Code Descriptions* on page 129.

Severity	It has three possible states: • Critical - Immediate action is required. It is displayed, for example, if a managed object goes out of service. • Major - Urgent action is required. It is displayed, for example, if the capability of the managed object is severely degraded. • Indeterminate - Level of severity cannot be determined
Remote	The IP Address of the object that reported the alarm. Click the IP address to access the object.
Source	The software module that reported the alarm. Together with the code it uniquely identifies an alarm.
Description	A textual description of the alarm.

4.27.5 PERFORMANCE

It is possible to check different performance parameters. For a description of the parameters, see the table below.

Parameter	Description
CPU	Shows CPU utilization. To have a 100% utilization for a longer time is not good but occasional peaks are acceptable. Reason for high utilization may be caused by running SRTP. Another reason may be that there are a lot of users registered on the Master.
CPU-R	Shows utilization of CPU resources allocated by different tasks. If the CPU resources are fully utilized it will prevent connection of more calls. One solution in that case can be to install an additional Base Station in the same coverage area.
MEM	Shows utilization of the RAM memory. If the utilization is continuously and significantly increasing then it can be due to memory leakage. It can also be due to a large number of simultaneous ongoing events. Another reason can be that a Base Station has to much to handle and a solution can be to divide the roles of Pari Master, Radio, and so on. on several Base Stations. The displayed utilization curve will never decrease as it shows the amount of memory that has been dedicated to a specific memory pool. Within each memory pool it can still be reused.

ETH0	Shows the traffic on the Base Station's Ethernet interface.
Concurrent calls	Shows the number of simultaneous ongoing calls on the Base Station's air interface. Maximum number of calls that can be handled simultaneous in air is 8. If the number of concurrent calls is 8 for a longer time, a solution could be to add an additional Base Station to the system.

1   Select **Diagnostics** > **Performance**

2   Select the check box(es) for the desired performance statistics.

3   Click **OK**.

4   One window shows statistics for the last 24 hours. The maximum possible value is displayed in the top-left corner. Click the left or right arrow buttons to see different time frames.

4.27.6 CONFIG SHOW

Under **Diagnostics** > **Config Show**, the configuration is displayed as a text output.

4.27.7 PING

The ping function is used to determine the response time from the IPBS to a certain IP address. It can be used to analyse the connection between the IP-DECT system components.

There are two ways to activate a ping function

Automatic pings (one or two IP addresses with individual time intervals)

1   Select **Diagnostics** > **Ping**.

2   Enter the IP addresses in the text fields under **Destination**.

3   Enter the time intervals in the text fields under **Interval (secs)**.

4   Click **OK**

5   To view the result, click **Performance** in the top menu and select **PING1** and **PING2**.

Ping (a ping is immediately sent to an IP address)

1   Select **Diagnostics** > **Ping**.

2   Enter an IP address in the **IP address** text field.

3   Click **Start**.

4.27.8 TRACEROUTE

The traceroute function displays how packets travel from the IPBS to a certain IP address. The result is an ordered list of IP addresses with the measured round trip time.

1   Select **Diagnostics** > **Traceroute**.

2   Enter an IP address in the **IP Address** text field.

3   Press **Enter** on the keyboard.

4.27.9 RFP SCAN

To scan for occupied system IDs of other IP-DECT systems within the coverage area, perform an RFP scan following the steps below.

Note: Executing an RFP scan will terminate all calls on the IPBS.

1   Select **Diagostics** > **RFP Scan**

2   Click **Start Scanning**.

4.27.10 SERVICE REPORT

To download a service report do the following:

1   Select **Diagnostics** > **Service Report**.

2   Click **download**.

3   Click **Save** and browse where to save the service report.

4.28 RESET

Some configuration changes requires a reset in order to take effect. A reset reboots the software. There are two ways to perform a reset:

- Idle reset - waits until there are no active calls in the IPBS.
- Immediate reset - clears all calls and resets the IPBS.

4.28.1 IDLE RESET

1   Select **Reset** > **Idle Reset.**

2   Click **OK**.

3   The IPBS will reset when there are no active calls.

4.28.2 IMMEDIATE RESET

1   Select **Reset** > **Reset**.

2   Click **OK**.

3   The IPBS will terminate all active calls and reset.

4.28.3 TFTP MODE

Note: When the IPBS is in TFTP mode it can only be reached using the *gwload* utility. This mode should not be used during normal operation.

4.28.4 BOOT

When the IPBS is in Boot mode it uses a small version of the firmware (minifirmware) which contains only the IP stack and the web interface.

1   Select **Reset** > **Boot**.

2   Click **OK**.

4.29 RESET USING THE RESET BUTTON

It is possible to do a hardware reset of the IPBS by pressing the reset button. The button is accessed through a hole in the back of the IPBS. See the applicable Installation Guide for the IPBS.

Note: Use a pointed object in an non conducting material to perform a reset.

Short press < 1 sec	Restart
Medium press ~3 sec. For IPBS2: When 3 sec. has gone, the LED on IPBS2 will start to flash in blue and the reset button can then be released.	Restart in TFTP mode. In TFTP mode the IPBS can be accessed only through the gwload application. This mode is intended for support and development departments.
Long press ~ 10 sec. For IPBS2: When 10 sec. has gone, the LED on IPBS2 will start to flash in blue, indicating the start of the factory reset process. Hence the reset button can then be released. When the LED (LED 1 for IPBS1) is steady amber/yellow, the factory reset process is complete. The device can now be restarted by disconnecting the supply voltage.	Factory reset - all configuration parameters will be set to default values.

5   COMMISSIONING

This section describes the visual inspection and tests that must be executed after completing the installation and initialization of the IP-DECT system. The purpose of the visual inspection and tests is to verify that all installation activities have resulted in a correctly functioning system. If it appears that a part is malfunctioning while the system is installed correctly (that is, no cabling faults, no configuration faults), the technician must consult the maintenance section included in this manual for fault finding.

5.1   RADIO COVERAGE VERIFICATION TESTS

The radio coverage verification consists of two tests:

• Base station operation test
• Coverage area test

Note: Be sure that all batteries in the handset are charged before executing the tests.

5.1.1   BASE STATION OPERATION TEST

The purpose of this test is to check if all base stations are operational.

1   Put a handset in the service display mode (DCA mode), see applicable User Manual for the handset.

2   Use the base station plan, see the applicable System Planning documentation for IP-DECT.

3   Move close to each base station and check that the handset locks to it (the service display should display the correct number).

After having checked that all base stations are operational proceed with the coverage area test.

5.1.2   COVERAGE AREA TEST

The purpose of this test is to verify that there is satisfactory field strength to enable good speech quality everywhere within the covered area (rooms, lift shafts, staircases). This test is executed with two handsets and requires two persons.

1   Place the handset in the service display mode (DCA mode) and call the other handset. One user of the handset should now start moving around the covered area. Both users must check that a good speech quality is maintained everywhere. Special attention should be paid to areas such as edges of the building and areas behind metal structures where there is a possibility of reduced speech quality.

2   Mark areas where cracking sounds or mutes are heard.

5.1.3   EVALUATION

After having performed the coverage area test, the results should be evaluated. If the coverage is not sufficient you should review the planning and move or add equipment.

5.2 CORDLESS EXTENSION NUMBER TEST

This test checks for each handset the complete connection from the IP-DECT system to the PBX. Furthermore it checks that the handsets' numbers have been correctly programmed. The test is performed by calling all handset from one specific handset.

1   Put all handset together in order of extension number on a table.

2   Go off-hook with each handset and check that the dial tone is heard.

3   Call with a handset (handset A) all other handsets sequentially and check that the handset with the corresponding number on its display rings when called.

4   Call handset A and check if it rings.

6 TROUBLESHOOTING

6.1 LOAD FIRMWARE USING THE GWLOAD TOOL

If the firmware is corrupt, for example if firmware download is interrupted the IPBS could become unreachable by the web GUI. It will not be possible to load new firmware or to start correctly. If this occurs, the IPBS runs on the bootcode and the Gwload tool (a tftp-style client used to repair a broken firmware) can be used to upload firmware.

1   Download the Gwload software from the IP-DECT system provider.

2   Set the IPBS in TFTP-mode by performing a medium (~3 sec) hardware reset, see 4.29 *Reset Using the Reset Button* on page 126.

3   Start a command window.

To update with wew firmware, execute the following command from the folder where the gwload.exe file is located:

IPBS:
gwload /setip /i <ipaddress> /gwtype 1201 /prot <..path/firmwarefilename> /go

4   If there is more than one IPBS in TFTP mode, select the unit to update and press enter.

6.2 FAULT CODE DESCRIPTIONS

This section lists the possible fault codes, their description and severity level.

Explanation of the table columns **C**, **M** and **I**:

C = Critical (IP-DECT) / Critical (Unite)
M = Major (IP-DECT) / Error (Unite)
I = Indeterminate (IP-DECT) / Warning (Unite)

Description	Code	Device	C	M	I
Interface down (Gateway) This is an alarm which is generated, if an physical interface which is configured to be up gets down.	0x00010001	IPBS		X	
Registration down (Gateway) This is an alarm which is generated if an configured outgoing registration is down.	0x00010002	IPBS		X	
Protocol error (Gateway) The gateway process receive a call clearing with cause code 'Protocol Error'. This can be an indication for an interop problem with some other equipment.	0x00010003	IPBS		X	
The LDAP replicator is not connected (Users)	0x00030001	IPBS		X	
CPU resources are not available (Radio)	0x00030101	IPBS			X
Standby master active (Master)	0x00030201	IPBS		X	
User registration failure (Master)	0x00030202	IPBS		X	
Emergency registration down (Master)	0x00030203	IPBS		X	

Connection to Radio lost (Master)	0x00030204	IPBS		X	
Primary/redundant trunk is down (Master)	0x00030205	IPBS		X	
Master active (Master) This event is generated when the Mirror becomes active.	0x00030206	IPBS			X
Master inactive (Master) This event is generated when the Mirror becomes inactive.	0x00030207	IPBS			X
Limit of static radios is reached (Master) This is an alarm which is generated when the number of radios in the radios list (Device Overview > Radios) is reaching 2100. The alarm is cleared once the number of radios goes below 2100.	0x00030208	IPBS		X	
Abnormal call release (Master) This event is generated when a call is released abnormally.	0x00030210	IPBS			X
Connection to Mobility Master lost (Mobility Master)	0x00030301	IPBS		X	
Cannot establish connection to Mobility Master (Mobility Master)	0x00030302	IPBS		X	
Connection to Master lost (Mobility Master)	0x00030303	IPBS		X	
Standby Mobility Master is active (Mobility Master)	0x00030304	IPBS		X	
Connection to Mobility Master lost (Crypto Master)	0x00030401	IPBS		X	
No Media data received (RTP) No RTP packets from remote side were received on a connected call. This points to either a NAT problem (private RTP address was given to remote side) or a general signalling problem (media negotiation).	0x00050001	IPBS		X	
Excessive loss of data (RTP) This event is generated if in a period of 10s more than 3% received RTP packets were lost. This is an indication of a network problem and it is recommended to check the involved media IP addresses and what kind of device that is involved.	0x00050002	IPBS		X	
Wrong payload type received (RTP) Caused by signalling/negotiation problems (interoperability). An endpoint sends RTP packets with a payload type other than negotiated. Wrong Payload Type is a message if there is a Media Problem with a another PBX.	0x00050003	IPBS		X	
Stun failed (RTP)	0x00050004	IPBS		X	
SRTP authentication failed (RTP)	0x00050005	IPBS		X	
SRTCP authentication failed (RTP)	0x00050006	IPBS		X	
ICE failed (RTP)	0x00050008	IPBS		X	

DTLS failed (RTP)	0x00050009	IPBS		X	
Unexpected message (H323) A message was received, which was not expected by the protocol in this state. This could be caused by network problems or by incompatible equipment.	0x00060001	IPBS		X	
Status inquiry (H323)	0x00060002	IPBS		X	
Signalling TCP failed (H323) The signalling transport connection could not be established. This usually means, the destination (IP) is not reachable. Check network connectivity.	0x00060003	IPBS		X	
Signalling time out (H323) A signalling timer expired. The reason for this could be a network problem or an interop problem.	0x00060004	IPBS		X	
SRTP key mismatch (H 323) The call signaling was aborted due to a mismatch of the SRTP key format.	0x00060005	IPBS		X	
Media incompatible (H 323)	0x00060006	IPBS		X	
NAT discovery failed (SIP)	0x00070001	IPBS		X	
Overload (SIP) The SIP protocol stack reached its build-in memory allocation limit. The total number message allocations is limited to be safe against denial-of-service attacks. Under normal working conditions the limit should not be reached.	0x00070003	IPBS		X	
Coder selection failed (SIP)	0x00070004	IPBS		X	
Media configuration failed (SIP)	0x00070005	IPBS		X	
DNS failed (SIP)	0x00070006	IPBS		X	
Internal error on media negotiation (SIP) Media negotiation failed which probably results in one-way audio.	0x00070007	IPBS		X	
DNS not working (SIP)	0x0007000b	IPBS		X	
Invalid URL (WebMedia)	0x00080001	IPBS		X	
Coder missing in URL (WebMedia)	0x00080002	IPBS		X	
Unexpected restart (watchdog/reset/power on) (Cmd) The system was restarted because of watchdog, trap or by pressing the reset button. This event is generated 60s after the restart.	0x000b0001	IPBS		X	
Unexpected message (TLS)	0x000c010a	IPBS			X
Unexpected message (TLS)	0x000c020a	IPBS			X
Bad MAC (TLS)	0x000c0114	IPBS			X
Bad MAC (TLS)	0x000c0214	IPBS			X
Decryption failed (TLS)	0x000c0115	IPBS			X
Decryption failed (TLS)	0x000c0215	IPBS			X

Record overflow (TLS)	0x000c0116	IPBS			X
Record overflow (TLS)	0x000c0216	IPBS			X
Decompression failure (TLS)	0x000c011e	IPBS			X
Decompression failure (TLS)	0x000c021e	IPBS			X
Handshake failure (TLS)	0x000c0128	IPBS			X
Handshake failure (TLS)	0x000c0228	IPBS			X
No certificate (TLS)	0x000c0129	IPBS			X
No certificate (TLS)	0x000c0229	IPBS			X
Bad certificate (TLS)	0x000c012a	IPBS			X
Bad certificate (TLS)	0x000c022a	IPBS			X
Unsupported certificate (TLS)	0x000c012b	IPBS			X
Unsupported certificate (TLS)	0x000c022b	IPBS			X
Revoced certificate (TLS)	0x000c012c	IPBS			X
Revoced certificate (TLS)	0x000c022c	IPBS			X
Expired certificate (TLS)	0x000c012d	IPBS			X
Expired certificate (TLS)	0x000c022d	IPBS			X
Unknown certificate (TLS)	0x000c012e	IPBS			X
Unknown certificate (TLS)	0x000c022e	IPBS			X
Illegal parameter (TLS)	0x000c012f	IPBS			X
Illegal parameter (TLS)	0x000c022f	IPBS			X
Unknown CA (TLS) A TLS connection could not be established because the CA of the remote certificate is not trusted. Check the rejected certificates for details.	0x000c0130	IPBS			X
Unknown CA (TLS) A TLS connection could not be established because the remote party does not trust the CA of the certificate of this device.	0x000c0230	IPBS			X
Access denied (TLS)	0x000c0131	IPBS			X
Access denied (TLS)	0x000c0231	IPBS			X
Decode error (TLS)	0x000c0132	IPBS			X
Decode error (TLS)	0x000c0232	IPBS			X
Decryption error (TLS)	0x000c0133	IPBS			X
Decryption error (TLS)	0x000c0233	IPBS			X
Export restriction (TLS)	0x000c013c	IPBS			X
Export restriction (TLS)	0x000c023c	IPBS			X
Protocol version (TLS)	0x000c0146	IPBS			X
Protocol version (TLS)	0x000c0246	IPBS			X
Insufficient security (TLS)	0x000c0147	IPBS			X
Insufficient security (TLS)	0x000c0247	IPBS			X
Internal error (TLS)	0x000c0150	IPBS			X
Internal error (TLS)	0x000c0250	IPBS			X
User cancelled (TLS)	0x000c015a	IPBS			X
User cancelled (TLS)	0x000c025a	IPBS			X

No renegotiation (TLS)	0x000c0164	IPBS			X
No renegotiation (TLS)	0x000c0264	IPBS			X
Service not found (Kerb client) The host account of the device has been deleted on the Kerberos server. Join the Kerberos realm again.	0x000c0403	IPBS		X	
Kerberos server unreachable (Kerb client) The device did not get a response from the Kerberos server. Make sure that the Kerberos server is up and its address is well configured on the devices.	0x000c0406	IPBS		X	
Kerberos cross realm failure (Kerb client) ***Kerberos: Cross-realm trust not configured:*** The user tried to log-in with a user account from a Kerberos realm that does not trust or is not trusted by the realm of the device. **Kerberos: Cross-realm password mismatch:** The password for the cross-realm trust is not the same on both of the Kerberos servers.	0x000c0407	IPBS		X	
Certificate validation is disabled until system time is set (X509) System time is not set but the current date is needed to validate if cryptographic certificates are valid. Therefore encrypted TLS connections will fail. Configure a NTP server or set the system time manually.	0x000c1000	IPBS			X
Certificate expired/Will expire soon (X509) The device certificate or one of the trusted certificates has already expired or will expire during the next 30 days. After the certificate has expired TLS connections using this certificate will fail. Replace the certificate with a new one.	0x000c1001	IPBS			X
RFP unsynchronized (RFPInit) Four common reasons: 1. The IPBS has lost contact for nine minutes with the RFPI used as synchronization source. 2. The IPBS is not PSCN synchronized (Primary Receiver Scan Carrier Number). 3. The IPBS is not MFN synchronized (Multiframe Number). 4. The IPBS is not slot number synchronized.	0x000e0005	IPBS		X	

Synchronization to reference system lost (RFPInit) Get the Sync Master to resynchronize to the reference sync either manually or automatically (scheduled). To select type of resynchronization action, see *Configure Sync Master IPBS* on page 88. To resynchronize manually, see *Reference Synchronization* on page 110.	0x000e0006	IPBS		X	
Other DECT system with same sysid detected (RFPInit)	0x000e0008	IPBS		X	
Sync master failed to resynchronize to reference (RFPInit)	0x000e0009	IPBS		X	
RFP restarted Burst mode controller of the IPBS restarted.	0x000e000a	IPBS		X	
Interface down (ipproc)	0x00110000	IPBS		X	
Interface not configured (ipproc)	0x00110001	IPBS			X
DHCP server not responding (ipproc)	0x00110002	IPBS		X	
Invalid UDP-RTP port base/range (ipproc)	0x00110019	IPBS		X	
Invalid UDP-NAT port base/range (ipproc)	0x0011001a	IPBS		X	
Invalid NAT port base/range (ipproc)	0x0011001b	IPBS		X	
ARP poisoning detected (ipproc)	0x00110041	IPBS		X	
Out of TCP/NAT ports (ipproc)	0x00110046	IPBS		X	
Out of TCP ports (ipproc)	0x00110047	IPBS		X	
TCP bind error (ipproc) Local error. TCP socket was trying to bind itself to a specific local port number. The port number was found to be in use by some other socket.	0x00110049	IPBS		X	
Out of UDP/RTP ports (ipproc)	0x00110050	IPBS		X	
Out of UDP ports (ipproc)	0x00110051	IPBS		X	
UDP bind error (ipproc) Local error. UDP socket was trying to bind itself to a specific local port number. The port number was found to be in use by some other socket.	0x00110053	IPBS		X	
No route to destination (ipproc)	0x0011005a	IPBS		X	

No route to destination, if down (ipproc) The IP routing process failed to deliver a packet explicitly directed to a specific network interface. The network interface was either down or disabled. Packets directed to a specific network interface are used for example by DHCP (UDP) and by PPTP Tunnels (TCP/GRE). If this error is reported for UDP broadcast packets rather often it usually indicates that DHCP client mode is configured for the interface but the interface is not connected to a network or disabled. In this case the DHCP mode should be changed to disabled.	0x0011005b	IPBS		X	
No route to destination, if unknown (ipproc)	0x0011005c	IPBS		X	
No route to destination, if unconfigured (ipproc)	0x0011005d	IPBS		X	
No route to destination, no gateway (ipproc)	0x0011005e	IPBS		X	
No route to destination, loop (ipproc)	0x0011005f	IPBS		X	
Memory Usage above 85% (box)	0x00120001	IPBS	X		
Radio busy for speech (Dect)	0x00140001	IPBS			X
Default encryption key timeout (Dect) Too long delay in the LAN/WAN network for early encryption to work. The problem can be solved by configuring a local Mobility Master. Even though a local Mobility Master is configured, the fault message will not disappear, i.e. it will be shown at first location registration attempt when the home Master must be reached. At the next location registration attempt, the key will be in the local Mobility Master and early encryption will work.	0x00140065	IPBS			X
Cipher timeout (Dect) This indicates that a call has been forcefully disconnected since the cipher option has been disabled in the radio.	0x00140066	IPBS		X	
Master connection timeout (Dect) A signaling timer expired. The reason for this could be a network problem between Radio and Master.	0x00140067	IPBS		X	
Failed to transfer Compact Unit communication block (Unite) Check that the Unite address is correct.	0x001a0001	IPBS			X
ICP Connection down	0x00200000	IPBS		X	
Read update script Failed to read script from update server.	0x00210001	IPBS		X	
Upload bootcode Failed to get the bootcode from update server.	0x00210002	IPBS		X	
Upload firmware Failed to get the firmware from update server.	0x00210003	IPBS		X	

Upload config Failed to get the config from update server.	0x00210004	IPBS		X	
Download config Failed to send the config to update server.	0x00210006	IPBS		X	

7 RELATED DOCUMENTS

System Description, IP-DECT System 52/1551-ANF 901 14 I

System Planning, IP-DECT System 51/1551-ANF 901 14

Installation Guide, Base Station 32/1531-ANF 901 43

Appendix A: How to Configure and Use the Update Server

A.1 Summary

Automatic update is based on configuration and firmware information stored on a standard web server and retrieved by the devices on a regular basis.

There are 2 modules in the device which work in tandem. The first is known as "UP0" and actually executes the upload and download of configuration information as well as the download of updated firmware. UP0 is controlled by commands as described below.

The second module is known as "UP1". It serves to poll a given website for changed configuration information. If certain conditions are met, UP1 will issue commands to UP0 to perform the requested updates.

UP0 can also receive commands from the "Update clients" page of the PBX Administration user interface.

A.1.1 System Requirements

One or more regular Web Server that can be accessed by all devices are required. This has been tested with Microsoft IIS and Apache, but any regular Web Server should do.

For best results, the Web Server should be able to maintain a large number of HTTP sessions simultaneously, since potentially all devices may attempt a configuration update at the same time. For example, Microsoft's Personal Web Server is not adequate, since it only support 10 simultaneous sessions.

Following URLs are supported: HTTP, HTTPS and TFTP.

A.1.2 Configuration in IP-DECT

See 4.9.1 *Configure Automatic Firmware Update* on page 94 on how to configure the IPBS for automatic update.

The URL parameter must point to the site where the file containing the commands is stored. Note that in this URL, no host names are supported. The web servers IP address must be used.

A.1.3 Setting the UP1 Parameters

If the URL ends with a '/' then a default filename is used based upon the product in question. If for example the URL for an IPBS1/IPBS4x0 is "http://1.2.3.4/configs/", it is expanded to "http://1.2.3.4/configs/update-IPBS.htm".

	Command filename
IPBS1/IPBS4x0	update-IPBS.htm
IPBS2/IPBS4x2	update-IPBS2.htm

The product type name used is the one used in the Version line on the devices Info page. Note that the extension is irrelevant, .htm or .txt or no extension at all may be used. On some Web servers, URLs are case sensitive.

The command file is retrieved initially after the configured poll interval (in minutes) is expired after boot. Short poll intervals can create substantial load on a big network. A value less than 15 minutes (which is the default) is therefore not recommended.

However, for new devices (that is, devices which have been reset to factory settings and never had a successful download of a command file), the command file is retrieved every minute (for up to 30 minutes). This is done so that a fresh device can quickly retrieve a site depending standard configuration when it is installed.

When the command file is retrieved, the commands found in the file are executed in sequence. Theoretically, all commands which can be typed in to a telnet session to the device or which appear in a config file can be used in the command file. However, in most cases, you will use config change commands and commands to the UP0/UP1 modules.

The command file is executed every time it is retrieved (depending on the poll interval). However, in most cases, you don't want it to be executed each time, but only once. For example, if you are about to deploy a certain configuration change to all IPBSs, then you want this change to be done once per IPBS only. This can be achieved by the check command:

mod cmd UP1 check <final-command> <serial>

The devices maintain an internal variable UPDATE/CHECK which is initially (or when the device is reset to factory settings) empty. The check command will compare the <serial> parameter with the UPDATE/CHECK variable. If it is equal, any further processing of the command file is cancelled.

If it differs, the remainder of the file will be processed and, after the last command is executed, the UPDATE/CHECK variable will be set to <serial> and the <final-command> will be executed. The following commands are useful values for <final-command>:

ireset	resets the device as soon it is idle
reset	resets the device immediately
iresetn	resets the device as soon it is idle, only if a reset is required
resetn	resets the device immediately, only if a reset is required
ser	this is a no-op

Often, configuration changes shall be made only during certain times (e.g. non-working hours). This can be achieved using the times command:

mod cmd UP1 times [/allow <hours>] [/initial <minutes>]

The times command will check the current time against <hours>. If it does not match this restriction, any further processing of the command file is cancelled. <hours> is a comma separated list of hours. Only those hours listed are considered valid times for execution of the command file.

mod cmd UP1 times /allow 12,23,0,1,2,3,4

The command above allows command executions only between 12:00 and 12:59 and 23:00 and 4:59 local time (on a 24h clock). Note that if the device has no time set, all command executions will be cancelled.

If the /initial parameter is set, the no commands will be executed within the first <minutes> minutes after the device has been booted. This is done to avoid firmware download and flashing when installing devices.

mod cmd UP1 times /allow 12,23,1,2,3,4 /initial 6

The command above suppresses any command file processing within the first six minutes after each boot of the device. If /initial is set, new devices (or those that have

been reset to factory settings), the command file will be retrieved even if it normally would be suppressed by the /allow parameter. This allows new devices to retrieve a site specific standard configuration quickly.

A.1.4   Setting the UP0 Parameters

To perform a firmware update, use the following command:

mod cmd UP0 prot <url> <final-command> <build-serial>

The command above downloads the new firmware from <url> and flash it to the device, then <final-command> is executed.

The IPBSs maintain an internal variable UPDATE/PROT which is initially (or when the device is reset to factory settings) empty. The prot command will compare the <build-serial> parameter with the UPDATE/PROT variable. If it is equal, no firmware will be loaded or flashed. If there is no UPDATE/PROT yet (like for a new device), <build-serial> is compared against the build number of the current firmware. After a successful download, UPDATE/PROT is set to <build-serial>. Note that <build-serial> is not checked against the firmware version actually loaded. It is your responsibility to keep this consistent.

If <url> ends with a slash ('/'), then a default firmware filename is added to the URL depending on the type of the device.

	Firmware filename
IPBS1/IPBS4x0	ipbs.bin
IPBS2/IPBS4x2	ipbs2.bin

mod cmd UP0 prot http://192.168.0.10/firm/ ireset 5.0.0

The command above determines if firmware 5.0.0 is already installed. If not, new firmware will be downloaded from the following location depending on type of device:
IPBS1/IPBS4x0: http://192.168.0.10/firm/ipbs.bin
IPBS2/IPBS4x2: http://192.168.0.10/firm/ipbs2.bin
The UPDATE/PROT variable will be set to 5.0.0 and the device will be reset as soon as it is idle.

Similar to the prot command, the boot command will update the boot code.

	Boot filename
IPBS1/IPBS4x0	boot_ipbs.bin
IPBS2/IPBS4x2	boot_ipbs2.bin

mod cmd UP0 boot http://192.168.0.10/firm ireset 5.0.0

The command above determines if boot code 5.0.0 is already installed. If not, new boot code will be downloaded from the following location depending on type of device:
IPBS1/IPBS4x0: http://192.168.0.10/firm/boot_ipbs.bin
IPBS2/IPBS4x2: http://192.168.0.10/firm/boot_ipbs2.bin
The UPDATE/BOOT variable will be set to 5.0.0 and the device will be reset as soon as it is idle.

Using UP0, device configurations can be saved to a web server.

mod cmd UP0 scfg <url>

This will cause the device to upload its current config to url This will be done using an HTTP PUT command. url must be writable thus. With url, some meta character strings are replaces as follows:

Sequence	Replacement	Example
#d	Current date and time	20040319-162544
#m	Device mac address	00-90-33-03-0d-f0
#h	Device hardware ID	ipbs-03-0d-f0
#b	Rolling backup index loops over 0 .. n-1 for each backup	5

Example IPBS1/IPBS4x0 and IPBS2/IPBS4x2 Boot and Firmware Update

This example shows an "update file" for the IPBS1/IPBS4x0 and IPBS2/IPBS4x2.

mod cmd UP0 prot http://172.20.8.128/mitel/firmware/ ireset 5.0.0

mod cmd UP0 boot http://172.20.8.128/mitel/boot/ ireset 5.0.0

A.1.5 Configuration File Backup

To make a backup of the configuration file, use the following command:

mod cmd UP0 scfg <url> [<final-command> <save-serial> [/force <hours>]]

The scfg command uploads the current configuration file to the specified <url>.

Example

mod cmd UP0 scfg http://192.168.0.10/configs/saved/#h#b5.txt no-op WEEKLY /force 168

The command above saves the device configuration file once a week with a backlog of 5 weeks.

A.1.6 Download Configuration File

To load a configuration file on the IP-DECT device use the following command:

mod cmd UP0 cfg <url> <final-command> <serial>

The command loads the configuration file, and all commands in it are executed.

A.1.7 Configure Microsoft IIS as an Update Server

To be able to upload (save) device configuration information on the web server, it must allow HTTP PUT requests. All other functions require HTTP GET permissions only.

You may want to restrict access to that site to certain network address ranges.

To avoid entering authentication data in every IPBS, it is recommended to allow anonymous read access. For write access (http PUT), authentication is needed with IIS ver. 6 and later. Authentication data needs to be configured in the devices that need to be backed up, e.g. the PARI Master, Master and Mobility Master.

Requirements for IP-DECT

• Version 5.1.X and later supports the authentication algorithm "md5-sess".

Requirements for Microsoft IIS

• Windows 2008 R2 server containing Microsoft IIS ver. 7.5.

- Windows 2012 server containing Microsoft IIS ver. 8.

To configure Microsoft IIS as an Update Server

The steps that are involved are shown in the figure below. The steps are described in more detail below the figure.
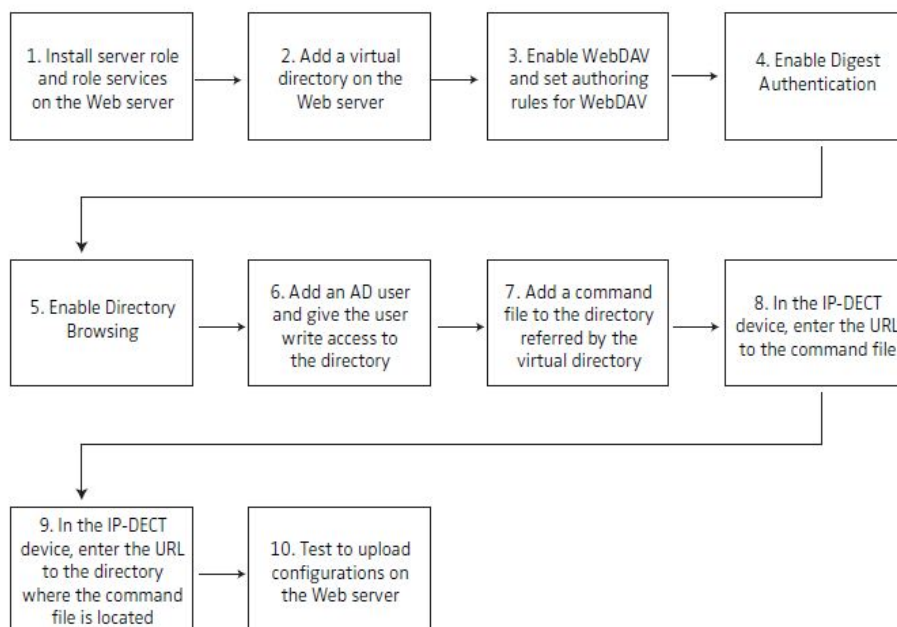

Figure 10. To configure Microsoft IIS as an Update Server.

1. Install server role and role services on the Web server

Windows 2008

1   Connect to the Windows 2008 R2 server.

2   In Server Manager, right-click on **Roles** and select **Add Roles (menu item)**. The **Add Roles wizard** starts.

3   Click **Next**.

4   Select the **server role Web Server (II)** check box.

5   Click **Next.**

6   Click **Next**.

7   Ensure that the following role services check boxes are selected and leave the rest unchecked:

    - Directory Browsing

    - WebDAV Publishing

    - Digest Authentication

8   Click **Next**.

9   Click **Install**.

Windows 2012

1   Connect to the Windows 2012 R2 server.

2   In Server Manager, right-click on **Manage** and select **Add Roles and Features (menu item)**. The **Add Roles and Features wizard** starts.

3   Click **Next**.

4   Select the **Role-based or feature-based installation** check box.

5   Click **Next.**

6   Select a server on which to install roles and features

7   Click **Next**.

8   Ensure that the following role services check boxes are selected and leave the rest unchecked:

        - *Directory Browsing*

        - *WebDAV Publishing*

        - *Digest Authentication*

9   Click **Next**.

10   Click **Next**.

11   Click **Install**.

2. Add a virtual directory on the Web server

1   In **Internet Information Services (IIS) Manager**, double-click on the server name and double-click **Sites**.

2   Right-click on **Default Web Site** and select **Add Virtual Directory... (menu item)**. The **Add Virtual Directory** window appears.

3   In the *Alias* **text** field, enter a name for the virtual directory.

4   In the **Physical path** field, click on the **...** button to the right of the field and browse to the location where the virtual directory shall be stored. Create a new virtual directory and name it.

5   Close the **Add Virtual Directory** window, click **OK**.

3. Enable WebDAV and set authoring rules for WebDAV

1   In **Internet Information Services (IIS) Manager,** left-click on **Default Web Site**.

2   Left-double click on **WebDAV Authoring Rules**

3   Left-click on **Enable WebDAV (link)**.

4   Left-click on **Add Authoring Rule..." (menu item)**. The **Add Authoring Rule** window is shown.

5   In section *Allow access to this content to:*, select the *All users* option.

6   In section *Permissions*, select the *Read, Source* and *Write* check boxes.

7   Click **OK**.

4. Enable Digest Authentication

Note: Digest Authentication requires that the Web server is joined to a domain.

1   Left-click on the virtual directory.

2   Left-double click on **Authenticaton**.

3   Select **Digest Authentication** and left-click on **Enable** in the **Actions** pane.

5. Enable Directory Browsing

1   Left-click on the virtual directory.

2   Left-double click on **Directory Browsing** and left-click on **Enable** in the **Actions** pane.

6. Add an AD user and give the user write access to the directory

Note: This section requires an existing Active Directory (AD) user.

1   Right-click on the virtual directory and left-click on **Edit Permissions... (menu item)**. The **Properties** window for the virtual directory is shown.

2   Click on the **Security** tab.

3   Click on **Edit...** (button). The **Permissions for virtual directory name** window is shown.

4   Click on **Add** (button). The **Select Users, Computers, Service Accounts, or Groups** window is shown.

5   In the **Enter the object names to select (examples):** text field, enter the name of an AD user. Click on **Check Names** (button) to the right of the text field.

6   Click **OK**.

7   In the **Permissions for virtual directory name** window: Allow modify permission for the AD user by selecting the *Allow* check box for the *Modify* permission.

8   Click **OK**.

9   Click **OK**.

7. Add a command file to the directory referred by the virtual directory

1   Add a command file to the directory referred by the virtual directory. For information on the command file syntax, see A.1.4 *Setting the UP0 Parameters* on page 139.

8. In the IP-DECT device (IPBS), enter the URL to the command file

1   See 4.9.1 *Configure Automatic Firmware Update* on page 94 on how to configure the IPBS for automatic update.

9. In the IP-DECT device (IPBS), enter the URL to the directory where the command file is located

1   Select **Services** > **HTTP Client**.

2   In section **Authenticated URLs**, enter in the **URL** text field the URL to the directory.

3   In the **User text** field, enter the user name of the AD user that was given write access, see *6. Add an AD user and give the user write access to the directory* on page 143.

4   In the **Password** text field, enter the password.

10. Test to upload configurations on the Web server

5   During the test period, set the poll interval to 1 minute.

6   When the command file has been run, check that the label data in the IPBS (select Services > Update) is the same as in the command file.

7   Check that the configuration file is located in the directory.

Appendix B: Local R-Key Handling

Local R-key handling assume that the check box for local R-key handling is selected, see 4.6.8 *enable/disable Local R-Key Handling* on page 70.

The following R-key functions are available during a call.

Key	Description
R	Put the ongoing call on hold and get a new line. (Dial the number to the second call.)
R0	Reject the incoming call.
R1	Terminate the ongoing call and switch to call on hold/incomming call.
R2	Switch between ongoing call and call on hold/incomming call.
R3	This function is normally used for three-party conference.
R4	Transfer call on hold to ongoing call and disconnect.
RR (unattended transfer)	Put the ongoing call on hold and dial the number to the destination where the last held call shall be transferred to.

Appendix C: Database Maintenance

This section describes how IP-DECT user configuration can be moved from one system to another. By moving users, one IP-DECT system can be split into many systems or several IP-DECT systems can be merged to one single system.

Before database merge you should consider if the IP-DECT R3 Multi Master concept can be used instead and whether it is possible to have several Masters on one site.

C.1 Prerequisites

For all systems involved in the database maintenance procedure:

- It is highly recommended to have the same software version running on all systems.
- If a user is moved to a system with a different SARI, the target system must be configured with multiple SARIs containing the SARI number of the originating system as well as its existing SARI. For more information, see 4.6.35 *enter sARI* on page 87.
- The systems must have the same DECT system name and the same DECT system password (configured under DECT > System) as well as the same device password (General > Admin).
- LDAP replication must not be activated.

C.2 Database Maintenance Procedure

1   Make sure the handsets that correspond to the moved user data have no contact with the system. Turn off the handsets or switch off the Radio(s) in the area where the handsets are located. Handsets should show "No system". Handsets may be desubscribed if they have connection to the system during database maintenance.

2   Save a configuration file from each Master involved. See 4.14 *Backup* on page 120.

3   Identify user records in the saved configuration files and modify them according to the desired plan. User records are located at the end of the file beginning after the row:

mod cmd FLASHDIR0 add-view 101 cn=PBX0

4   To remove a user, remove the corresponding line.

To add a user (from another file), insert a line that has been removed from another file. Remove the following attributes:

(guid;bin=###)

(usn=###)

where ### denotes an arbitrary value.

5   Save modifications to the configuration files.

6   Make sure that step 1 is met, and upload configuration files to the corresponding entities. See 4.22.1 *Update Configuration* on page 118.

7   Reset in order to make the changes take effect, see 4.28 *Reset* on page 125.

Removing a User Example

This example shows part of the configuration file. There may also be other attributes in the used system.

Before Removal

mod cmd FLASHDIR0 add-view 101 cn=PBX0

mod cmd FLASHDIR0 add-item 101
(cn=1950)(guid;bin=80319FC0E909D311905C00013E00EFC8)(dn=1950)(h
323=1950)(e164=1950)(pbx=<user admin="no"/>)(pbx=<gw
name="DECT_CEg" ipei="002020173394"
subs="977e9bfc568c8223197e4195bec9ec28"/>)(usn=14)

mod cmd FLASHDIR0 add-item 101
(cn=1951)(guid;bin=7B7C9D01E909D311905C00013E00EFC8)(dn=1951)(h
323=1951)(e164=1951)(pbx=<user admin="no"/>)(pbx=<gw
name="DECT_CEg" ipei="002020173479"
subs="90bd79116daec066105610822cabc1e7"/>)(usn=15)

After Removal

mod cmd FLASHDIR0 add-view 101 cn=PBX0

mod cmd FLASHDIR0 add-item 101
(cn=1950)(guid;bin=80319FC0E909D311905C00013E00EFC8)(dn=1950)(h
323=1950)(e164=1950)(pbx=<user admin="no"/>)(pbx=<gw
name="DECT_CEg" ipei="002020173394"
subs="977e9bfc568c8223197e4195bec9ec28"/>)(usn=14)

Adding a User Example

This example shows part of the configuration file. There may also be other attributes in the used system.

Before Addition

mod cmd FLASHDIR0 add-view 101 cn=PBX0

mod cmd FLASHDIR0 add-item 101
(cn=1950)(guid;bin=80319FC0E909D311905C00013E00EFC8)(dn=1950)(h
323=1950)(e164=1950)(pbx=<user admin="no"/>)(pbx=<gw
name="DECT_CEg" ipei="002020173394"
subs="977e9bfc568c8223197e4195bec9ec28"/>)(usn=14)

After Addition

mod cmd FLASHDIR0 add-view 101 cn=PBX0

mod cmd FLASHDIR0 add-item 101
(cn=1950)(guid;bin=80319FC0E909D311905C00013E00EFC8)(dn=1950)(h
323=1950)(e164=1950)(pbx=<user admin="no"/>)(pbx=<gw
name="DECT_CEg" ipei="002020173394"
subs="977e9bfc568c8223197e4195bec9ec28"/>)(usn=14)

mod cmd FLASHDIR0 add-item 101
(cn=1951) (dn=1951)(h323=1951)(e164=1951)(pbx=<user admin="no"/
>)(pbx=<gw name="DECT_CEg" ipei="002020173479"
subs="90bd79116daec066105610822cabc1e7"/>)

The guid;bin and usn attributes are not inserted. The system will create these attributes when the file is uploaded to the device.

Appendix D: Load Balancing

Load balancing can be used in an IP-DECT system when the number of handsets exceeds what an IP-PBX is able to register.

When load balancing the traffic is distributed over several IP-PBXs which can be done in two ways using:

- fixed connections for users on each Master towards *multiple* IP-PBXs.
- dynamic connection for users on each Master towards IP-PBX *network* using DNS services.

D.1 Load Balancing Using Fixed Connection Towards IP-PBXs

When the number of users exceeds what an IP-PBX is able to register, you can load balance using several IP-PBXs where each Master in the IP-DECT system is connected to a fixed IP-PBX.

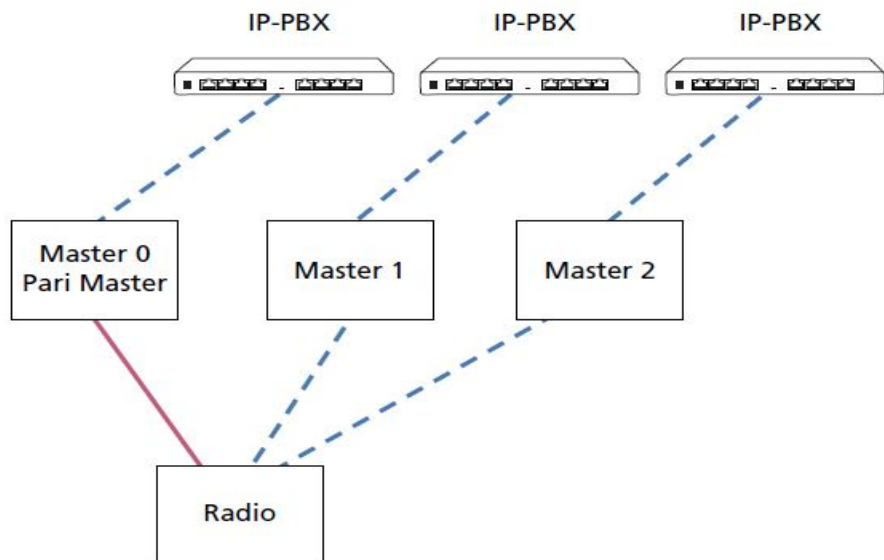**Note:** For redundancy, an alternative gatekeeper/proxy should always be used.

Figure 11. Load balancing using fixed connection towards IP-PBXs.

1   Select **DECT** > **Master.**

2   In the drop-down list, select **SIP/UDP**, **SIP/TCP** or **SIP/TLS** protocol.

3   Enter the IP address, domain name or host name and optionally port of proxy (e.g. proxy1.mitel-rd.com:5060) to the SIP proxy (registrar) in the Proxy text field.

4   To get redundancy: Depending on how many alternative SIP proxys that are used, do as follows:

In the Alt. Proxy 1 text field: Enter the IP address, domain name or host name and optionally port of proxy (e.g. proxy2.mitel-rd.com:5060) to the alternative SIP proxy (registrar).

In the Alt. Proxy 2 text field: Enter the IP address or host name and optionally port of proxy (e.g. proxy3.mitel-rd.com:5060) to the alternative SIP proxy (registrar).

Note: The Alt. Proxy 2 text field cannot be used if the Proxy and the Alt. Proxy 1 text fields contain domain names.

In the Alt. Proxy 3 text field: Enter the IP address or host name and optionally port of proxy (e.g. proxy4.mitel-rd.com:5060) to the alternative SIP proxy (registrar).
Note: The Alt. Proxy 3 text field cannot be used if the Proxy and the Alt. Proxy 1 text fields contain domain names.

5   Reset in order to make the changes take effect, see *4.28 Reset*.

D.2   Load Balancing Using Dynamic Connection Towards IP-PBX Network

When the number of users exceeds what an IP-PBX is able to register, you can use load balancing towards an IP-PBX network. Using DNS services, users on each Master are dynamically connected towards the IP-PBX network. In addition to the load balancing of the traffic, redundancy is also archived.
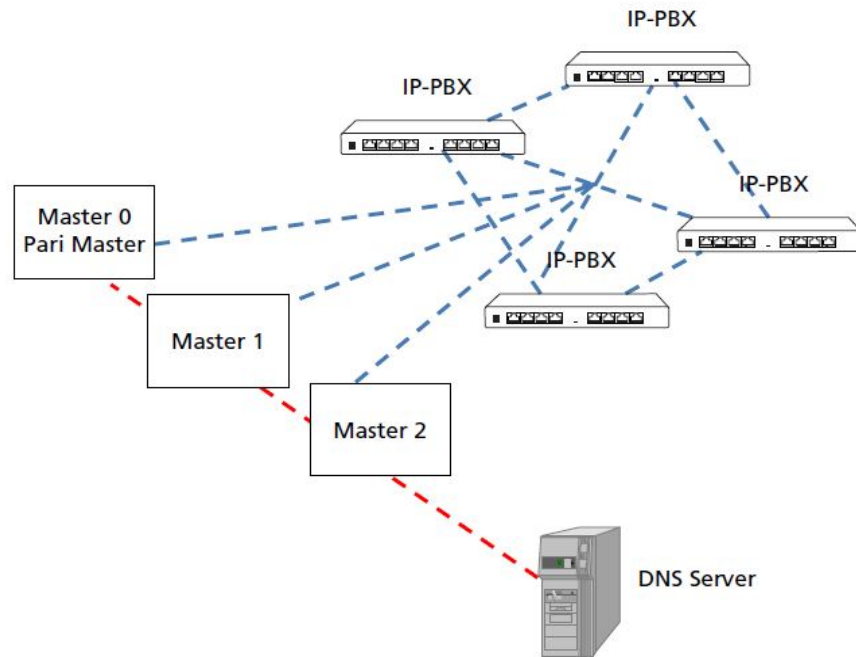

Figure 12. Load balancing using dynamic connection towards IP-PBX network.

D.2.1   How the Load Balancing Works

When you register a handset, a SRV-type query is sent to the DNS server asking for existing SIP proxys (IP-PBXs) in the domain defined in the Master. The DNS server will reply with a list of SRV (Service) records, one for each IP-PBX. Each SRV record contains a priority and a weight value. Lower priority value means more preferred. When there are two or more records with the same priority, then the weight value determines which IP-PBX the user should be dynamically connected to.

A DNS server assign each user a primary and a secondary proxy address using DNS-SRV service mechanism.

D.2.2 Local Site Redundancy

If redundancy is wanted in a remote site, that is you want to be able to make emergency phone call if the WAN connection to the central site goes down, a local site proxy server, e.g. SRST (Cisco), can be used in the remote site, see figure 13 on page 150.
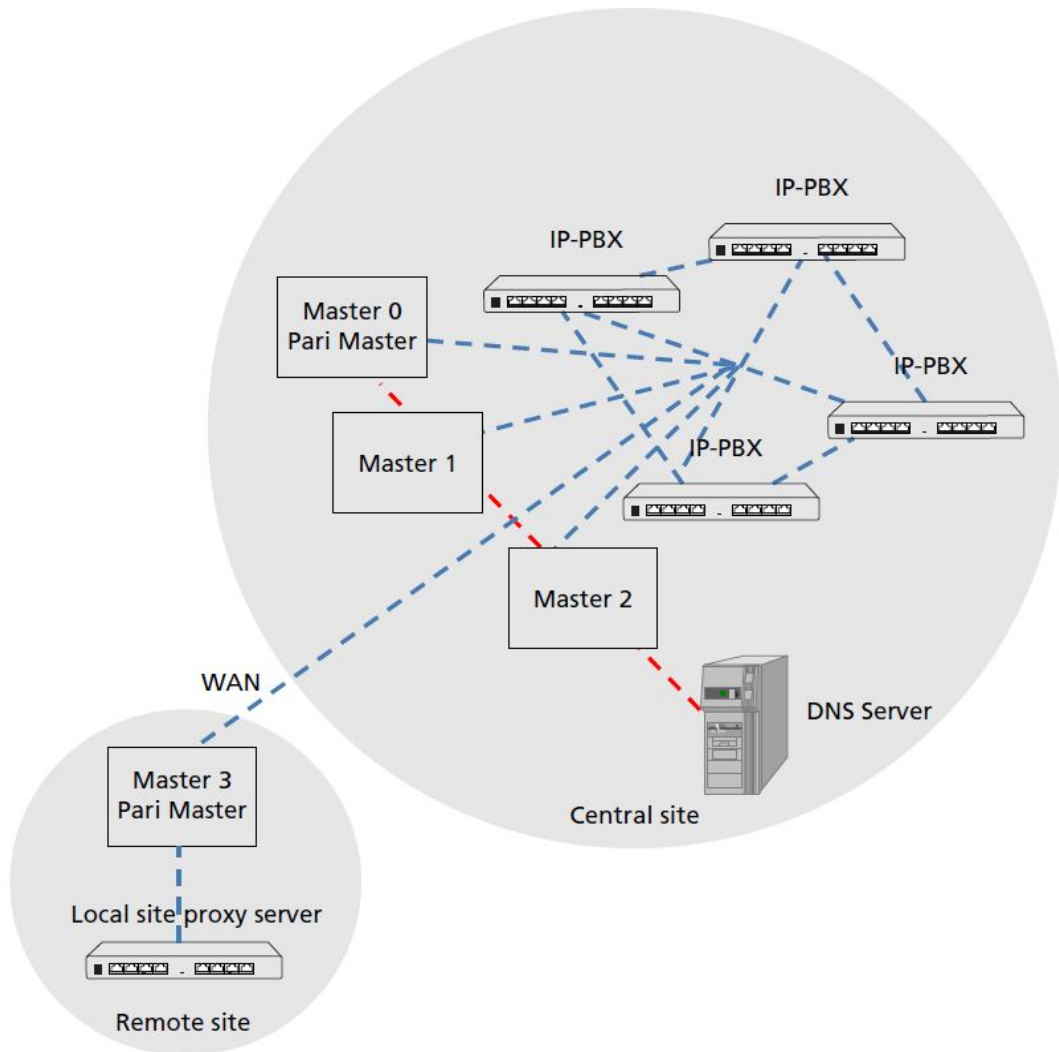

Figure 13. Redundancy in the remote site using a local site proxy server.

D.2.3 About SRV Records

Record format

An SRV record has the form:.

_Service._Proto.Name TTL Class SRV Priority Weight Port Target

- **Service**: the symbolic name of the desired service.
- **Proto**: the protocol of the desired service; this is usually either TCP or UDP.
- **Name**: the domain name for which this record is valid.
- **TTL**: standard DNS time to live field.
- **Class**: standard DNS class field (this is always IN).

- **Priority**: the priority of the target host, lower value means more preferred.
- **Weight**: A relative weight for records with the same priority.
- **Port**: the TCP or UDP port on which the service is to be found.
- **Target**: the hostname of the machine providing the service.

An example of an SRV record might look like this:

    _sip._udp.mitel-rd.com. 86400 IN SRV 0 5 5060 sipserver.mitel-rd.com.

This points to a server named sipserver.mitel-rd.com listening on TCP port 5060 for SIP protocol connections. The priority given here is 0, and the weight is 5.

SRV records must contain the fully qualified domain name (FQDN) of the host.

How to set priority and weight

SIP clients always use the SRV record with the lowest-numbered priority value first, and only fall back to other records if the connection with this record's host fails. Thus a service may have a designated "fallback" server, which will only be used if the primary server fails. Only another SRV record, with a priority field value higher than the primary server's record, is needed.

If a service has multiple SRV records with the same priority value, clients use the weight field to determine which host to use. The weight value is relevant only in relation to other weight values for the service, and only among records with the same priority value.

In the following example showing five records, both the priority and weight fields are used to provide a combination of load balancing and backup service.

    _sip._udp.mitel-rd.com. 86400 IN SRV 10 60 5060 bigbox.mitel-rd.com.

    _sip._udp.mitel-rd.com. 86400 IN SRV 10 20 5060 smallbox1.mitel-rd.com.

    _sip._udp.mitel-rd.com. 86400 IN SRV 10 20 5060 smallbox2.mitel-rd.com.

    _sip._udp.mitel-rd.com. 86400 IN SRV 20 50 5060 backupbox1.mitel-rd.com.

    _sip._udp.mitel-rd.com. 86400 IN SRV 20 50 5060 backupbox2.mitel-rd.com.

The first three records with priority 10 are primary servers and the last two records with priority 20 are secondary servers.

For each client, a primary server is selected at random with the help of the weight values 60, 20 and 20. This will distribute all clients on the primary servers according to the weight values.

If a client's primary server goes down, the client will use the secondary server instead, i.e. backupbox1.mitel-rd.com and backupbox2.mitel-rd.com.

D.2.4 Load Balancing Using Dynamic Connection: Master Settings

1   Select DECT > Master.

2   In the drop-down list, select "SIP" protocol.

3   Enter the SIP server's domain address in the *Proxy* text field.

4   A local site proxy server (IP-PBX), e.g. SRST (Cisco), can be used to make emergency phone call in case that the WAN connection goes down, see D.2.2 *Local Site Redundancy* on page 150.
     Enter the IP address or host name and optionally port of proxy (e.g. proxy2.mitel-rd.com:5060) to the local site proxy server in the Alt. Proxy text field.

5   Reset in order to make the changes take effect, see *4.28 Reset*.

6   Repeat step 1 to 5 for all existing Masters.

D.2.5   Load Balancing Using Dynamic Connection: DNS Server Settings

The example below shows the settings in Microsoft Windows Server where the DNS server is installed.

1   From a Microsoft Windows Server with the DNS server installed, open the DNS management tool.

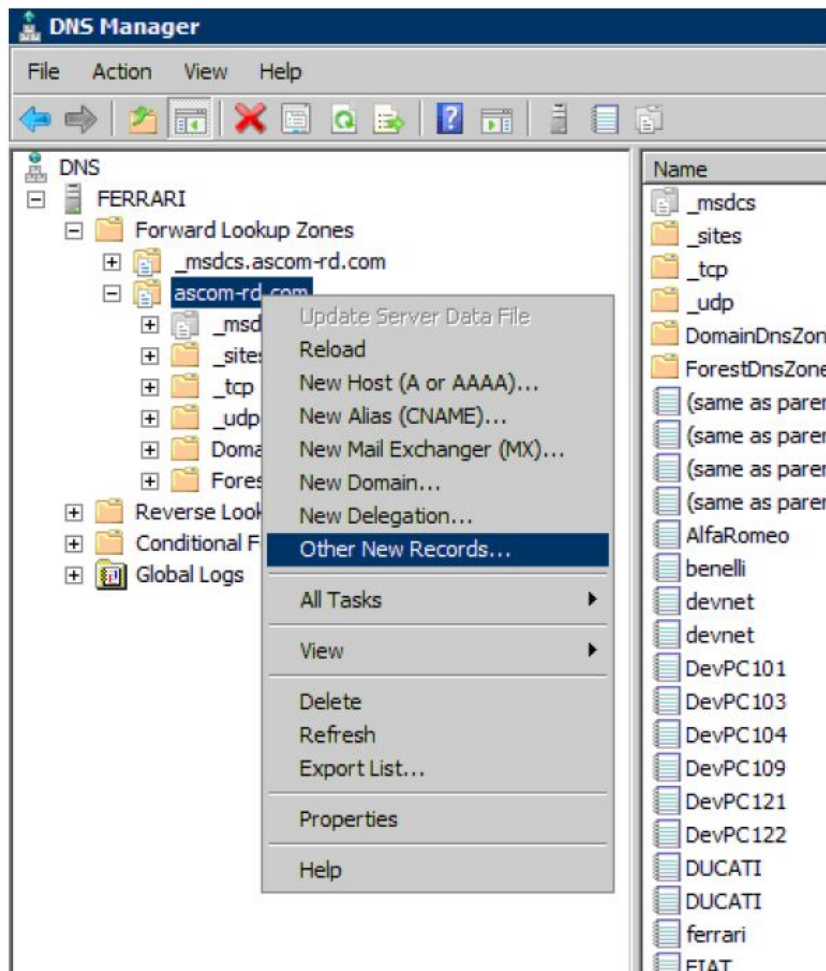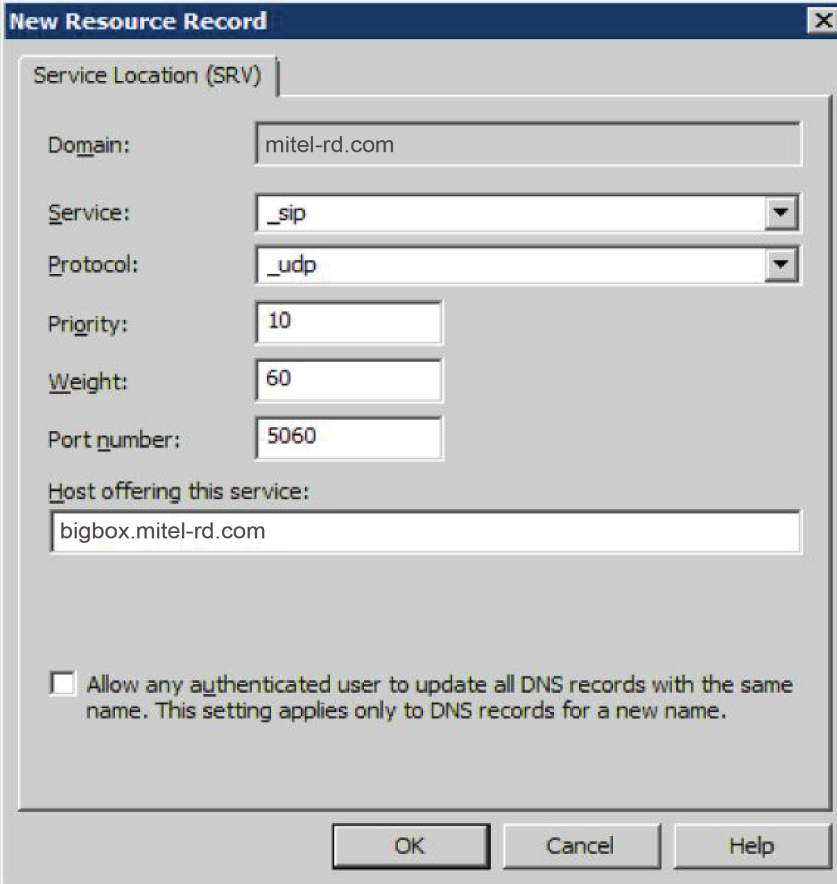2   Right click the domain (or subdomain) you are assigning this service to and select **Other New Records...**.

Figure 14. Select "Other New Records...".

3   Scroll down to Service Location (SRV) in the list.

4   In the "New Resource Record" window, see Figure 15, do as follows:

Enter "_sip" in the *Service* field.

Enter _udp in the *Protocol* field.

Assign a priority and weight. For information on how to set priority and weight, see D.2.3 *About SRV Records* on page 150.

Enter "5060" as the port number.

Enter the host name of your SIP server (IP-PBX). Note: The host name must be a fully qualified domain name (FQDN).

Click **OK**.

Figure 15. New resource record settings

5   You can view your new SRV record by clicking on the _udp item under your domain.

6   Right click the domain (or subdomain) where the new SRV record is located and select "New Host (A)...".

7   In the "New Host" window, see Figure 16, do as follows:

Enter in the *Name* field the host name of your SIP server (IP-PBX).

Verify that the fully qualified domain name (FQDN) is the correct one.

Enter the IP address of your SIP server.

Click "Add Host".

Figure 16. New host settings

8   Repeat step 1 to 7 for all existing IP-PBXs.

Appendix E: Update Script for Configuration of Kerberos Clients

The update script is as follows:

mod cmd UP1 check resetn serial002

config add NTP0 /addr 192.168.42.136

config write

config activate

vars create CMD0/KCMD p <join+realm="negrealm1"+user="neguser1"+
password="negpwd1"+force="true"+disable-local="true"+kerberos-rc4=
"true"><server+realm="negrealm1"+address="192.168.42.34"><server+
realm="negrealm2"+addres="192.168.42.99"/></join>

Description of the update script:

Command line 1: mod cmd UP1 check resetn serial002

By inserting this into the update script file the update server will check the variable "check" and if the value (serial002) is different from the value in the update server this script will be executed and the box will be rebooted afterwards.

Command line 2: config add NTP0 /addr 192.168.42.136

By inserting this into the update script the local Time server is configured with IP address to valid time server and active time can be retrieved. Correct time is very important in Kerberos for joining of realm and for login purpose.

Command line 3: vars create CMD0/KCMD p ....

The format of this line is very important. It is very important to only modify the data surrounded with double quote (""). This script describes the mandatory data, the other data is set to default values. All parameters set by the Add-tab (see section 1) is possible to set with this script.

The XML format is as follows:

<join realm="..." host="..." user="..." password="..." disable-local="..." force="..."><server realm="..." address="..." port="..." secondary-address="..." secondary-port="..."/></join realm>

realm: The realm to join
host: The host name for the box (optional, otherwise the hardware id will be used)
user: Admin user name from the Kerberos server
password: Admin password from the Kerberos server
disable-local: the config flag will be set accordingly (true or false, optional, defaulting to false)
force: tells if an existing realm membership shall be discarded (true or false, optional, defaulting to false)
server: multiple servers may be given

In the above example two servers are configured one for the Kerberos server and one if using an Active Directory or Standby Kerberos server.

Appendix F: Import Server Certificate in the Web Browser

To access the GUI for an IPBS using secure web access (https), the certificate for the IPBS can be installed in the web browser to avoid getting certificate error messages.

To install the certificate, perform the following two steps:

Step 1. Create a certificate. See *F.1 Create a Certificate*.

Step 2. Install the certificate in the web browser. See *F.2 Import the Certificate*.

F.1   Create a Certificate

Note: Make sure the name you use to access the IPBS is in the "Common Name" of the certificate (e.g. IP-address) or if the name is an FQDN, in the "DNS Name". The Web Browser will require a match when validating the certificate information.

Create a certificate by selecting one of the following two types of certificate handling options:

- Self-signed certificate

  This option is for customers not planning on having their certificates signed by public or private CAs. Self-signed certificates provide encryption but do in most cases not provide authentication. For more information see *Self-signed Certificates* on page 51.

- Certificates signed by a Certificate Authority (CA)

  Two options are possible:

  A Certificates signed by the customer's own CA. Customers possessing the knowledge and infrastructure to house their own CA could build an internal enterprise CA, enabling them to sign (approve) their own certificate requests. This would make the customer a private CA.

  B Certificates signed by a trusted public third party entity/organization. There are only about a dozen issuers who have the authority to sign certificates for servers worldwide. An example is VeriSign. To use a public CA for certificate approvals the IP-DECT system would in most cases need to be connected to the Internet and hold a fully qualified domain name. For more information see *Certificate Signing Request (CSR)* on page 52.

F.2   Import the Certificate

The instructions below apply for Internet Explorer version 11 and might differ for later versions.

Note: If your PC is running Windows Vista or later, select "run as administrator" for Internet Explorer.

1   Access the GUI for a device. A security warning window will appear when using secure web access (https) to access the GUI.

Figure 17. Security warning window
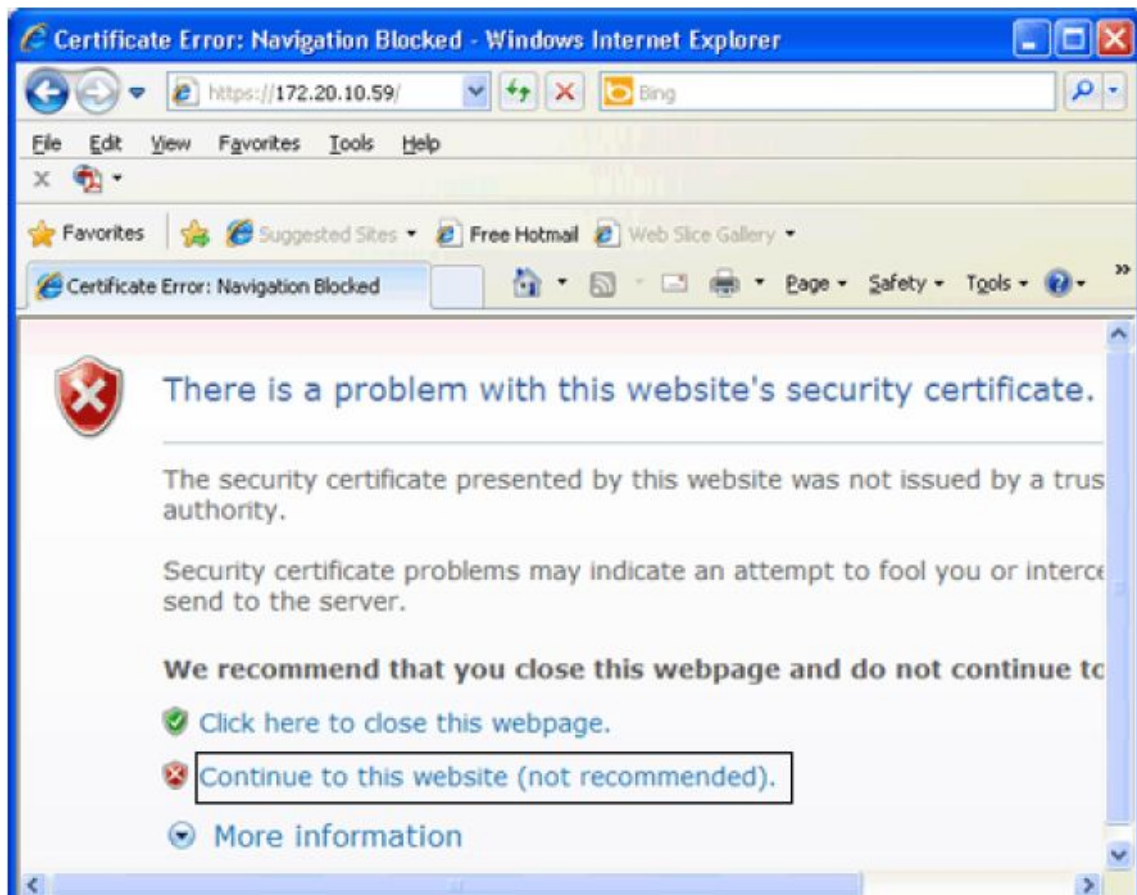
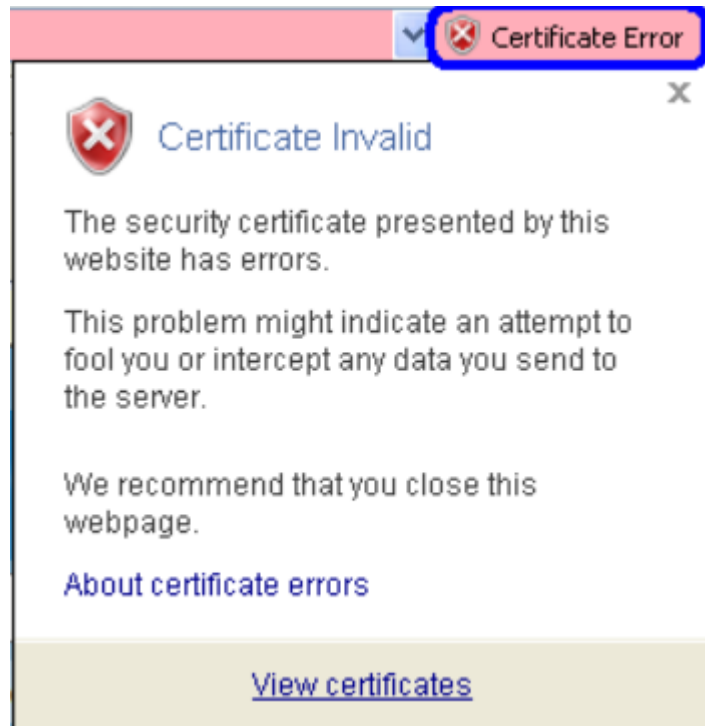2   In the security warning window, click on the text link **Continue to this website (not recommended)**. The login window for the device will appear.

3   Click on the Certificate Error notification in the Security Status bar (next to the Internet Explorer Address bar), see Figure 18. The Security Report window will appear, see Figure 18.

Figure 18. Screen shot of the login window, with the "Security Status bar highlighted.
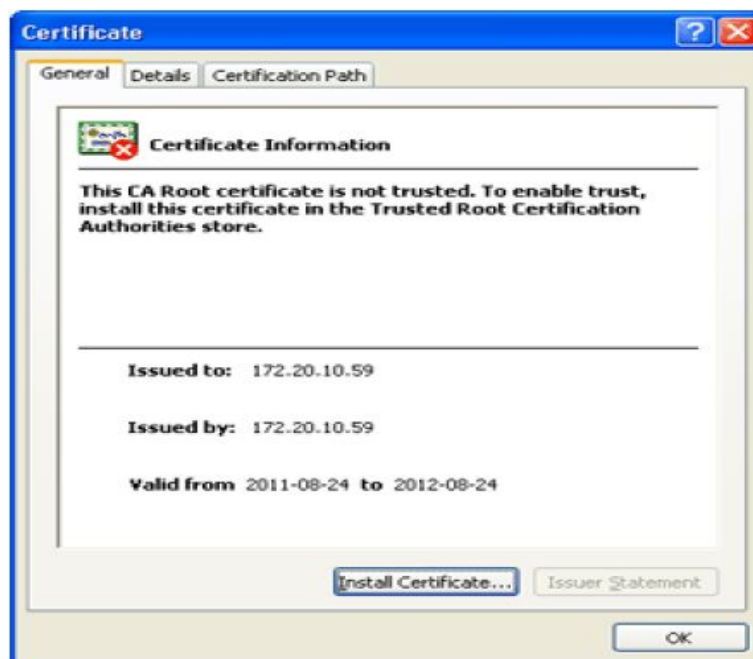
Figure 19. The Security Report window

4   In the Security Report window, click on the blue text link **View certificates**. The Certificate window will appear.

Figure 20. The Certificate window.

5   In the Certificate window, click on the button **Install Certificate...**. The Certificate Import wizard is started.

6   Click on **Next**.

7   Ensure that option **Automatically select the certificate store based on the type of certificate** is selected, see Figure 21. Click on **Next**.
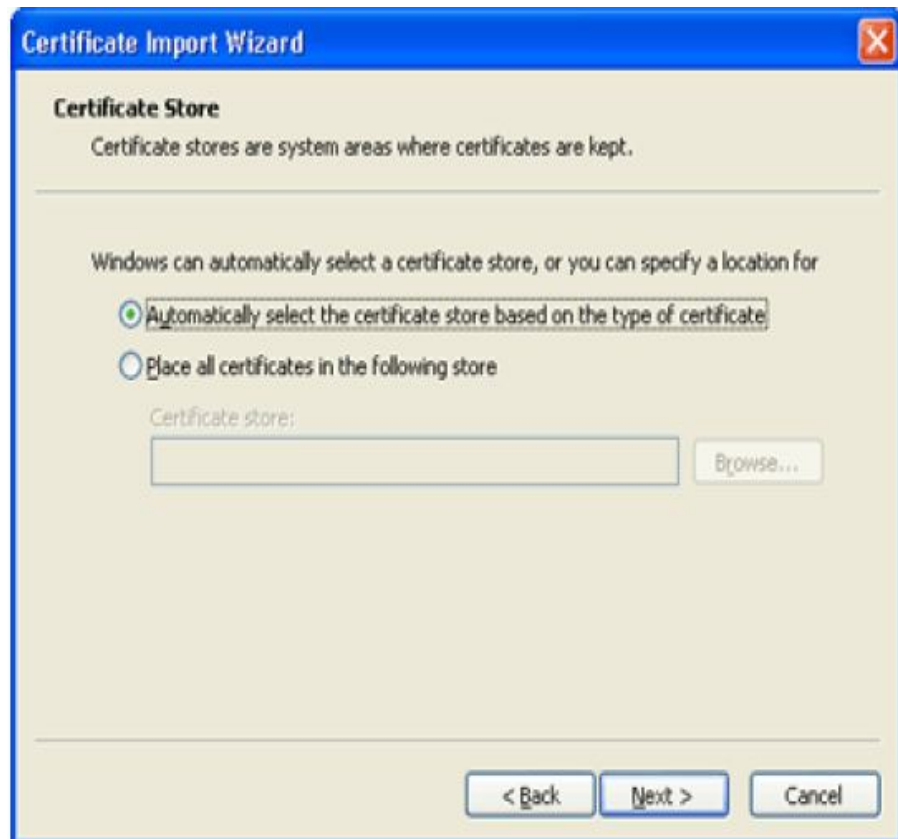

Figure 21. The Certificate Import wizard.

8   Click **Finish** to complete the Certificate Import wizard. The Security Warning window will appear.

9   Click **Yes** to install the certificate.

## Appendix G: Import Client Certificate in the Web Browser

If mutual TLS authentication is used, a trusted client certificate with the associated private key must be available in the web browser's certificate store. IP DECT uses the Subject Alternative Name (SAN) certificate extension to map a client certificate to a user account. The entity that issues the client certificate must use one of the following SAN formats when including the user id:

• rfc822Name - The user id is based on the e-mail format defined in the RFC 822 standard
• otherName, Microsoft, User Principal Name (UPN) - The user id is based on the UPN format, used in Microsoft Windows system.

Perform the following steps to import the client certificate provided by your IT department in the web browser. The instructions below apply for Internet Explorer version 11 and may differ for later versions:

1   In the Windows Start menu, go to the **Control Panel** and select **Network and Internet** > **Internet Options**.

2   Click the **Content** tab and click **Certificates**.

Figure 22. The Internet Properties window
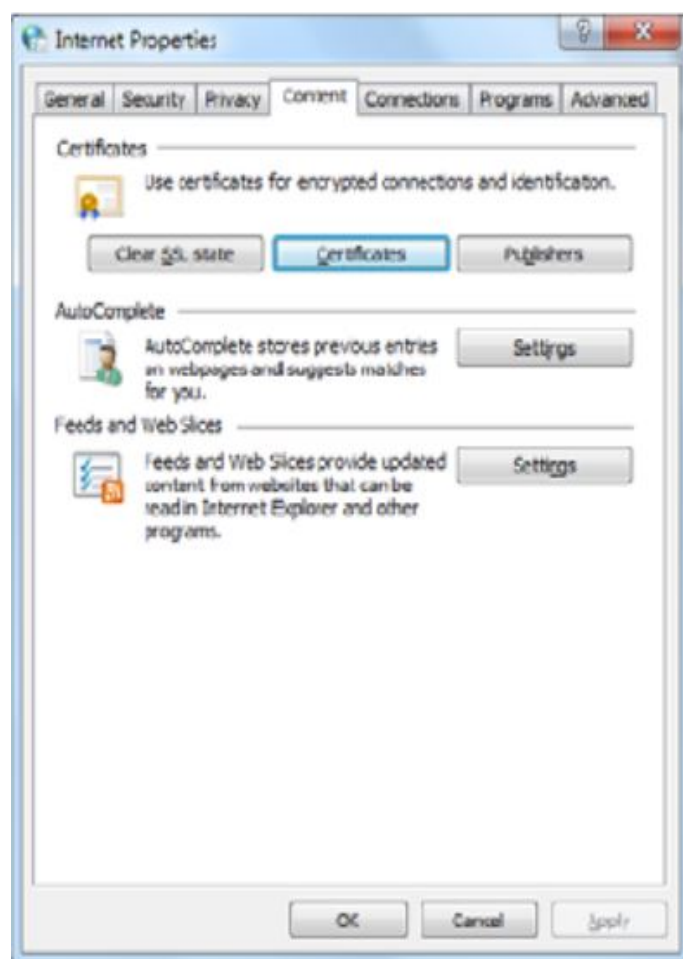
3   Click **Import...**. The Certificate Import Wizard opens.

4   Click **Next**.

---

5   Click **Browse...** and find your client certificate provided by your IT department.

6   Click **Next**.

7   Select **Place all certificates in the following store** and ensure that the certificate store is selected.

Figure 23. The Certificate Import Wizard
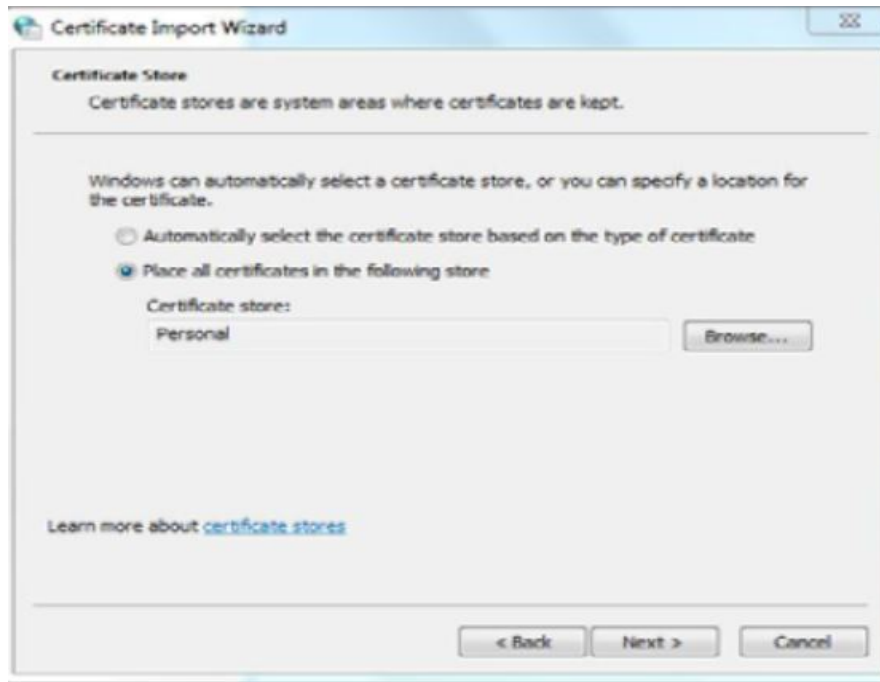
8   Click **Next** and click **Finish**.

9   Select the imported certificate in the Certificates window and ensure that Client Authentication is mentioned under Certificate intended purposes.

Figure 24. The Certificates window
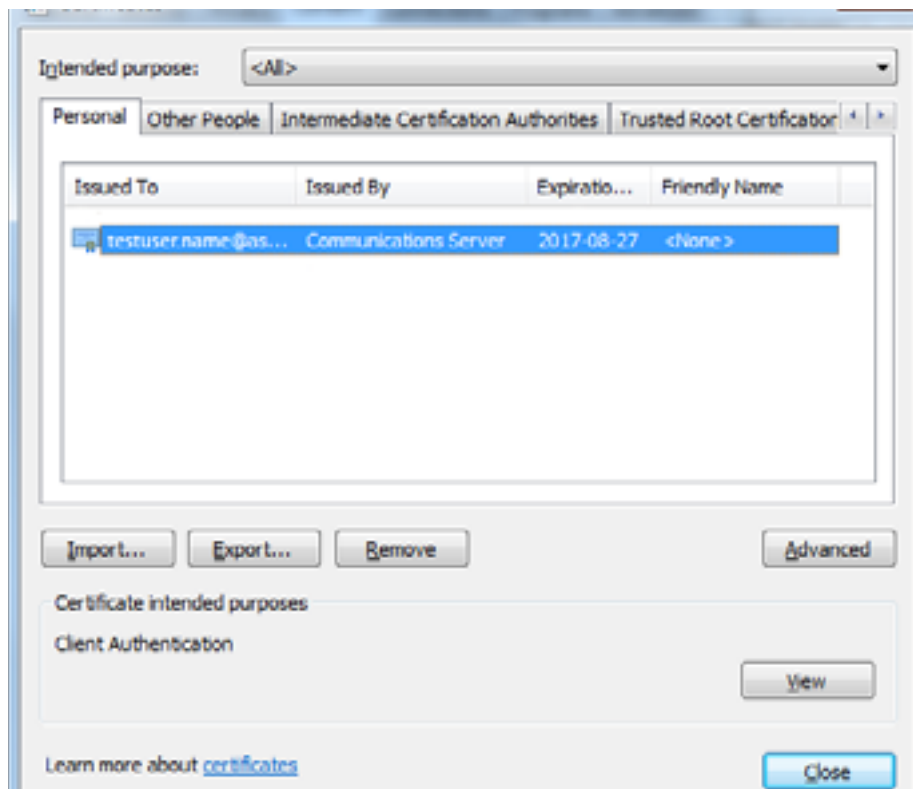
10   Click **Close**.

Appendix H: Used IP Ports

Destination	Source	Protocol	To	From	Description
53	Dynamic	UDP DNS	DNS server	IPBL/IPBS	
67	68	UDP DHCP	DHCP server	IPBL/IPBS	
69, Dynamic	Dynamic	UDP TFTP	TFTP server	IPBL/IPBS	Update firmware
80	Dynamic	TCP HTTP	IPBL/IPBS	Client PC	Web configuration over HTTP
80	Dynamic	TCP HTTP	PARI Master	IPBL/IPBS	Event and Alarm forwarding
88	Dynamic	UDP KERBEROS	Kerberos server	IPBL/IPBS	Login with Kerberos server accounts
123	Dynamic	UDP NTP	NTP server	IPBL/IPBS	
123	Dynamic	UDP NTP	IPBL/IPBS	NTP client	NTP service
137	Dynamic	UDP NETBIOS	WINS server	IPBL/IPBS	
161	Dynamic	UDP SNMP	IPBL/IPBS	SNMP manager	
389	Dynamic	TCP LDAP	Kerberos server	Alternative Kerberos server	
389	Dynamic	TCP LDAP	Master	Standby Master	
443	Dynamic	TCP HTTPS	IPBL/IPBS	Client PC	Web configuration over HTTPS
443	Dynamic	TCP HTTPS	PARI Master	IPBL/IPBS	Event and Alarm forwarding
464	Dynamic	UDP KERBEROS	Kerberos server	IPBL/IPBS	Join Kerberos realm
514	Dynamic	UDP SYSLOG	Syslog server	IPBL/IPBS	Logging
547	546	UDP DHCPv6	DHCPv6 server	IPBL/IPBS	
636	Dynamic	TCP LDAPS	Kerberos server	Standby Master alternative	
636	Dynamic	TCP LDAPS	Master	Standby/ Mirror Master	
1716–1717	Dynamic	TCP H.323	Master	Radio	

1718–1719	Dynamic	TCP H.323	Radio	PARI Master	
1718–1719	Dynamic	UDP H.225	Master	Radio	UDP session timer minimum 120 s.
1718–1719	Dynamic	UDP H.225	Mobility Master	Master	UDP session timer minimum 120 s.
1718–1719	Dynamic	UDP H.225	Mobility Master	Mobility Master	UDP session timer minimum 120 s.
1718–1719	Dynamic	UDP H.225	Crypto Master	Mobility Master	UDP session timer minimum 120 s.
1718–1719	Dynamic	UDP H.225	Radio	Radio	Multicast and broadcast messaging (load balancing). UDP session timer minimum 120 s.
1718–1719	Dynamic	UDP H.225	Master	Standby/ Mirror Master	UDP session timer minimum 120 s.
1722–1723	Dynamic	TCP H.323	PARI Master	Radio	
1724–1725	Dynamic	TCP H.323	Radio	PARI Master	
1726–1727	Dynamic	TCP H.323	Radio	Radio	Multicast and broadcast messaging (load balancing)
1728–xxxx (depending on the number of masters)	Dynamic	TCP H.323	Radio	Non-PARI Master	See system description for details
1814, 1816	Dynamic	TCP UNITE	Master	Unite	Messaging
1815, 1817	Dynamic	TCP UNITE	Unite	Master	Messaging
3217	3217	UDP UNITE	IPBL/IPBS Unite	Unite IPBL/IPBS	IP-DECT Device Management, Fault Reporting, Service Discovery No UDP session timeout allowed
3478	Dynamic	UDP STUN	STUN server	Master	SIP NAT support

3478	Dynamic	UDP STUN/ TURN	STUN/ TURN server	Radio	ICE, Media NAT support
5060	Dynamic	UDP/TCP SIP	Proxy	Master	
5061	Dynamic	TCP SIP over TLS	Proxy	Master	
8080	Dynamic	TCP	Unite Device Manager	IPBL/IPBS	For download of SW.
10147	Dynamic	TCP	Unite Device Manager	Master	Device management for handset.
10217	Dynamic	TCP	Unite Device Manager	Master	Myco data channel
12346	Dynamic	TCP UNITE	Master	Device Manager	Device management for handset.
16384–65535	Dynamic within that range	UDP RTP	Radio	Media Port range is configurable.	No UDP session timeout.

Appendix I: Configure DHCP Options

IPBS include a DHCP client which allows the IP interface to be configured from a DHCP server. In addition to that, IPBS also allow configuring a number of settings via special DHCP vendor options.

I.1 System Requirements

To use vendor specific DHCP options, a DHCP server that supports such options is required. Most popular DHCP server implementations such as the Microsoft Windows DHCP service and the Linux dhcpd do so.

I.2 Configuration

For the DHCP server to support vendor specific options, the options must be made known to the server. Consult the accompanying documentation which comes with your DHCP server implementation how to do this.

I.3 Supported Options

Name	Data type	Array	Code	Meaning	How to code
H323 gatekeeper	IP address	Yes	200	Defines the IP address of both the primary and the alternate gatekeeper for the device. This is only required, if gatekeeper discovery is not feasible	This is an array of IP addresses. Put the primary gatekeepers IP into the first entry, the alternate gatekeepers IP into the second entry. Further entries are ignored.
H323 gatekeeper id	String	No	201	The gatekeeper id of the gatekeeper the device likes to register with. Usually required only if several gatekeepers are running and a particular one must be chosen during gatekeeper discovery	Type the gatekeeper id as configured in the gateway or PBX configuration into the string field.

POSIX TZ	String	No	202	Defines both the time zone and the daylight saving time information.	This option is in fact identical to the standard DHCP option number 88 (TZ). However, various DHCP servers do not support this option, so it is provided as a redundant vendor specific option. If your DHCP server supports option 88, the vendor specific option is not needed.
Default coder	String	No	203	Defines the preferred coders for H.245 coder negotiation, as well as the packet size when sending RTP packets and the use of CNG and VAD.	This string option must contain the value of the "/coder" option in the configuration file, e.g. **G729A,40,esx**. Additional options are: e - Exclusive, s - Silence Compression, x - Enable Secure RTP (SRTP), n - No DTMF Detection.
VLAN ID	Word (16bit)	No	206	The 802.1q VLAN ID for traffic sent and received by the device	Enter the numerical ID into the 16bit edit field
VLAN Priority	Byte (8bit)	No	207	The 802.1p VLAN priority for traffic sent by the device	Enter the numerical priority into the 8bit edit field
TOS Bits	String	No	208	The values for the IP TOS/DSCP field in the IP header of UDP-RTP and TCP-signaling packets sent by the device (Bit 0..2 'precedence', bit 3..6 'type of service')	Enter the comma separated numerical priorities into the string field. You may prefix with **0x** to specify hexadecimal numbers (or **0** to specify octal numbers). The default for RTP packets is 0xb8 (RFC 3246 - Expedited Forwarding), for signaling packets it is 0x68 (RFC 3246 - Assured Forwarding). 0xb8,0x68 for example defines the default values

Enbloc dialling	Byte (8bit)	No	209	The number of seconds dialled digits are kept in IP-DECT before they are sent en-bloc to the gatekeeper	Enter the number of seconds into the 8bit edit field. A value of **0** indicates that en-bloc dialling is turned off and digits are sent to the gatekeeper as they are dialled
Dialtone type	Byte (8bit)	No	210	The type of dialtone to generate locally	Enter the numeric dialtone type (**0** - EUROPE-PBX, **1** - EUROPE-PUBLIC, **2** - US, **3** - UK, **4** - ITALY-PUBLIC, **5** - CZECH-PBX, **6** - CZECH-PUBLIC, **7** - SWEDEN, **8** - FRANCE, **9** - SWISS, **10** - ITALY-PBX, **11** - BELGIUM, **12** - NETHERLANDS, **13** - NORWAY, **14** - DENMARK, **15** - GERMANY, **16** - SPAIN, **17** - FINLAND, **18** - AUSTRIA, **19** - IRELAND, **20** - AUSTRALIA, **21** - NEWZEALAND, **22** - MALAYSIA, **23** - TURKEY, **24** - RUSSIA, **25** - SOUTH AFRICA, **26** - BRAZIL)
Faststart	Byte (8bit)	No	211	Disable/Enable the H245 faststart procedure	To disable enter **0**, otherwise enter **1** into the 8bit edit field
H245-Tunnelling	Byte (8bit)	No	212	Disable/Enable H245 tunneling	To disable enter **0**, otherwise enter **1** into the 8bit edit field
Update URL	String	No	215	URL to retrieve update commands from. This is identical to the /url option parameter of the UP1 module	Complete URL as in **http://192.168.0.10/file.txt**. No symbolic host names are supported
Update Poll Interval	Word (16bit)	No	216	Standard poll interval in minutes. This is identical to the **/poll** option parameter of the UP1 module	Interval in minutes

I.4 Disabling the DHCP Client

In certain circumstances, it is convenient to partly disable the DHCP client. This way, the device still gets its IP address from the DHCP server, however, additional settings possibly supplied by the DHCP server are ignored. This is especially useful if in a given setup, some devices are to be configured differently but the majority is still configured by DHCP.

This can be achieved using the following config file options:

config change UP1 /no-dhcp	The update server uses the config files configuration even though there is a configuration supplied from DHCP (innovaphone vendor options "Update URL [215]" and "Update Poll Interval [216]" are ignored).
config change DHCPn /no-vlan	The VLAN settings use the config files configuration even though there is a configuration supplied from DHCP (innovaphone vendor options "VLAN ID [206]" and "VLAN Priority [207]" are ignored).
config change DHCPn /no-vendor	All vendor options are ignored.

I.5 Known Problems with Lengthy Options

The minimum space available for options in a BOOTP/DHCP record is 312 byte. There are some extension mechanisms but only a few DHCP servers support it. The Windows 2000 DHCP server for example does not, but silently truncates options not fitting in this 312 byte space.

I.6 Known Problems with VLAN Configurations

The handling of the 802.1q VLAN ID is a bit tricky. If not hard configured otherwise, the device will request a DHCP lease using the Ethernet switch ports default VLAN ID (that is, it will not send any VLAN header). It will thus receive a DHCP offer dedicated to devices on that VLAN. If this offer includes a VLAN ID option, the device will not accept the offered lease, set the VLAN ID to the value received in the otherwise disregarded offer and start the DHCP process all over again. Now, the DHCP request will be issued on a new VLAN ID. Therefore, the DHCP server will now send an offer dedicated for devices on that new VLAN. This will most probably be a different DHCP scope.

As a consequence, DHCP options on a non-default VLAN must be configured twice. The VLAN ID option itself must be configured in the default VLANs DHCP scope. All other options must be configured in the new VLANs DHCP scope.

Be sure to configure the VLAN in both scopes identically. If not, the DHCP client process will never terminate, since it will always detect a changed VLAN ID, set the VLAN ID and restart the DHCP process.

Here is how DHCP leases are handled in detail:

First boot

The client will broadcast a DHCP DISCOVER, expecting an OFFER from the server including all requested parameters. If the client intends to use the offered lease, it will

issue a request for the offered lease. Once it receives an ACK for the lease requested, it will configure itself accordingly. All lease information is stored in the devices config file using the /laddr option (unless suppressed using /no-keep).

Re-boot

If there is lease information (in the /laddr config file option), the client will broadcast requests for the same lease again. If there is no answer within 30 seconds, the device will configure itself using the parameters in /laddr. It will nevertheless continue to request this lease from the DHCP server again (every 30 seconds, a broadcast will be sent).

If the server acknowledges the old lease, the client will check for changes in the DHCP options and re-configure itself accordingly. Changed options will be saved in the config file.

If the server rejects the lease using a NAK, the client will forget about the lease and continue to operate like it does for the first boot.

First boot with VLAN ID option received

If an offered lease includes the VLAN-ID option and the ID proposed differs from the VLAN ID the devices currently operates with (that is, from the id configured in the devices configuration), the device will change its VLAN ID to the one received in the VLAN-ID option. It will not request the lease though. Instead, it will continue to send DISCOVER requests on the new VLAN ID. If a lease is obtained there, all lease information is stored in the config file as usual.

You can disable the VLAN-ID processing using the /no-vlan option.

Reboot with VLAN ID

If the device finds lease information in the config file at boot time and if there is a VLAN ID different from the devices current VLAN-ID, it will re-configure itself to the new VLAN ID and try to request the saved lease as usual. If the lease is rejected with a NAK by the server, the device will re-configure itself to the pre-configured VLAN ID and try to DISCOVER a new lease as usual.

I.7 VLAN set with LLDP

From version 7.1.X, VLAN is also set with LLDP if provided by the switch. See

I.8 Changing Configuration Options set by DHCP Options

If a device has been configured by DHCP, those parameters cannot be changed. Any attempt to do so will issue a "Reset required" message.

Mitel

Powering connections

mitel.com