Avaya IP-DECT Base Station and IP-DECT Gateway

Installation and Operation Manual

Software version 7.2x

21-604149
Issue 8
02/2016

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website:

https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"**Hosted Service**" means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLEON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. " Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third party components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at:

https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components, to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL

INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com , or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com , or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Introduction

This document describes how to install and operate the following equipment:

- IPBS [1]
- IPBL [2]

The document is intended as a guide for installation, troubleshooting and maintenance purposes and are relevant for the following personnel:

- System administrator
- Service technician

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

For information about supported PBXs contact your supplier.

Related Documentation

System Description, Avaya IP DECT System.

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

Abbreviations and Glossary

Base Station	Common name for IPBS, DECT Base Station (BS3x0) and TDM-DECT Base Station.
DECT	Digital Enhanced Cordless Telecommunications: global standard for cordless telecommunication.
DECT Base Station	Another name for *BS3x0*
TDM-DECT Base Station	Another name for DB1.
DHCP	Dynamic Host Configuration Protocol
DTMF	Dual Tone Multiple-Frequency
FER	Frame Error Rate
GUI	Graphical User Interface
IP	Internet Protocol: global standard that defines how to send data from one computer to another through the Internet
IPBL	Previously called *IP-DECT Gateway* or, more commonly, as "the Blade"
IPBS	Also referred to as *IPBS Base Station*. 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
PBX	Private Branch Exchange: 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
RSSI	Radio Signal Strength Information
RTP	Real-Time Transport Protocol
SST	Site Survey Tool
ToS	Type of Service
VLAN	Virtual Local Area Network

Description

This section gives a general description of the following devices:

- IPBS1, see *IPBS1*
- IPBS2, see IPBS2 on page 12
- IPBL, see IPBL on page 16
- DECT Base Station, see DECT Base Station (BS3x0) on page 19.
- TDM-DECT Base Station, see DB1 on page 21

IPBS1

The following versions of the IPBS1 are available:

- IPBS1 with internal antenna
- IPBS1 with external antennas

IPBS1 with Internal Antenna

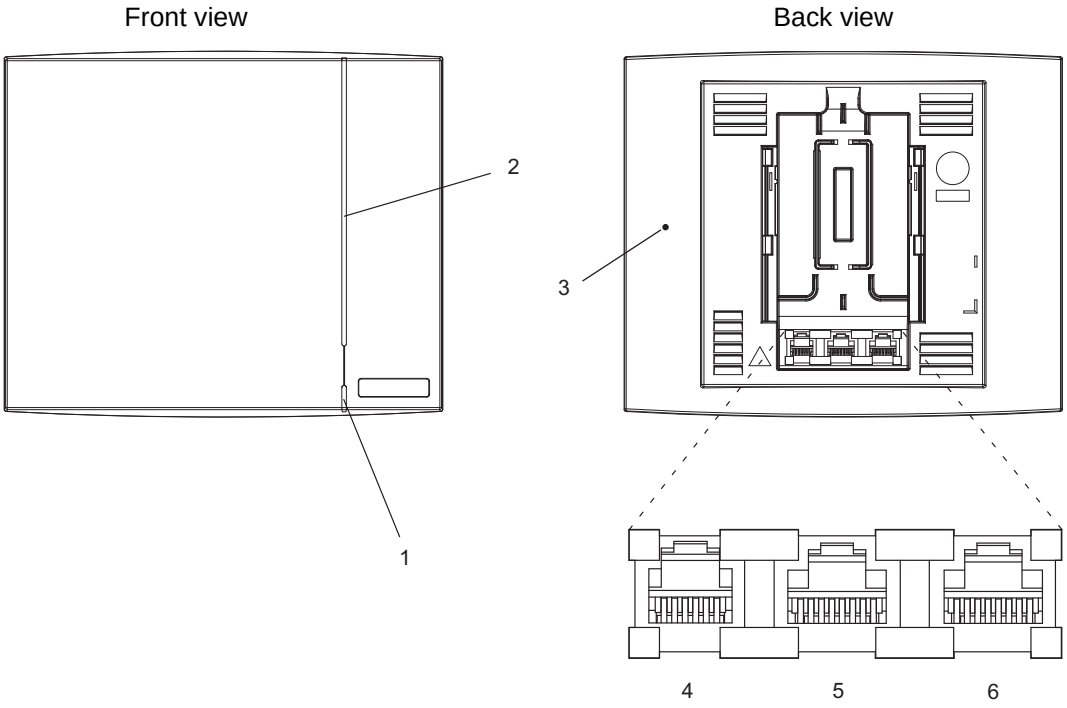


Figure 1. IPBS1 Overview

Contents of the Box

The box in which the IPBS1 is packed contains:

- An IPBS1 with integrated antennas
- A patch cable (approx. 1 m)
- A mounting bracket
- Two screws with wall plugs

Power Distribution

The IPBS1 can be powered using the following methods:

- Power over Ethernet, IEEE 802.3af
- A local AC-adapter

Note: For more information about power distribution, see Power the Base Station on page 44.

Software

The software in the IPBS1 can be updated by downloading new software without disconnecting the equipment. The new software is stored in flash memory. See System Downgrade for IPBS2 and DB1 on page 132 for information.

Connectors

- Two 8-pin RJ45 modular jacks for LAN/PoE and powering
- A 6-pin RJ12 modular jack for factory testing

LEDs

Status of LED1 (lower LED)	Description
Steady Green	Operational
Flashing fast amber	Download of firmware in progress.
Steady Amber	TFTP mode
Alternating red/green	No Ethernet connection

Status of LED2 (upper LED)	Description
Not lit	IPBS1 operational and no traffic on the IPBS1. Air synchronization OK.
Steady green	IPBS1 operational and traffic on the IPBS1. Air synchronization OK.
Slow flashing green	Fully occupied with traffic. Air synchronization OK.
Flashing amber	Air synchronization inadequate and no traffic.
Slow flashing amber	Air synchronization inadequate and fully occupied with traffic.
Steady amber	Air synchronization inadequate and traffic.
Flashing red	No air synchronization - searching for air sync candidates.
Quick flashing red	Download of RFP software in progress.

Note: All amber statuses are warnings that Air synchronization, although still adequate, is fading and might be lost. A flashing red indicates lost Air synchronization.

IPBS1 with External Antennas

The IPBS1 is available with two omni-directional external antennas. Other external antennas can be mounted as well. This section contains the differences between the IPBS1 with internal and external antennas. For all other information see IPBS1 with Internal Antenna on page 10.

Contents of the Box

- The box in which the IPBS1 is packed contains:
- An IPBS1 for external antennas
- Two antennas
- A mounting bracket
- Two screws with wall plugs

> **Note:** The IPBS1 cannot be mounted with the antennas pointing downwards as the mounting bracket does not support it.

Insert the antennas into the IPBS1 before following the installation instructions in Install the Base Station on page 35.

IPBS2

The following versions of the IPBS2 are available:

- IPBS2 with internal antenna
- IPBS2 with internal antenna for IP Office
- IPBS2 with external antennas

The IPBS2 is backward compatible with the IPBS1 when it comes to coverage, functionality, accessories and mounting bracket. If an old IPBS1 has to be replaced you just reuse the mounting bracket and install the IPBS2.

IPBS2 with Internal Antenna

This description also applies to the IPBS2 with internal antenna for IP Office. The following versions are available:

- IPBS2-C3A/1A,
- IPBS2-C4A/1A e
- IPBS2-Z3A/1A

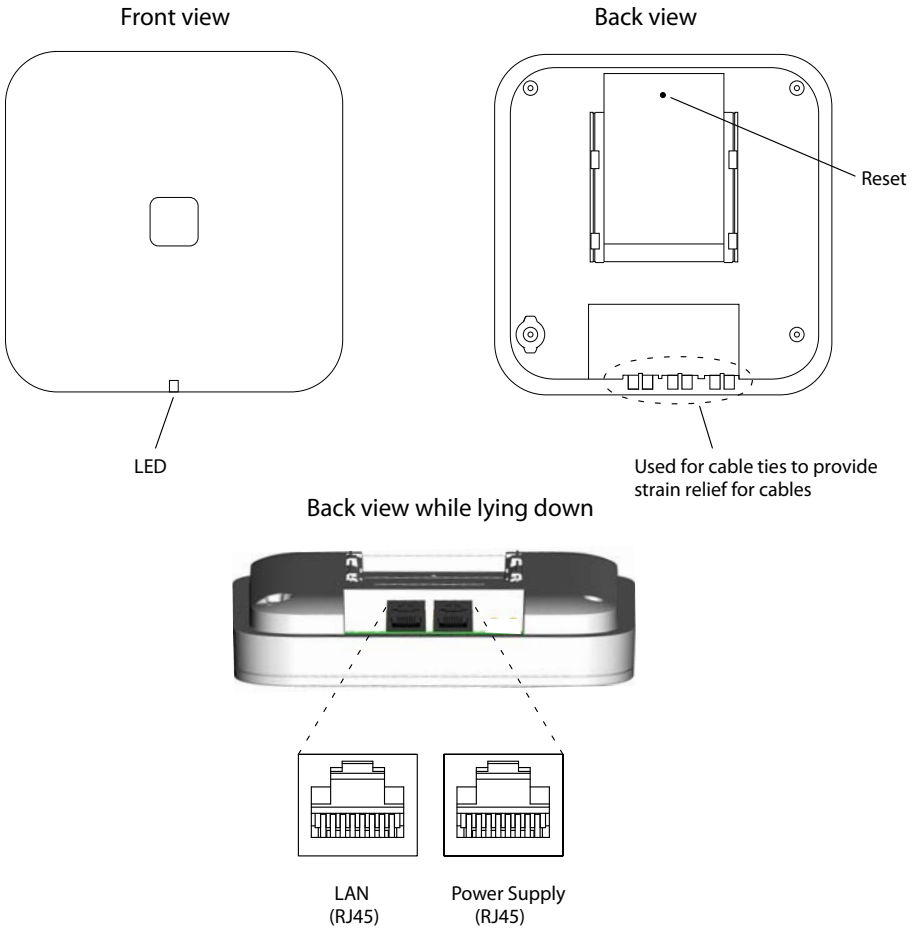


Figure 2. IPBS2 Overview

Contents of the Box

The box in which the IPBS2 is packed contains:

- An IPBS2 with integrated antennas
- A mounting bracket
- Two screws with wall plugs

Power Distribution

The IPBS2 can be powered using the following methods:

- Power over Ethernet, IEEE 802.3af

Note: Brazil is a POE only solution.

Note: For more information about power distribution, see Power the Base Station on page 44.

Software

The software in the IPBS2 can be updated by downloading new software without disconnecting the equipment. The new software is stored in flash memory. See System Downgrade for IPBS2 and DB1 on page 132 for information.

Connectors

- Two 8-pin RJ45 modular jacks for LAN/PoE and powering

LEDs

The IPBS2 has one RGB LED to indicate status. This section describes the different indications and when they shall be used. In the illustrations below: Each blink pattern is represented by a number of blocks where each block is 100 ms. Light grey blocks means that the LED is off. Whenever the indication is changed the new pattern always starts from the first block.

Idle/OK	Solid blue. 	IPBS2 operational and no traffic on the IPBS2.
Starting up/ searching	100 ms blue, 100 ms off. 	The IPBS2 is in start-up phase, e.g. waiting for parameters from Master, or is searching for air synchronization.
Active traffic	400 ms off, 2000 ms blue. 	IPBS2 operational and traffic on the IPBS2.
Fully occupied for speech traffic	400 ms red, 2000 ms blue. 	Fully occupied with traffic.
Software download	400 ms blue, 600 ms off. 	Download of firmware in progress.

Mini firmware	100 ms yellow, 100 ms off. 	The IPBS2 is in mini firmware mode.
TFTP mode	Solid yellow. 	TFTP mode.
Error	100 ms red, 100 ms off. 	No Ethernet connection.
Fatal error	Solid red. 	Fatal hardware error.
Deployment: Good sync	2000 ms blue, 400 ms yellow. 	The IPBS2 is in deployment mode and has good air sync coverage.
Deployment: Bad sync	400 ms blue, 600 ms off, 400 ms blue, 600 ms off, 400 ms yellow. 	The IPBS2 is in deployment mode and does not have adequate air sync coverage.
Deployment: No sync	2000 ms red, 400 ms yellow. 	The IPBS2 is in deployment mode and has no air sync coverage.

IPBS2 with External Antennas

This section contains the differences between the IPBS2 with internal antenna and the IPBS2 with external antennas. For all other information see IPBS2 with Internal Antenna on page 12.

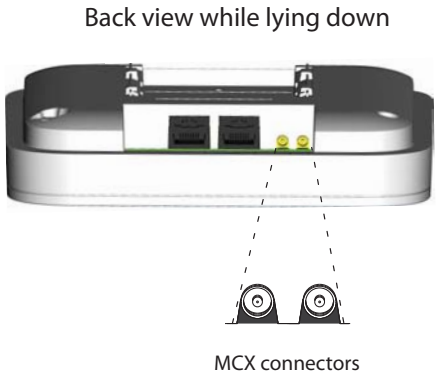


Figure 3. IPBS2 with MCX connectors for external antennas.

Contents of the Box

The box in which the IPBS2 is packed contains:

- An IPBS2 with external antennas.
- A mounting bracket
- An antenna bracket
- Two antenna coaxial cables.
- Two antennas.
- Four screws with wall plugs

IPBL

The following version of the IPBL is available:

- IPBL IP-DECT Gateway 110/230 VAC

Overview

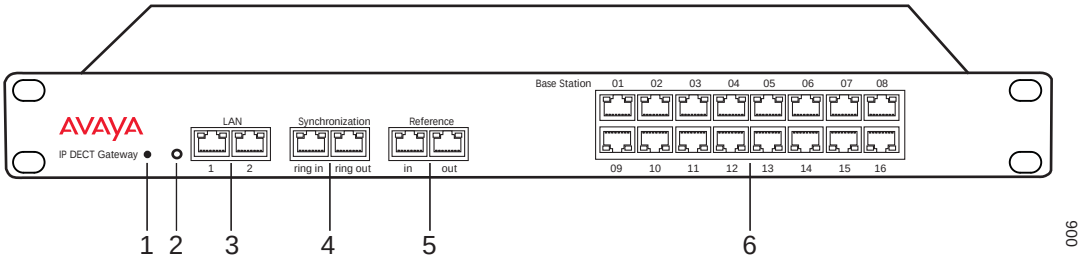


Figure 4. Overview of the IPBL

Pos.	Name	Function
1	Reset	Resets the IPBL, see Reset Using the Reset Button on page 142 for more information.
2	Status LED	Indicates the status on the IPBL.
3	Lan	10BASE-T/100BASE-T Ethernet interface. LAN1 port must be used in the IP-DECT system (LAN2 port is for administration only).
4	Synchronization	Sync ring in and sync ring out interfaces.
5	Reference	Reference sync in and reference sync out interfaces.
6	Base station 01-16	ISDN U_{PN} DECT base station interfaces.

Power Supply

The power supply are located at the rear of the IPBL. The IPBL can be powered using the following alternatives:

- 110/230 VAC (*only IPBL IP-DECT Gateway VAC/VDC*)

Note: For more information, see Power the IPBL on page 50.

Software

The software in the IPBL can be updated by downloading new software without disconnecting the equipment. The new software is stored in flash memory. See System Downgrade for IPBS2 and DB1 on page 132 for information.

LED indication

Status LED	**Description**
Not lit	Not powered, status is not defined.
Flashing slow green	When pressing the reset button.
Flashing fast green	Firmware update or clear config after long reset.
Steady green	Status OK, system is fully operational.
Steady red	Status Fail, system error condition.
Steady amber	System is in TFTP server mode.

Base station LED 	**Description**
Not lit	No U_{PN} link established.
Flashing	U_{PN} link established (activated state), RFP is not operational.
Steady	RFP is fully initialised and operational.

Base station LED 	**Description**
Not lit	No speech activity in RFP.
Flashing	All speech channels occupied in RFP.
Steady	Speech activity in RFP.

Sync/Ref sync LED 	**Description**
Not lit	No sync communication established.
Steady	Communication established.

Sync/Ref sync LED 	**Description**
Not lit	Sync port not selected as input sync source.
Flashing	Sync port selected as input sync source but the sync signal is not in sync.
Steady	Sync port selected as input sync source and the sync signal is in sync.

Lan LED	Description
Not lit	No link.
Flashing	Link present and network activity.
Steady	Link present, but no network activity.

Lan LED	Description
Not lit	10 Mbps operation.
Steady	100 Mbps operation.

DECT Base Station (BS3x0)

The following versions are available:

- BS330-9131 (EU) with Internal antenna
- BS330-9134 (US) with Internal antennas
- BS340-9131 with External antenna

DECT Base Station

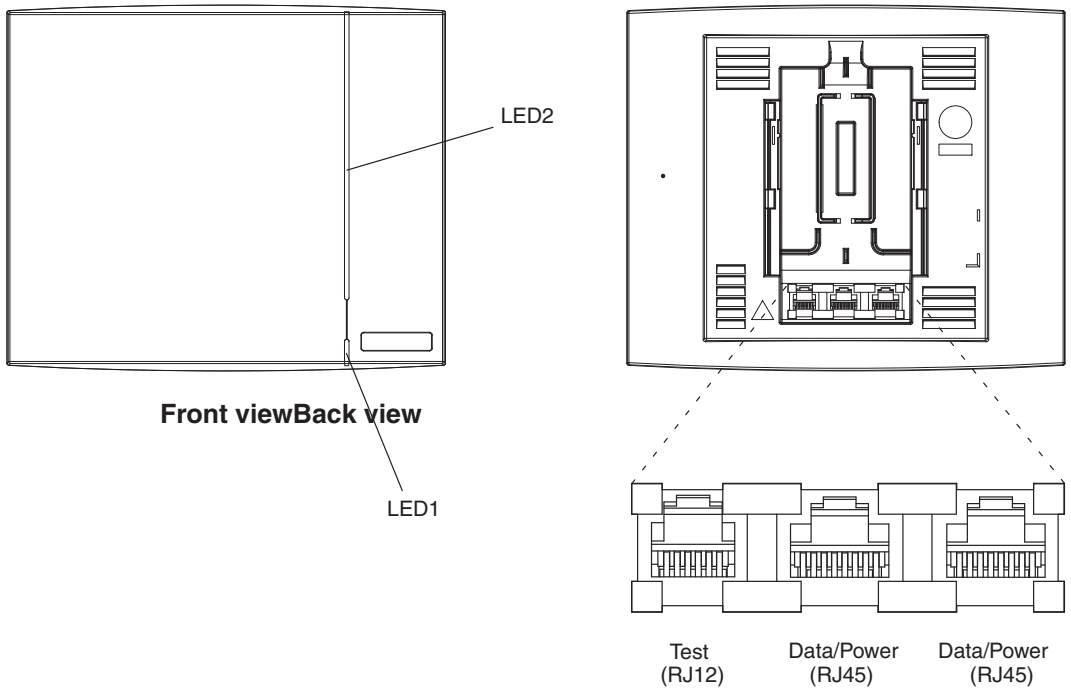


Figure 5. BS3x0 Overview

Contents of the Box

The box in which the base station is packed contains:

- A base station
- Two antennas (only base station with external antenna)
- A mounting bracket
- Two screws with wall plugs

Power Distribution

The base station can be powered using the following methods:

- From the IPBL via the Express Powering Pair (EPP) and data pairs
- With a local AC-adapter

Note: For more information about power distribution, see Power the Base Station on page 44.

Software

The software in the BS3x0 can be updated by downloading new software without disconnecting the equipment. The new software is stored in flash memory. See System Downgrade for IPBS2 and DB1 on page 132 for information.

Connectors

- Two 8-pin RJ45 modular jacks for data and powering
- A 6-pin RJ12 modular jack for factory testing

LEDs

Status of LED1 (lower LED)	Description
Steady Green	Power LED

Status of LED2 (upper LED)	Description
Not lit	Base station operational and no traffic on the base station.
Flashing green	Fully occupied with traffic.
Steady green	Base station operational and traffic on the base station.
Flashing amber	Software is being downloaded to the base station
Steady amber	Base station is OK, but not available (self-test, not initialized, no communication with IPBL)

DB1

The following versions of the DB1 are available:

- DB1 with internal antenna
- DB1 with external antennas

The DB1 is backward compatible with the BS3x0 when it comes to coverage, functionality, accessories and mounting bracket. If an old BS3x0 has to be replaced you just reuse the mounting bracket and install the DB1.

DB1 with Internal Antenna

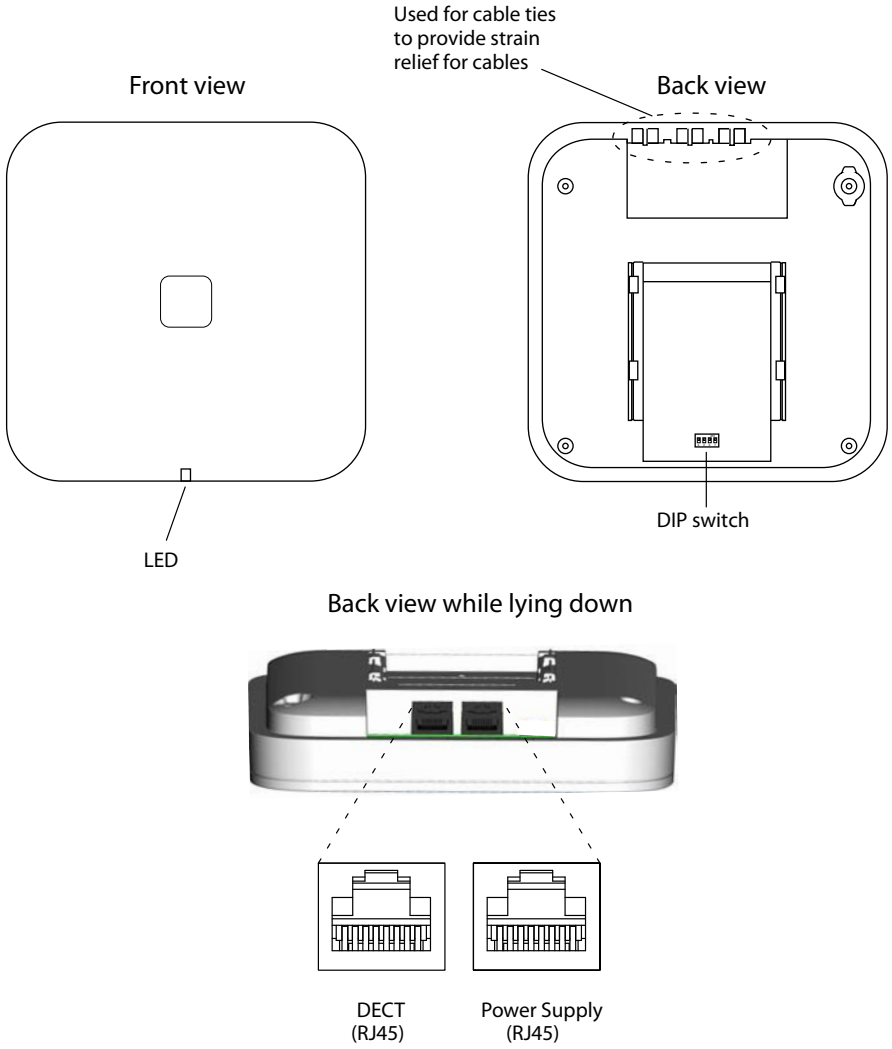


Figure 6. DB1 Overview

Contents of the Box

The box in which the DB1 is packed contains:

- A DB1 with integrated antennas
- A mounting bracket
- Two screws with wall plugs

Power Distribution

The DB1 can be powered using the following methods:

- From the IPBL via the Express Powering Pair (EPP) and data pairs
- With a local AC-adapter

Note: For more information about power distribution, see Power the Base Station on page 44.

Software

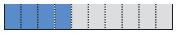
The software in the DB1 can be updated by downloading new software without disconnecting the equipment. The new software is stored in flash memory. See System Downgrade for IPBS2 and DB1 on page 132 for information.

Connectors

- Two 8-pin RJ45 modular jacks for data and powering

LEDs

The IPBS2 has one RGB LED to indicate status. This section describes the different indications and when they shall be used. In the illustrations below: Each blink pattern is represented by a number of blocks where each block is 100 ms. Light grey blocks means that the LED is off. Whenever the indication is changed the new pattern always starts from the first block.

Idle/OK	Solid blue. 	DB1 operational and no traffic on the DB1.
Starting up	100 ms blue, 100 ms off. 	The DB1 is in start-up phase, i.e. waiting to be initialized by the IPBL.
Active traffic	400 ms off, 2000 ms blue. 	DB1 operational and traffic on the DB1.
Fully occupied for speech traffic	400 ms red, 2000 ms blue. 	Fully occupied with traffic.
Software download	400 ms blue, 600 ms off. 	Download of firmware in progress.

Error	100 ms red, 100 ms off.	U_{PN} layer 1 communication error.
Fatal error	Solid red.	Fatal hardware error.

DIP Switches

The DIP switches can be found on the back of the DB1, see figure 6 on page 22.

Note: DIP switch 2, 3 and 4 shall be set to ON.

Set DIP switch 1 to ON or OFF as follows:

DIP switch 1: ON	IPBL mode, when the DB1 is to be connected to an IPBL.
DIP switch 1: OFF	Integral mode, when the DB1 is to be connected to an I5/I55 system.

DB1 with External Antennas

This section contains the differences between the DB1 with internal antenna and the DB1 with external antennas. For all other information see DB1 with Internal Antenna on page 22.

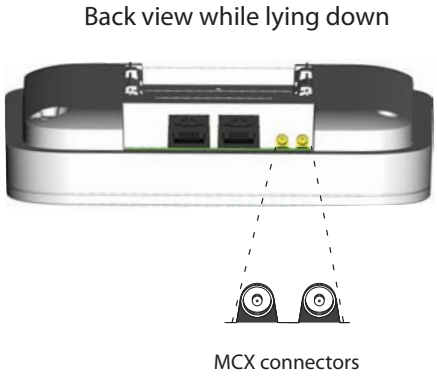


Figure 7. DB1 with MCX connectors for external antennas.

Contents of the Box

The box in which the DB1 is packed contains:

- A DB1 with external antennas.
- A mounting bracket

- An antenna bracket
- Two antenna coaxial cables.
- Two antennas.
- Four screws with wall plugs

AC-adapter

The AC-adapter is used to power a base station locally.

Note: The maximum length of cable from adapter must not exceed 10 meters.

Versions (different type of mains plug)

For European countries except U.K.	Art. no.: 130137B	Order. no.: BSX-0013
For U.K.	Art. no.: 130136B	Order. no.: BSX-0014
For NA	Art. no.: 130138A	Order. no.: BSX-0015
For Australia	Art. no.: 130139B	Order. no.: 660261

IMPORTANT: If local power supply is used for the RFPs, the EPP cable pair must NOT be connected.

Safety Instructions

For safe and efficient operation, observe the guidelines given in this manual and all necessary safety precautions. Follow the operating instructions and adhere to all warnings and safety precautions located on the product and this manual.

- Installation and service is to be performed by service persons only.
- IPBL must be connected to a mains socket outlet with a protective earthing connection.
- IPBL must be mounted in a Restricted Area Location (RAL) in Sweden, Finland and Norway.
- Ensure that the voltage and frequency of the mains power socket matches the voltage and frequency inscribed on the equipment's electrical rating label.
- Never install telephone wiring during a thunderstorm.

  Note: Avoid touching or punching down the IPBS/RFP signal and power pairs as there is 48Vdc or 24Vdc present on these wires at all times.

- Always install the base station conforming to relevant national installation rules.
- Disconnect all power sources before servicing the equipment.
- Use only approved spare parts and accessories. The operation of non-approved parts cannot be guaranteed and may cause damage or danger.
- Only approved power supplies according to valid editions of EN/IEC/CSA/UL/AU/NZS 60950 are to be used when the IPBS/RFPs are powered by local power supplies.

Protection Against Electrostatic Discharge (ESD)

Integrated circuits are sensitive to ESD.To avoid damage caused by ESD, service engineers and other people must handle equipment and boards carefully.

Electronic equipment has become more resistive to ESD, but we see an increase of situations where static electricity can build up. This is caused by an increasing application of man–made fibres like nylon, acrylic, etc. which are capable of generating ESD of 10,000 Volts and more.

Walking across a nylon carpet, even for a few feet, could cause a person to be charged–up to more than 10,000 Volts.
Under these conditions, if a system board or a (C)MOS device is touched it could easily be damaged. Although the device may not be totally defective, it is often degraded, causing it to fail at a later date without apparent reason.

To make sure that equipment and parts are well protected during shipment, special packaging materials are utilized. System boards will be shipped in anti–static bags and (C)MOS devices and other sensitive parts in small shielded boxes.

ESD Handling

In the interest of quality and reliability, it is advisable to observe the following rules when handling system parts:

- Keep parts in their protective packaging until they are needed.
- When returning system parts like EEPROMS to the factory, use the protective packaging as described.
- Never underestimate the damaging power ESD can have and be especially careful when temperatures are below freezing point and during very warm weather in combination with low humidity. Make sure that the environmental conditions remain within the limits specified in the components' data sheets.

IMPORTANT: In the interest of quality and reliability system boards and other parts returned for exchange or credit may be refused if the proper protective packaging is omitted!

Safety Aspects

IP-DECT Base Station

The IP-DECT Base Station meets the valid editions of safety standard EN/IEC/CSA/UL/AU/NZS 60950-1. The system is a class III equipment for stationary wall mounting.

DECT Base Station BS3x0 and TDM-DECT Base Station DB1

The DECT Base Station BS3x0 and TDM-DECT Base Station DB1 meets the valid editions of safety standard EN/IEC/CSA/UL/AU/NZS 60950-1. The system is a class III equipment for stationary wall mounting.

IP-DECT Gateway (IPBL)

The IPBL meets the valid editions of safety standard EN/IEC/CSA/UL/AU/NZS 60950-1.

Regulatory Compliance Statements (EU/EFTA only)

The equipment are intended to be used in the whole EU&EFTA.

The equipment are in compliance with the essential requirements and other relevant provisions of R&TTE Directive 1999/5/EC. The Declarations of Conformity may be consulted at:

http://support.avaya.com/DoC

The IP-DECT Base Stations, BS3x0 Base Station, TDM-DECT Base Station DB1 and IP-DECT Gateway are marked with the label CE.

Regulatory Compliance Statements (USA and Canada only)

FCC compliance statements

The equipment have been tested and found to comply with the limits for a Class B digital device (Base Stations), pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. The equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/tv technician for help.

Information to user

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- this device may not cause harmful interference, and
- this device must accept any interference received, including interference that may cause undesired operation.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

- this device may not cause interference, and
- this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1. l'appareil ne doit pas produire de brouillage, et

2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

IC Requirements for Canada

This Class B digital apparatus (Base Stations) complies with Canadian ICES-003.

Cet appareil numérique (stations de base) de la Classe B conforme á la norme NMB-003 du Canada.

This Class A digital apparatus (IP-DECT Gateway) complies with Canadian ICES-003.

Cet appareil numérique (IP-DECT Gateway) de la Classe A conforme á la norme NMB-003 du Canada.

Modifications

Any modifications not expressly approved by Avaya could void the user's authority to operate the equipment.

Exposure to radio frequency signals

This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. The antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

IP Security

IP Security Terminology

SSL/TLS

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

TLS is a security mechanism based on cryptography (see *Cryptography*) and is used for encrypting communications between users and TLS-based Websites. The encryption is designed as a means to create barriers to eavesdropping and tampering with any transmitted data.

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

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

CSR 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.

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 algorithms 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.

Introduction to IP Security in IP-DECT

A secure system requires more planning than an unsecured system.

Secure Web Access (https)

For IP-DECT devices

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

For more information see Configure the HTTP settings on page 115 .

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 84.

2. Certificate Handling Options with Device Certificates

There are three 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 86.

- 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 87.

- 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 88.

IP-DECT Administrative Functions

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 Configure the HTTP settings on page 115.

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 Certificates on page 84.

Configuration - Secure RTP

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

For more information see Secure RTP on page 102.

Installation of the Base Station

This section describes how to install the IPBSs, BS3x0 and DB1. All three base stations can be fixed to a wall, a ceiling, a pole or a beam, by means of the mounting bracket included. When fixing the base station to a wall or ceiling the included plugs and screws must be used. When fixing it to a pole or beam a strap or a flexible metal band must be used, this is not included.

Note: Fixing the base station to metal surfaces requires special consideration and is not recommended for several reasons. If this is unavoidable try to ensure a distance between the base station and the metal surface of, preferably, 1 meter.

Base Station Cabling

Recommended base station cable is a standard CAT5 unshielded ethernet cable with minimum 26 AWG copper conductors, this cable is also used for powering the base station. It is assumed that installation personnel know how to crimp RJ45 connectors to a cable.

Note: Since the distance between the base station and the wall is limited, a RJ45 modular jack without cable retention must be used.

Note: Ensure that during the installation of an base station, each base station is given an extra length (5-10 metres) of cable because it is possible that it will have to be moved for one reason or another.

Install the Base Station

The base station can be mounted vertically or horizontally. Mount the base station at places and positions as determined in the base station plan, see the applicable System Planning documentation for IP-DECT. The base station must be placed in a way that it is not facing large metal objects such as large heating pipes.

Fix the Mounting Bracket to a Wall

Fix the mounting bracket (see figure 8 on page 36) to the wall as follows:

1. Hold the mounting bracket with its flat side against the wall with the text ‘TOP’ upwards and mark the two holes. The minimum distance between the upper hole and the ceiling or any object above the base station must be at least 65 mm for IPBS1 and 100 mm for IPBS2 and DB1, see figure 8 on page 36. If the distance is less than 65/100 mm, the base station cannot be slid onto the bracket.
2. When using wall plugs: Drill the two holes using a ∅ 6 mm drill and insert the included wall plugs.

3. Position the mounting bracket with its flat side to the wall and fasten it with the two included ∅ 3.5 mm screws.

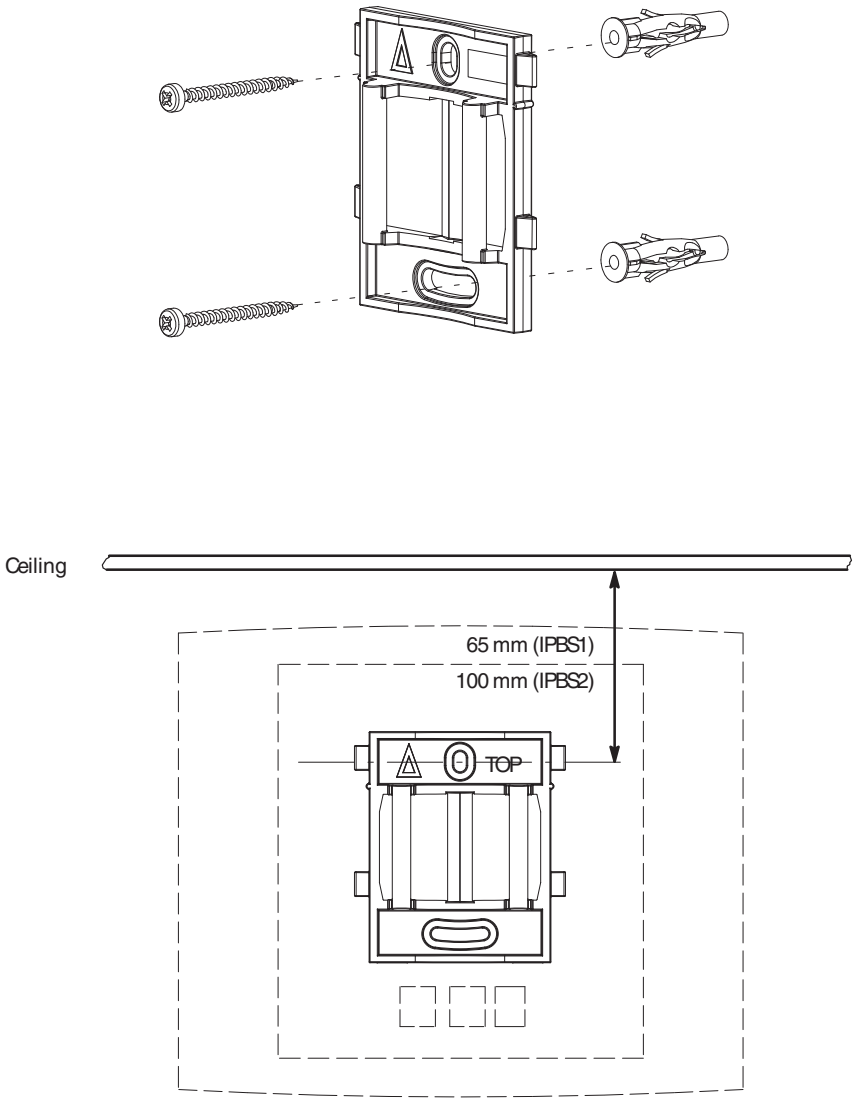


Figure 8. Fixing the mounting bracket to a wall.

Fix the Mounting Bracket to a Ceiling

Fixing to a ceiling is done in the same way as the a wall, see *Fix the Mounting Bracket to a Wall*. When the base station has to be positioned above a suspended ceiling, make sure that the front of the base station points downwards.

Fix the Mounting Bracket to a Pole or Beam

The mounting bracket can be fixed to a pole (diameter ≥ 45 mm) or a beam (wider than 50 mm) by means of a strap or flexible metal band less than 30 mm wide. The strap or flexible metal band is not included in the box.

1. Fix the mounting bracket to a pole or beam using the metal band, see figure 7 on page 37.

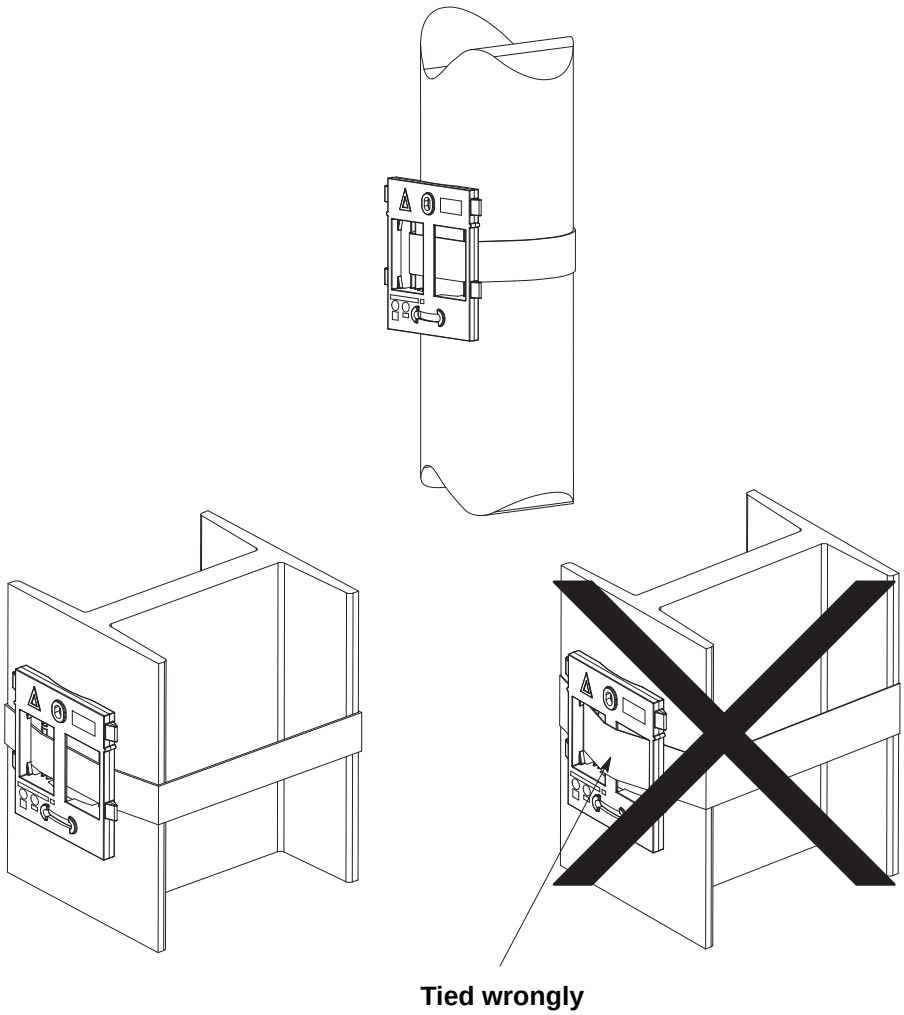


Figure 9. Fixing the mounting bracket to a pole or beam.

Use the Cable Ducts for IPBS1

When the base station IPBS1 is mounted to the wall, cable ducts can be used to route the wiring through.

1. Fix the cable duct to the wall in one of the positions shown in figure 8 on page 38.

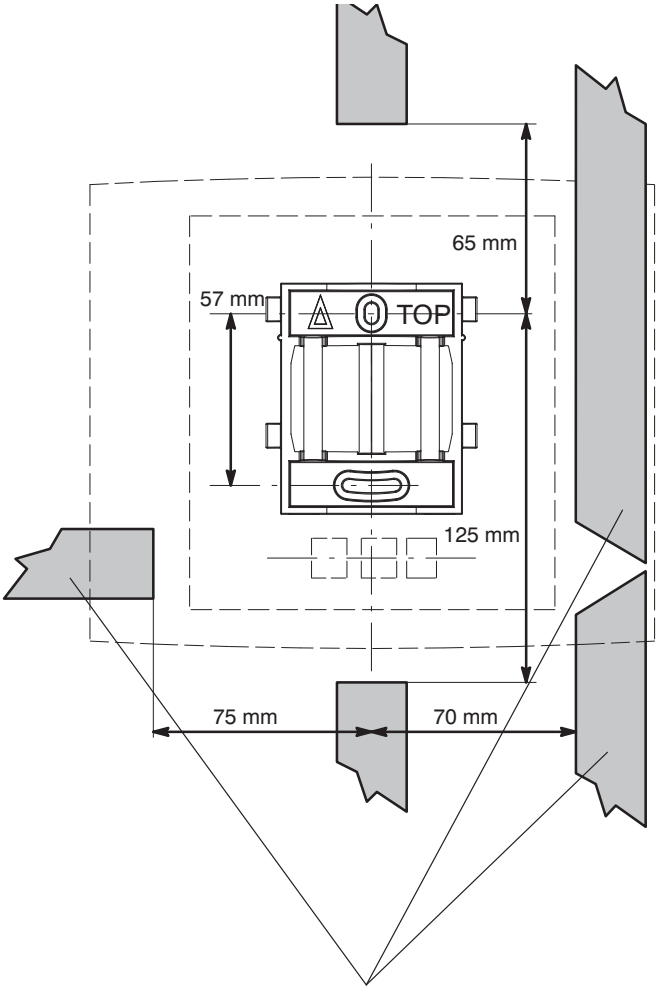
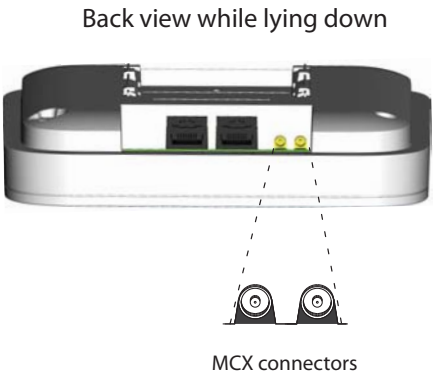


Figure 10. Minimum distances between a cable duct and the mounting bracket

Connect External Antennas (only IPBS2 and DB1)

1. Position the included antenna bracket above the mounting bracket with a minimum distance of 74 mm (250 mm maximum) and mark the two holes for the antenna bracket, see figure 11 on page 40 (1).
2. When using wall plugs: Drill the two holes using a ∅ 6 mm drill and insert the included wall plugs.
3. Position the antenna bracket to the wall and fasten it with the two included ∅ 3.5 mm screws.

4. Mount the two included coaxial cables on the antenna bracket figure 11 on page 40 (2). Fasten the coaxial cables with the lock nuts which are found on the coaxial cable antenna connectors.
5. Mount the antennas on the antenna connectors (2).
6. Connect the coaxial cables to the MCX connectors on the base station.



7. Mount the base station (3), see 4. Mount the Base Station on page 44.

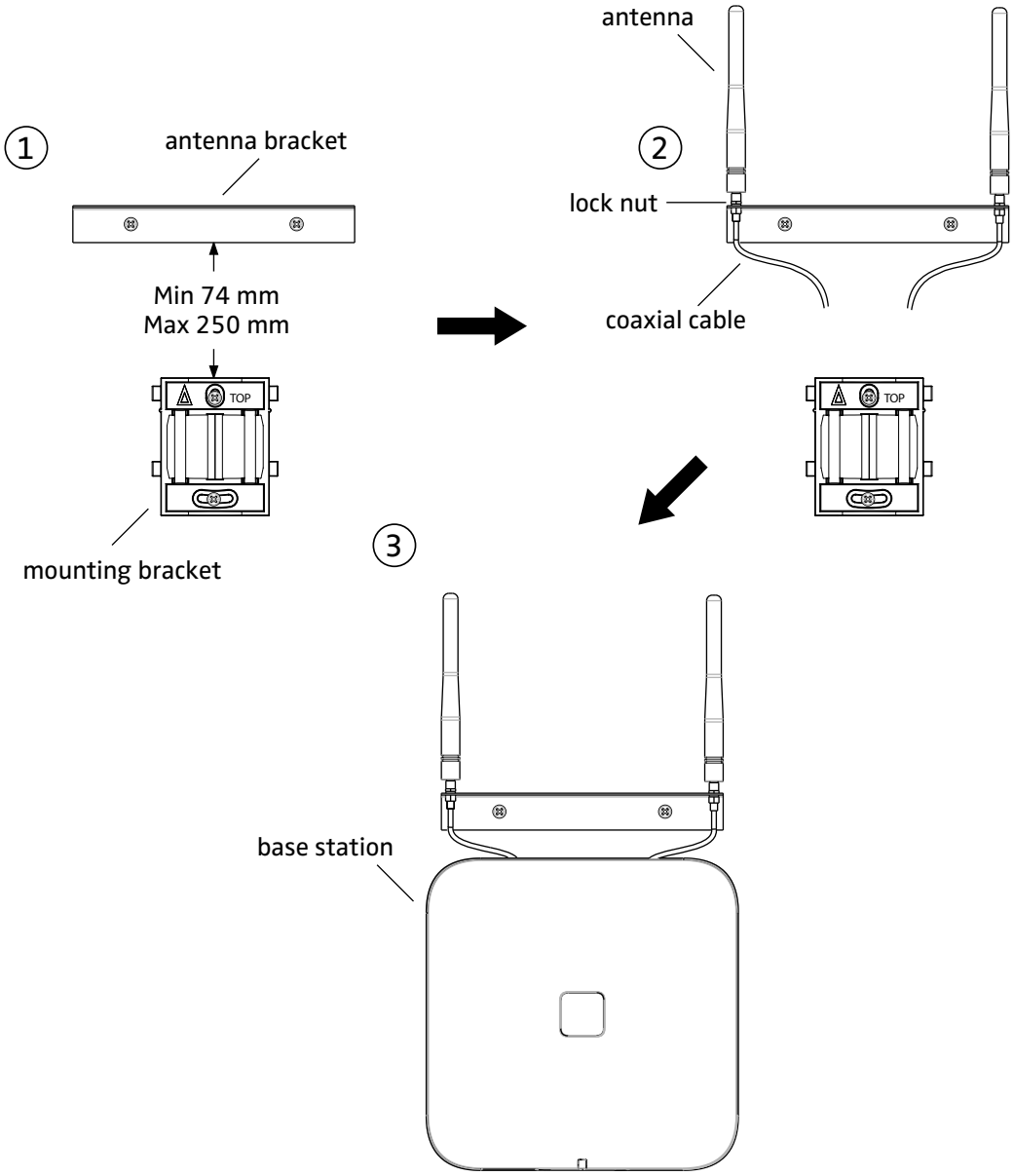


Figure 11. Connect external antennas.

Secure the Cable

For safety reasons secure the base station cable to a convenient point at about 30 cm from the base station.

If for some reason the base station drops, it is secured by the cable.

Pinning

1. Cut the cable to the correct length and connect the cable to a RJ45 modular jack.
2. For information on the pinning of the data jack see the following:

- IPBS, Pin the IPBS Cable on page 42.
- BS3x0 and DB1, Pin the BS3x0/DB1 Cable on page 43.

Tip:
Do **not** plug the connector in the base station yet.

Note: Since the distance between the base station and the wall is limited, a RJ45 modular jack without cable retention must be used.

Pin the IPBS Cable

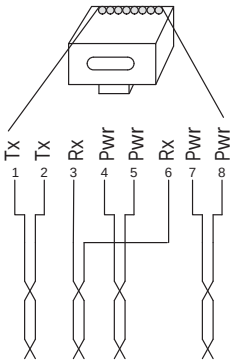


Figure 12. Connector pinning of the LAN/PoE connector, power feed over the spare cable pairs.

RJ45 modular jack

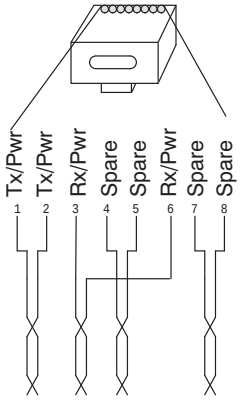


Figure 13. Connector pinning of the LAN/PoE connector, power feed over the Rx/Tx data cable pairs.

Pin the BS3x0/DB1 Cable

Figure 11.

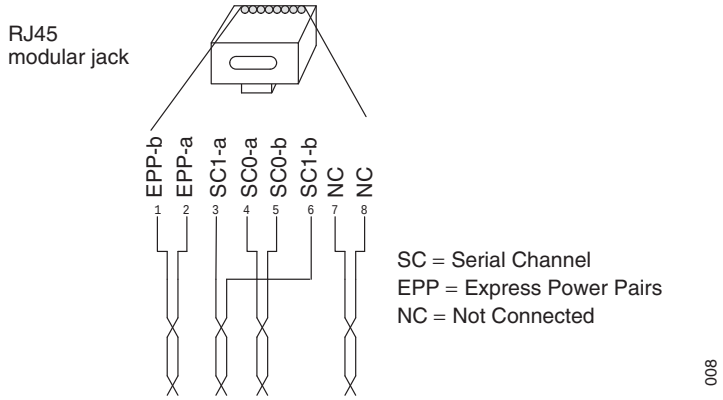
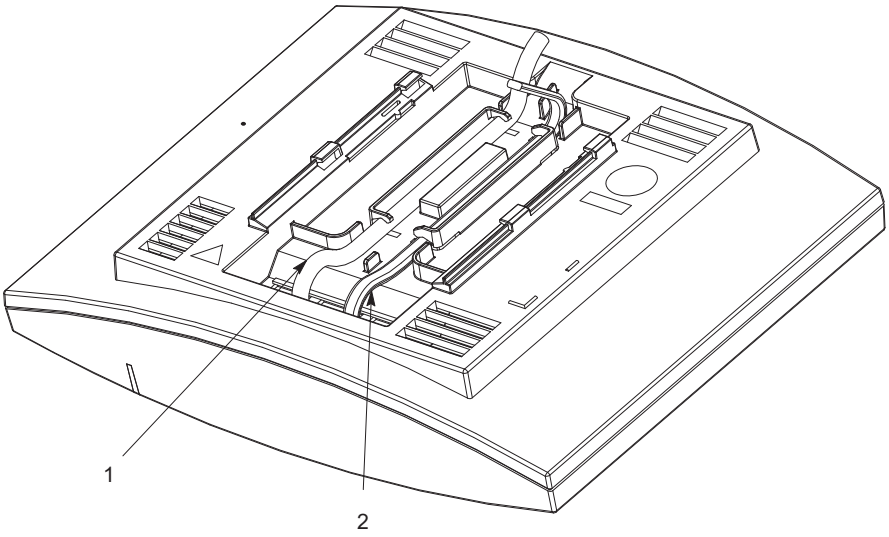


Figure 14. Connector pinning of the Data connector

IMPORTANT: If local power supply is used, the EPP cable pair must NOT be connected.

Connect the Base Station Cables

1. Only for IPBS1: If it is required that the cables enter the base station centrally from above, guide the cables through the recess in the middle of the base station as shown below.



2. Plug the modular jack of the data cable into one of the data/power connectors.
3. When an AC-adapter is used:
   - Plug the modular jack of the AC-adapter in one of the data/power connectors.
   - Plug the AC-adapter into a wall-outlet.

4. Mount the Base Station

Hold the base station flat against the mounting bracket and move it downwards until it clicks, see below.

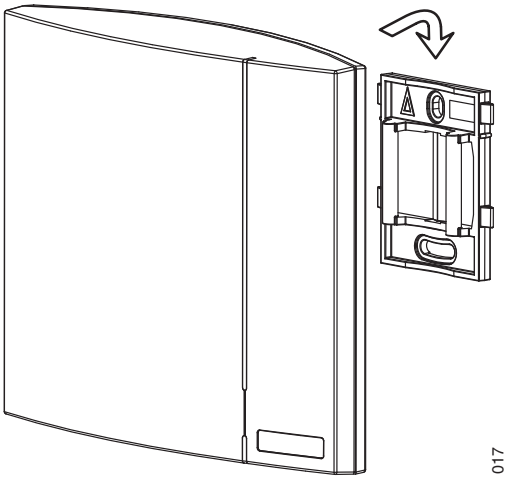


Figure 15. Mounting of the IPBS.

Power the Base Station

The base station is powered the following ways:

- Power over Ethernet (only IPBS).
- Power over Express Powering Pairs (EPP) and data pairs (only BS3x0 and DB1)
- By a local power supply.

> **Note:** Do not power the base station using both power supplies. Parallel powering will not harm the base station but it can disturb the signalling.

Power the IPBS over Ethernet

The IPBS supports Power over Ethernet, IEEE 802.3af, class 2. The power source will allocate 7W to the IPBS. This must be regarded when planning the powering of the IPBSs so that the power limit of the PoE power source is not exceeded.

The PoE standard supports two ways of feeding the power:

- Power over the Rx/Tx data pairs.
- Power over the spare cable pairs.

Both power feed methods are supported in the IPBS, it is also insensitive to change of the polarity.

Power the BS3x0 and DB1 over Express Powering Pair (EPP) and data pairs

When a base station is powered remotely via the IPBL, the maximum length between the base station and the IPBL depends on the supply voltage, the number of twisted pairs used and the wire size. The length of the cable should never exceed "data-limited" length of the cable, see Appendix B: Update Script for Configuration of Kerberos Clients on page 161.

Power the Base Station with a Local Power Supply

Powering the base station with a local power supply can be done using the second data/power inlet on the base station. The base station can be powered individually by an AC-adapter. The AC-adapter is provided with an 8-pin RJ45 plug that can be plugged into the *Power Supply* jack. For specification see AC-adapter on page 25.

Note: Only approved power supply according to valid editions of EN/IEC/CSA/UL/AU/NZS 60950 is to be used when the base station is powered by a local power supply.

Installation of the IPBL

This section describes how to install the IPBL.

Install the IPBL

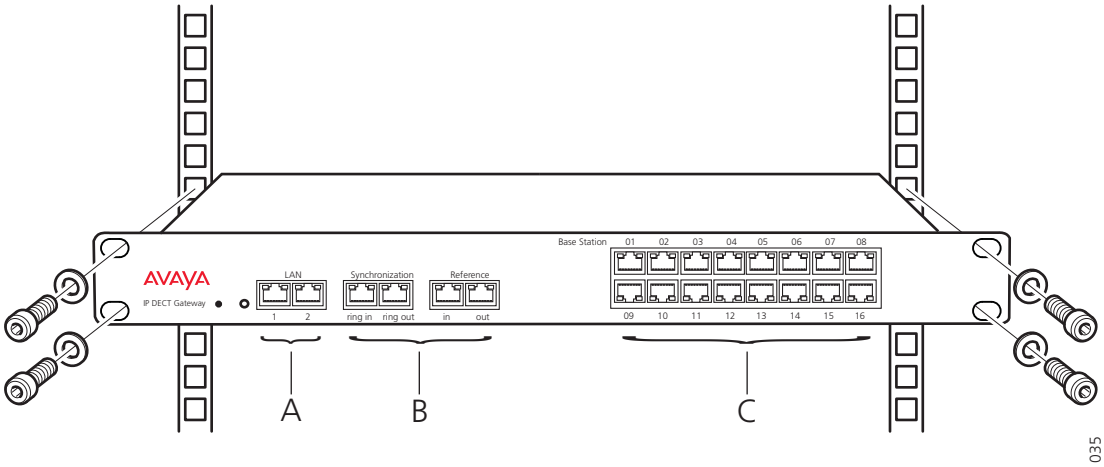


Figure 16. Install the IPBL

The main steps of the installation is described below:

1. Install the IPBL in a standard 19’’ rack.
2. Pin the cables, see Pin the IPBL Cable on page 48.
3. Attach the power cable, see Power the IPBL on page 50.
4. Connect the cables in the following order:

- Ethernet cable (A) LAN1 port must be used in the IP-DECT system (LAN2 port is for administration only).
- Synchronization cable (ring sync, reference sync) (B)
- Base station cable (RFP cable) (C)

IMPORTANT: The connected RFPs must not be connected to protective earth.

- Monitor the total current consumption from the GUI. See Environment on page 140. Make sure it not exceeds the following values:

- Max current consumption is 1,9/0,9 A when supplied with 110/230 VAC.

Note: The IPBL current consumption is 0,3 A and is included in max current consumption.

For more information of power consumption of the RFPs, see Appendix B: Update Script for Configuration of Kerberos Clients on page 161.

Pin the IPBL Cable

All data cables used for the IPBL is standard CAT5 unshielded cable. It is assumed that installation personnel know how to crimp these connectors to a cable.

Synchronization Cable

The maximum cable length between two IPBLs must not exceed 2000 meters.

- Cut the cable to the correct length.
- Connect the cable to a RJ45 modular jack. For information on pinning, see figure 12 and figure 13.
- Label the cable.

Sync IN

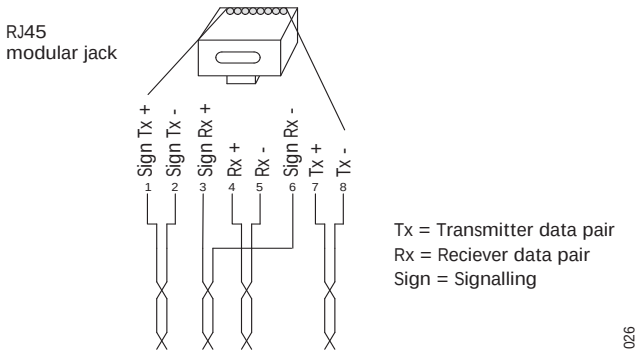


Figure 17. Connector pinning of the Sync IN cable

Sync OUT

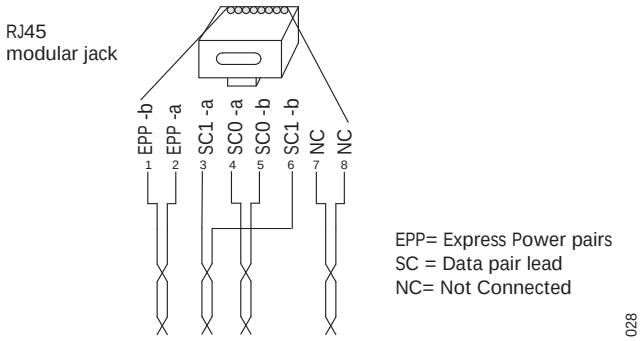


Figure 18. Connector pinning of the Sync OUT cable

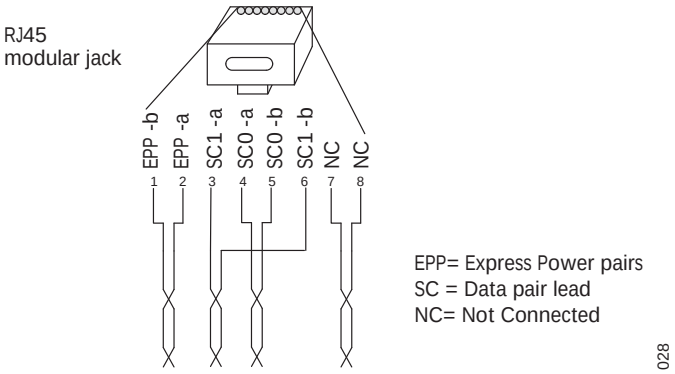
RFP Cable

The RFP cable connects the IPBL with the RFPs. The maximum cable length between IPBL and a single RFP must not exceed 1500 meters.

> **Note:** Ensure that during the installation, each RFP is given an extra length (5-10 metres) of cable because it is possible that it will have to be moved for one reason or another.

1. Cut the cable to the correct length.
2. Connect the cable to a RJ45 modular jack. For information on the pinning, see below.

> **IMPORTANT:** If local power supply is used for the RFP, the EPP cable pairs must NOT be connected.

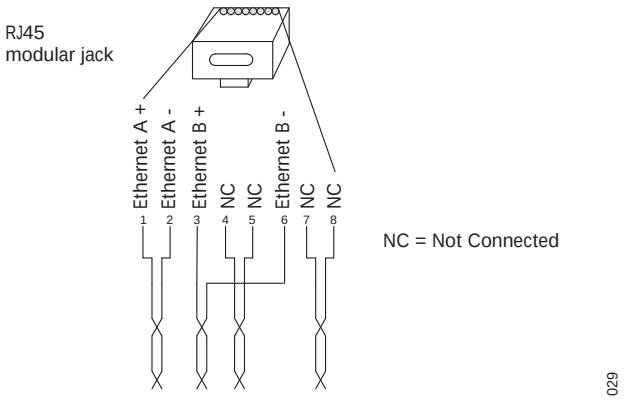


3. Label the cable.

LAN Cable

Note: The TX/RX crossover/straight cable feature does not work in the IPBL. It must be a straight cable between the IPBL and the switch port.

1. Cut the cable to the correct length.
2. Connect the cable to a RJ45 modular jack. For information on the pinning, see below.



3. Label the cable.

Power the IPBL

The IPBL power supply connector is located at the rear. The power supply feeds both the IPBL and the connected RFPs. The IPBL is powered with 110/230 VAC, 60/50 Hz.

110/230 VAC

- The 110/230VAC (100 – 240 VAC) power input is protected against overload by a 4A fuse. The IEC 60320 type C14 (male) connector consists of:
  - live lead (1)
  - neutral lead (2)
  - protective earth (3)

Figure 14.

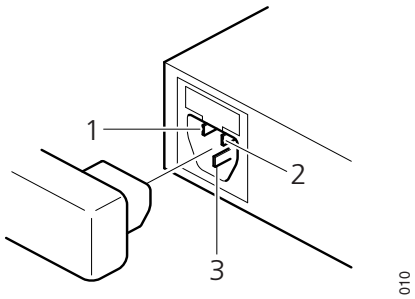


Figure 19. Pinning of the 110/230 VAC power supply

1. Connect the power cable on the IPBL.
2. Connect the power cable in a wall socket with protected earth.
3. The IPBL is switched on.
4. Connect the cables in the following order:
   - Ethernet cable (A) LAN1 port must be used (LAN2 port is for administration only).
   - If you enable RSTP, both the ports are utilized by the system. See Enabling RSTP (only for IPBL) on page 132
   - Synchronization cable (ring sync, reference sync) (B)
   - Base station cable (RFP cable)

   Note: The connected RFPs must not be connected to protective earth.
5. Monitor the total current consumption from the GUI.
6. Ensure that the current consumption does not exceed the following values:

   Note: Max current consumption is 1,9/0,9 A when supplied with 110/230 VAC. The IPBL current consumption is 0.3 A.

Configuration

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

1. Configure the Master, see Configure the Master on page 64.
2. Configure the Standby Master, see Configure the Standby Master on page 65.
3. Configure the slaves/radios, see Configure the Slave/Radio on page 66.

Note: When the IPBS/IPBL is reconfigured to another role (for example from being a Standby Master to becoming a Master), a factory reset should be done. See Reset Using the Reset Button on page 142.

Requirements

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

- PC
- 10/100base-T Ethernet connection

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

The GUI has been tested with Internet Explorer 7.x and Firefox 3.x, but can also be operated with other browsers in compliance with the requirements above.

Access the GUI

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) and ipbl-xx-xx-xx (IPBL), where xx-xx-xx is the end of the MAC address.

Note: The IPBL name is always ipbl-xx-xx-xx regardless if LAN1 (MAC xx-xx-xx-xx-xx) or LAN2 (MAC yy-yy-yy-yy-yy) is used.

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 Determine the IP Address on page 54.

Access the GUI and change the default password as described in Change the Default Password on page 56.

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

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/IPBL. If there is no DHCP server in the network, the IPBS/IPBL 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 Set DHCP Mode on page 91.

> **Note:** After the first startup the DHCP mode should be changed from "automatic" to either "client" or "off", see Set DHCP Mode on page 91.

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

- In a Network without a DHCP Server on page 54.
- In a Network with a DHCP Server on page 55.

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/IPBL has been used before, it must be restored to factory default settings by performing a long hardware reset, see Reset Using the Reset Button on page 142.

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

   > **Note:** For IPBS, a power adapter must be used.
   > For IPBL, make sure to use the LAN1 port.

2. Ensure that the computer has an IP address within the same IP address range as the IPBS/IPBL (192.168.0.1).
3. Perform a hardware reset by shortly pressing the reset button.
   The IPBS/IPBL 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/IPBL GUI.

5. After the first startup, do the following:
   On the IPBS: Select LAN1 > DHCP
   On the IPBL: 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's MAC address can be found on the label on the box and on the label on the backside. The IPBL's MAC address can be found on the label on the box. The hexadecimal numbers (xx-xx-xx-xx-xx-xx) represent the MAC address.

Note: Make sure to use the LAN1 port for the IPBL.

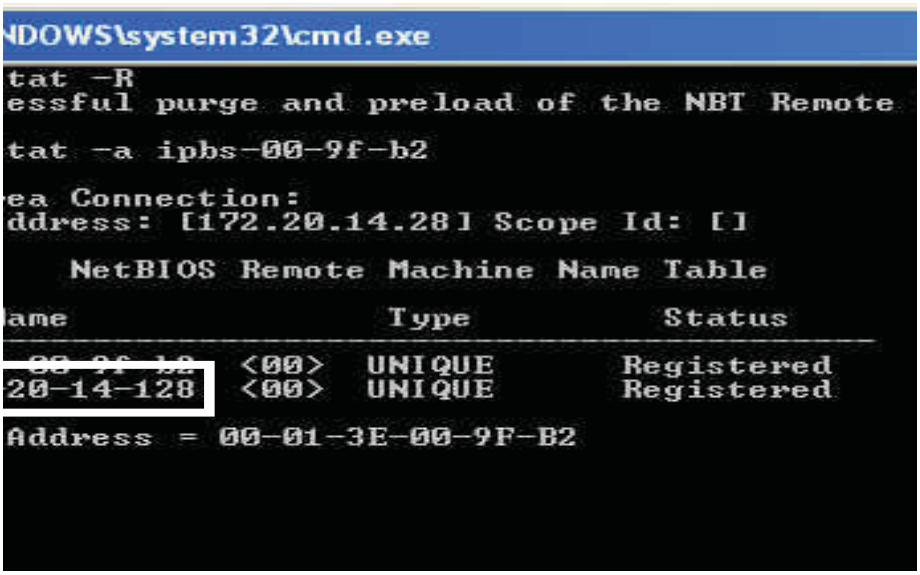
Note: In order to determine the IP address it is necessary that the computer is connected to the same LAN (broadcast domain) as the IPBS/IPBL.

Determine the IP address following the steps below:

Note: If the IPBS/IPBL has been used before, it must be restored to factory default settings by performing a long hardware reset, see Reset Using the Reset Button on page 142. 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**
   For IPBL: **C:\>nbtstat -a ipbl-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/IPBL do the following:
   On the IPBS: Select LAN1 > DHCP
   On the IPBL: Select LAN1 > DHCP
6. In *Mode* drop-down list, change the DHCP mode from "automatic" to "client" or "disabled".

Change the Default Password

1. Enter the IP address determined in *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".

GUI Web Access

Login Page

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

NOTE: Logging out of the IPBS/IPBL application is done by closing the web browser, to be completely logged out.

Access Levels

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

- 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	*Auditors*
User Administrators	• Add, update and remove users	User Administration	User Administrators on page 58
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	System Administrators on page 59

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.

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 System Administrators on page 59 for more information.

User Administrators

IPBS/IPBL is not supplied with preinstalled user administration accounts. Therefore, the first user administration account must be created by a system administrator (see System Administrators on page 59). If additional user administration accounts are needed they must also be created by a system administrator, see Managing User Administrators on page 61.

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 Access the GUI on page 53 and access the device using a web browser.
2. Click the link labelled *User Administration.*
3. A login window is opened.
4. Enter user name and password for a user administrator.
5. Click "OK" to login.
6. Click the "Show" link.
7. The User Administration page is displayed.

   See the figure below for a sample.

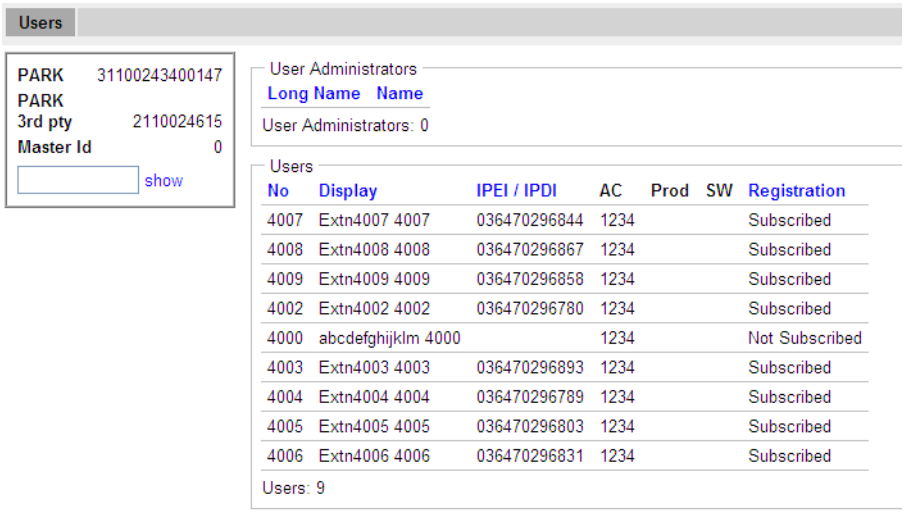


Figure 20. User Administration Sample.

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 61.
- *Users* in the lower right section. Refer to Add Users on page 68.

System Administrators

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

Log in as System Administrator

To login as a system administrator:

- Follow Access the GUI on page 53 and access the device using a web browser.
- Click the link labelled *System Administration.*
- A login window is opened.
- Enter user name and password for a system administrator.
- Click "OK" to login.

Following tasks can be done:

- Managing the default system administrator account, see The Default System Administrator Account on page 60.

- Managing additional system administrator accounts, see Additional Administrator Accounts on page 60.

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 Centralized Management of Admin/Auditor Accounts Using Kerberos on page 72).

To create an additional administrator account, do as follows:

1. Log in as system administrator (see Log in as System Administrator on page 59).
2. Select General > Kerberos Server
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 Access Levels on page 57 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 59).
2. Select General > Kerberos Server
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 Access Levels on page 57 for a description of access levels.)
4. Click "OK".

The account row is updated.

To delete an additional administrator account, do as follows:

5. Login as system administrator (see Log in as System Administrator on page 59).
6. Select General > Kerberos Server
7. On the row to be deleted, select the *Delete* check box.
8. Click "OK".

The account row is deleted.

Managing User Administrators

Create a User Administrator

IPBS/IPBL 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 59).
2. Select "Users".
3. Click "show" .
4. The *User Administration* page (see figure 20 on page 59 for a sample) is displayed.
5. Click "new".
6. Select the "User Administrator" radio box. The window layout transforms.
7. Enter a long name.
8. Enter a name (NOTE: This field is used for login).

9. Enter a password.
10. Confirm the password.
11. Click "OK".

View and Modify a User Administrator

1. Login as System Administrator (see System Administrators on page 59).
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 System Administrators on page 59).
2. Select "Users".
3. Click "show".
4. In the *User Administrators* section, click the hyperlink to be deleted below the *Long Name* heading. An *Edit User* window is opened.
5. Click "Delete".

The User Administrator is deleted and the windows is closed.

Simplified GUI

Note: This feature is only applicable for IPBS.

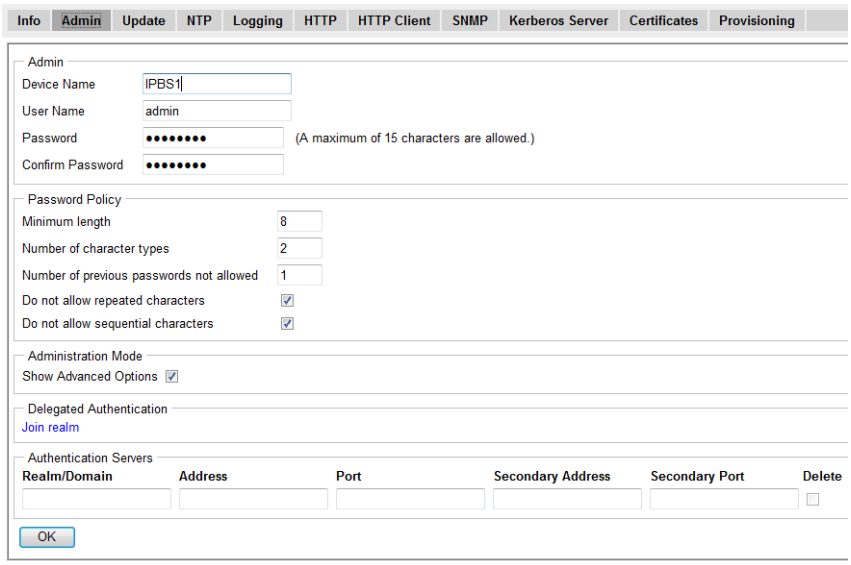
The simplified Graphical User Interface (GUI) makes it very easy to configure small IP-DECT systems. Only those GUI pages are visible which are needed for a basic configuration so in the basic administration interface the required configuration settings are kept to a minimum.

The basic administration interface is the default setting for Compact IPBS.

Change the Interface to Advanced View

To change the basic administration interface to the advanced view do the following:

1. Select General > Admin.
2. In the *Administration Mode* section select the "Show Advanced Options" check box.
3. Click "OK".
4. Refresh the web browser to make the hidden sub menus and tabs visible.



Change the Interface to Basic View

To change the advanced administration interface to the basic view do the following:

1. Select General > Admin.
2. In the *Administration Mode* section, clear the "Show Advanced Options" check box.
3. Click "OK".
4. Refresh the web browser to decrease the number of visible sub menus and tabs.

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 Operation on page 71.

1. Determine the address and access the GUI, see Access the GUI on page 53.
2. Change the default password, see Change the Default Password on page 56.

   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 Configure LDAP Server on page 96.

3. Set a static IP address and set DHCP to off, see Set a Static IP Address on page 92.
4. Set the mode to Active or Mirror, see Select Mode on page 103.
5. Perform a reset to restart the IPBS/IPBL in Master mode, see Reset on page 141.
6. Select DECT > System and enter password.
7. Select system name and password, see Change System Name and Password on page 99.
8. Set default language, see Set Default Language on page 100.
9. Select supplementary services, see PARI on page 108.
10. Set frequency band, see Set Frequency Band on page 100.
11. Configure the Master settings, see Configure Gatekeeper on page 104.
12. Set the Master IP address to 127.0.0.1, see PARI on page 108.
13. Perform a reset to restart the IPBS/IPBL in Master mode, see Reset on page 141.

If problem to access the Master from a certain PC after the reset;

- Open a command window in windows by selecting Start > Run and enter "cmd" in the Open: text field.
- Enter the following commands

arp -d	(Delete the arp cache)
nbtstat -R	(Empty the nbtstat cache)

- Restart the web browser.

14. Select supplementary services, see PARI on page 108.
15. Assign PARI, see PARI on page 108.
16. Enter SARI, see SARI on page 108.
17. Enter AIWS2 IP address, see Configure Messaging on page 111

18. Configure air synchronization, see Configure Air Synchronization on page 109.
19. Enter the Time Server address, see Trust List on page 84.
20. Reset in order to make the configuration changes take effect, see Reset on page 141.

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 Operation on page 71.

1. Determine the address and access the GUI, see Access the GUI on page 53.
2. Change the default password, see Change the Default Password on page 56.
3. 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 Configure LDAP Replicator on page 97.
4. Set a static IP address and set DHCP to off, see Set a Static IP Address on page 92.
5. Enter system name and password, this should be the same system name and password as in the Master. See Change User Name and Password on page 72.
6. Enter Primary Master IP Address.
7. Set the mode to Standby Master, see Select Mode on page 103.
8. Configure the Master settings, see Configure Gatekeeper on page 104.
9. Enter Master IP address, see PARI on page 108.
10. Select supplementary services, see PARI on page 108.
11. Assign PARI, see PARI on page 108.
12. Configure air synchronization, see Configure Air Synchronization on page 109.
13. Enter WSM IP address, see Configure Messaging on page 111.
14. Enter the Time Server address, see Trust List on page 84.
15. Configure LDAP replicator, enter the IP address, user name and password to the LDAP server. Alternative LDAP server must not be entered. Check the Enable check box, see Configure LDAP Replicator on page 97.
16. Reset in order to make the configuration changes take effect, see Reset on page 141.

If problem to access the Standby Master from a certain PC after the reset;

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

- Enter the following commands
  arp -d(Delete the arp cache)
  nbtstat -R(Empty the nbtstat cache)
- Restart the web browser.

Configure the Slave/Radio

This section describes how to configure the Slave. Each configuration step is briefly described in the step list below, for more detailed information see the corresponding subsection in Operation on page 71.

> **Note:** When one Slave is configured, the configuration can be saved and uploaded to the other Slaves in the system.

1. Determine the address and access the GUI, see Access the GUI on page 53.
2. Change the default password, see Change the Default Password on page 56.
3. Set DHCP mode to "Client", see Dynamic IP address using DHCP on page 93.
4. Enable the Radio in the IPBS/IPBL, see Enable the Radio on page 107.
5. If the radio acts as a Standby Master, perform the following:
6. Configure LDAP replicator, enter the IP address, user name and password to the LDAP server and the alternative LDAP server. Check the Enable check box, see Configure LDAP Replicator on page 97.
7. Enter the system name and password, this must be the same system name and password as in the Master, see Change System Name and Password on page 99.
8. With LDAP replication enabled, the password will be verified against the Master. If the password is wrong a single dot (.) will appear in the text field.
9. Set the mode to Slave, see Select Mode on page 103.
10. Enter Master and Standby Master IP addresses, see 7.5.14 Enter IP Address to the Pari Master on page 63. PARI on page 108
11. Configure air synchronization, see Configure Air Synchronization on page 109.
12. Enter the Time Server address, see Trust List on page 84.
13. Reset in order to make the configuration changes take effect, see Reset on page 141.
14. Save the configuration of the Slave, see Backup on page 132.

Configure the rest of the IPBS/IPBL following the steps below:

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

15. Determine the address.

16. Select Update > Config and browse to the previously saved configuration. Click "OK".
17. Reset in order to make the configuration changes take effect, see Reset on page 141.
18. Repeat step 1 to 3 for all Slaves.

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 Operation on page 71.

1. Determine the IP address and access the GUI, see Access the GUI on page 53.
2. Change the default password, see Change the Default Password on page 56.
3. Set a static IP address and set DHCP to off, see Set a Static IP Address on page 92.
4. Set the mode to Master, see Select Mode on page 103.
5. Perform a reset to restart the IPBS/IPBL in Master mode, see Reset on page 141.
6. Select system name and password, see Change System Name and Password on page 99.
7. Set subscription method, see Set Subscription Method on page 99.
8. Configure authentication code, see Configure Authentication Code on page 100.
9. Set default language, see Set Default Language on page 100.
10. Set frequency band, see Set Frequency Band on page 100.
11. Enable carriers, see Enable Carriers on page 101.
12. Set Master Id, see Configure Gatekeeper on page 104.
13. Assign PARI, see PARI on page 108. Note: If two IPBss are configured for coverage test of air sync, both IPBS must have the same system ID.
14. Enter SARI, see SARI on page 108.
15. Reset in order to make the configuration changes take effect, see Reset on page 141.
16. For coverage test of speech sync, register one handset in the IPBS configured as Sync Master, see Add Users on page 68.
17. Set the mode to Deployment, see Select Mode on page 103.

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 two 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 Anonymous Registration on page 68.
- Individual Registration can be used if a few new handsets shall be added to the IP-DECT System. The IPEI is entered manually, see Individual Registration on page 69.

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	The name of the user, need to be unique throughout the system. This is the name presented in a called party´s display, unless this is configured in the IP-PBX.	30
• Display Name	Optional, will be shown in the handset display when the handset is idle.	30
• Name	Optional, the user name.	30
• Number	Mandatory, the phone number extension, need to be unique throughout the system.	30
• Password	Optional, is used for registration towards the gatekeeper.	30

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.
4. To view the list: Select Users > Anonymous.
   - 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.
   - Repeat step 3 - 4 for all handsets.

     Note: For safety reasons, when the Anonymous Registration is finished change the Subscription Method to "*Disable*"otherwise anyone with knowledge of the System AC could register to the IP-DECT System. See below for more information.
5. Select DECT > System.
6. Disable anonymous registration by selecting "Disable" in the Subscription drop-down list. Click "OK".

Individual Registration

1. Select DECT > System.
2. In the *Subscriptions* drop-down list, select "With System AC" or "With User AC". Click "OK".
3. **Tip:** See also Set Subscription Method on page 99 for more information.
4. Select "Users".
5. Click "New".
6. 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. This is the name presented in a called party´s display, unless this is configured in the IP-PBX.	30

• Display Name	Optional, will be shown in the handset display when the handset is idle.	30
• Name	Optional, the user name.	30
• Number	Mandatory, the phone number extension, need to be unique throughout the system.	30
• Password	Optional, is used for registration towards the gatekeeper.	15
• IPEI / IPDI	Mandatory, the unique identification number of the handset.	
• Auth. Code	Optional, the individual authentication code for this user. Automatically created by default. Can be modified manually.	

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

Log out/Log in Users

This section describes how to log out and log in users to the IP-DECT system. For example, when using a shared handset for shift workers.

Log out Users

Logout the handset for any subscribed user in the system by calling the supplementary services feature for logout (see PARI on page 108), optional individual AC code and hang up.

Example where #11*$# is the feature for logout and 1234 is the AC code: #11*1234#.

Log in Users

To log in a user, see Assign Handsets to Users on page 68

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/IPBL.

The GUI for the IPBS and IPBL are similar. Screen shots from the IPBS are used as default.

General

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

- Name the equipment
- Change Administrator User Name and Password
- Kerberos
- Configure the NTP settings

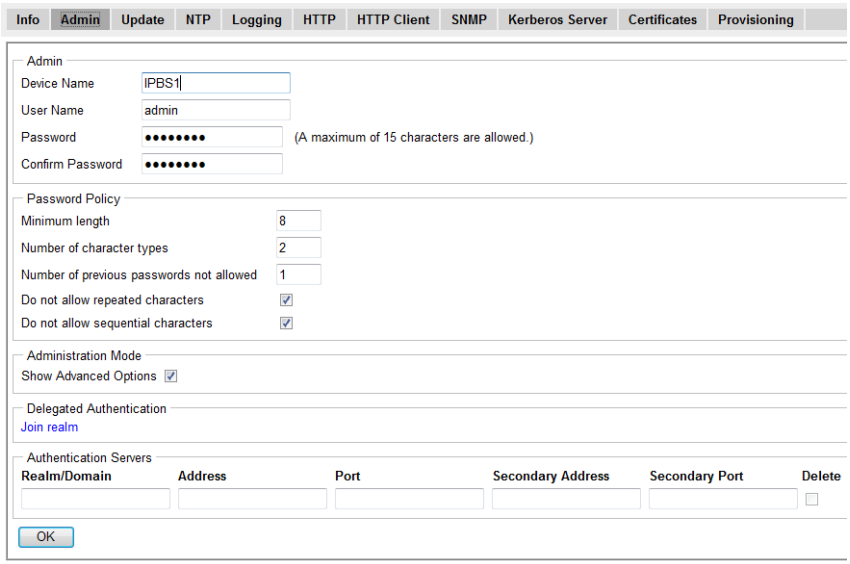


Figure 21. Assigning a administrator name, username, and password.

Name the IPBS/IPBL

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

1. Select General > Admin.
2. Enter a name in the Device Name text field.
3. Click "OK".

Change User Name and Password

The user name and password are used to access the IPBS/IPBL 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".

Centralized Management of Admin/Auditor Accounts Using Kerberos

In software version 3.x.x, each IPBS/IPBL 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/IPBLs and then want to administrate these user accounts at one central location (Kerberos server). When an IPBS/IPBL is setup as a Kerberos server the IPBS/IPBL act as an authentication server for the rest of the IPBSs/IPBLs 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/IPBL to act as a Kerberos server, do the following:

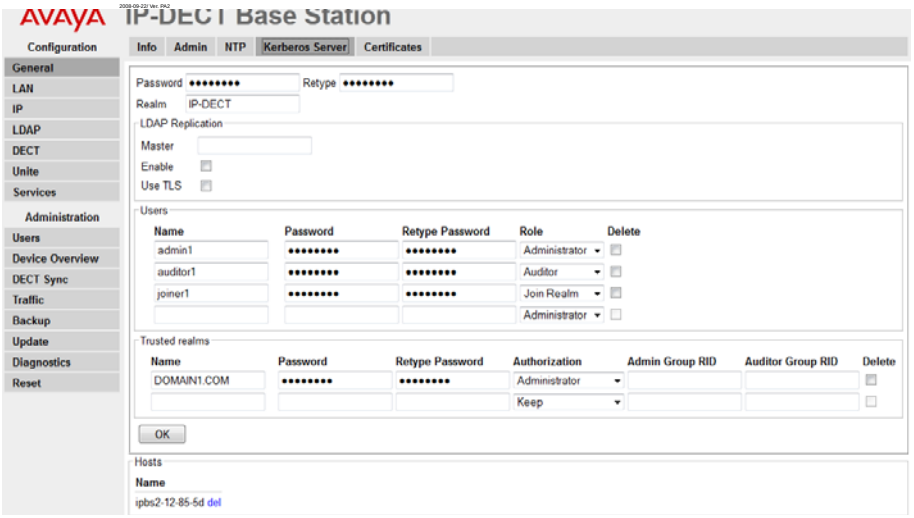


Figure 22. Configure the Kerberos server.

1. Make sure that the IP address of a NTP time server is specified. Select General > NTP.
2. Select General > Kerberos Server.
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

7. Click "OK".

Set up the client

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

- Configure IPBS/IPBL as a client in a small existing system (few clients), see *Configure IPBS/IPBL as a client in a small existing system (few clients)*.
- Configure IPBS/IPBL as a client in a large existing system (many clients), see Configure IPBS/IPBL as a client in a large existing system (many clients) on page 75.
- Configure IPBS/IPBL as a client in a new system, see Configure IPBS/IPBL as a client in a new system on page 76.

Configure IPBS/IPBL 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/IPBL as a client, do the following:

1. Make sure 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:

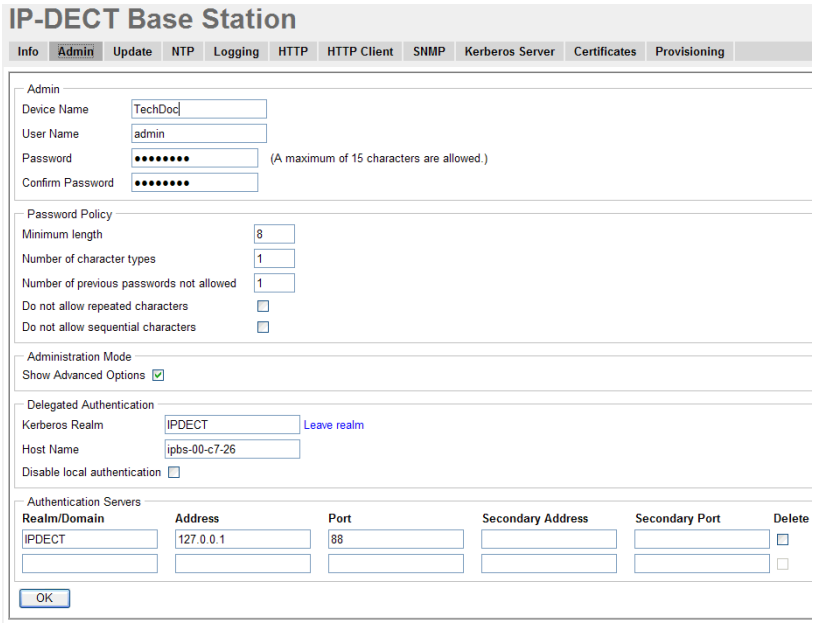


Figure 23. Configure the Kerberos client.

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 the realm account on the Kerberos server.
4. Click "Join".

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

Requirements for IPBS/IPBL: 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 B: 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 B: 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 77.

Configure IPBS/IPBL as a client in a new system

Precondition: The IPBS/IPBL 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).
   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 text field is filled out automatically.
8. Click "OK".

Log in using Kerberos

1. Make sure 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.

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 compromises user account on the Kerberos server than changing the local user accounts on each IPBS/IPBL.

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/IPBL 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/IPBL using their Windows user name and password in the Active Directory (AD). 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:

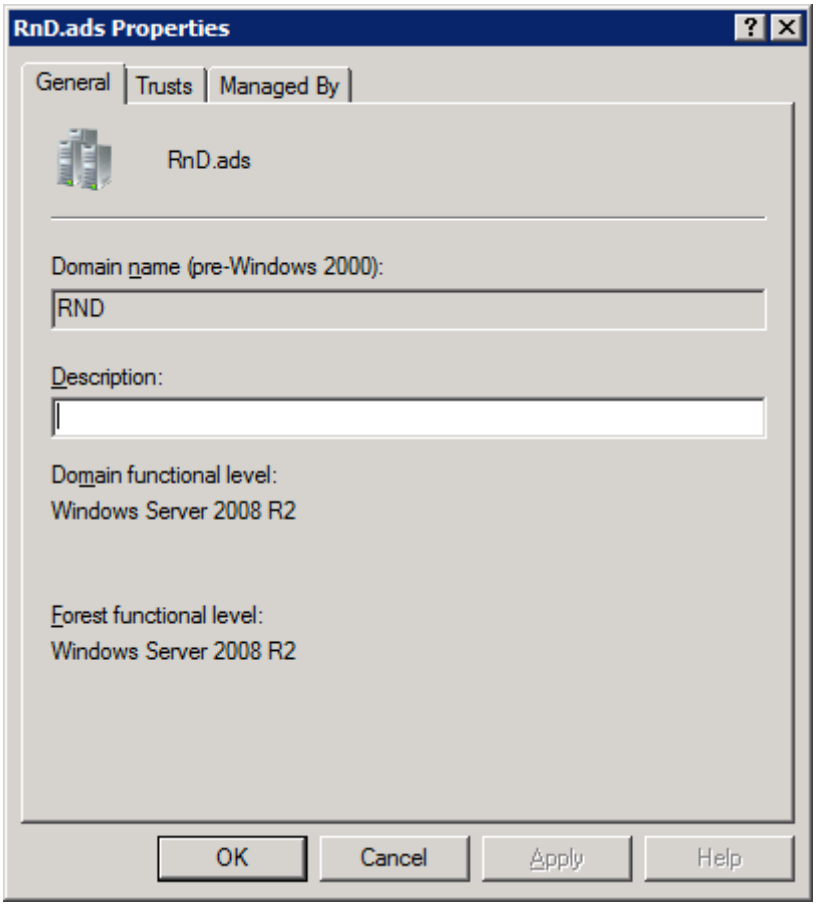
Requirements for IPBS1, IPBS2 and IPBL:

- 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 74.
- 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

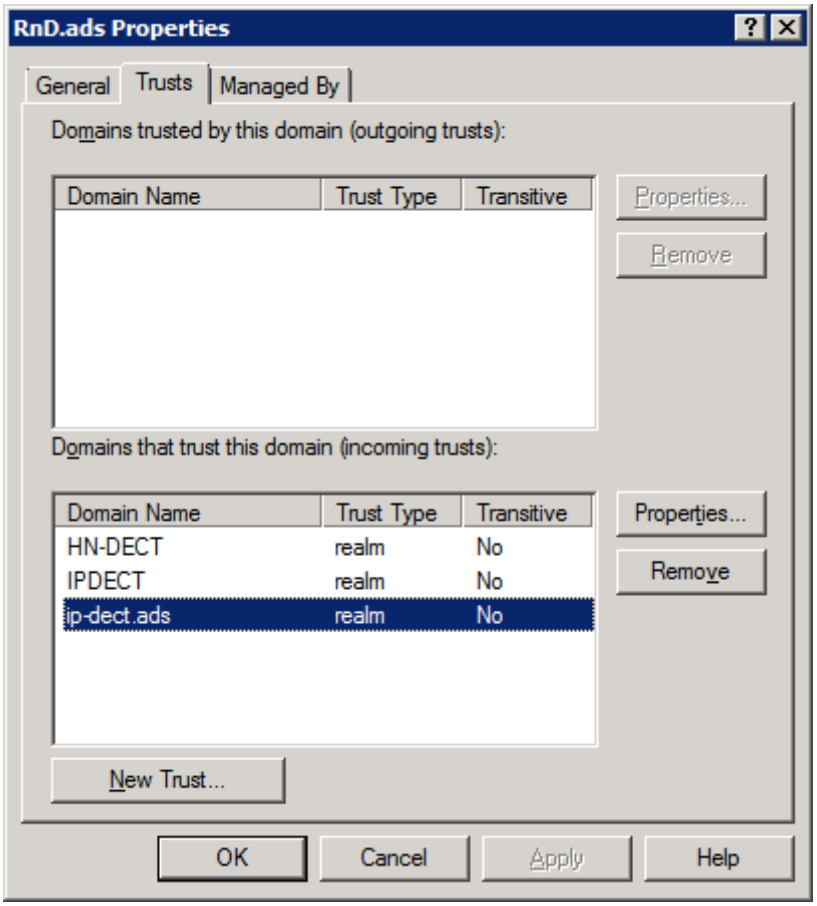
1. The trust relationship must be configured in the AD server.Connect to the Windows 2008 R2 server.
2. In the Windows Start menu select Administrative Tools > Active Directory Domains and Trusts

3. Right-click the realm name you wish to establish a cross realm trust with and select "Properties".
4. Select the General tab and make a note of the windows realm name.

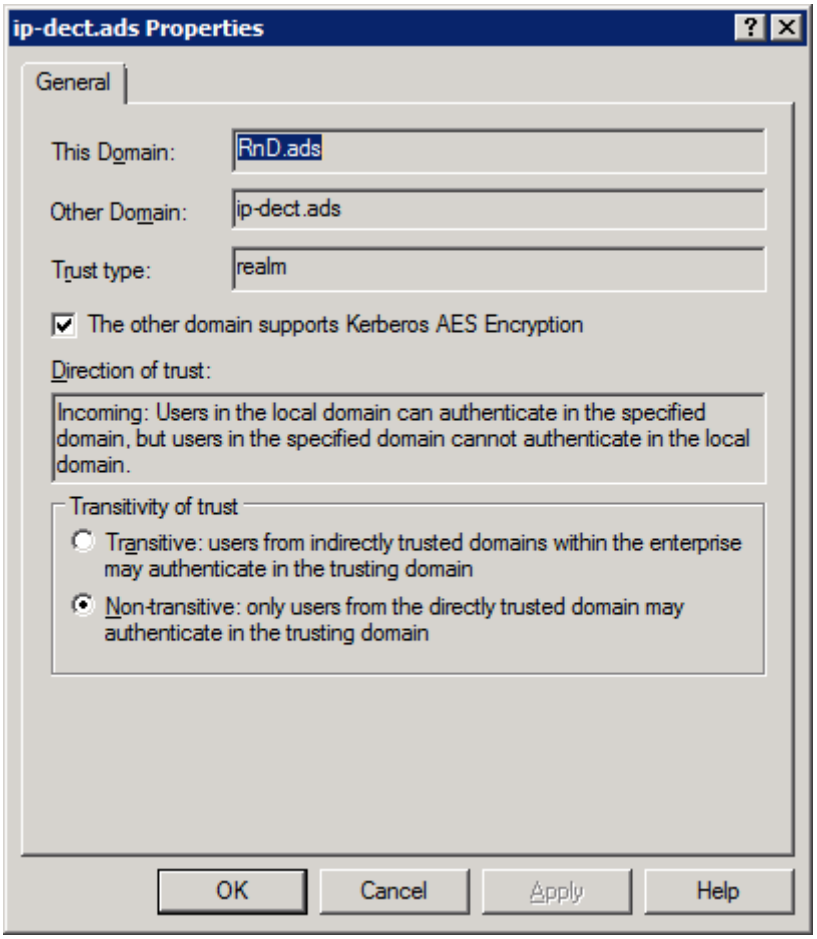


5. Click the Trusts tab and click "New Trust...".
6. The New Trust Wizard appears. Click "Next".
7. Enter the name of the Kerberos realm. Must be capital letters. Click "Next".
8. Select "Realm trust". Click "Next".
9. Select "Nontransitive". Click "Next".
10. Select "One-way incoming". Click "Next".
11. 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".
12. Click "Next".
13. Click "Finish"

14. Click the Trusts tab. Select the realm that you have established a cross realm trust with and click "Properties...".



15. Select the The other domain supports Kerberos AES Encryption check box.



16. Click "OK".

On IPBS1, IPBS2 and IPBL (the Kerberos server):

17. Select General > Kerberos Server.
18. 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.
19. In the *Password* text field, enter the password entered in step 13.
20. 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.

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**.

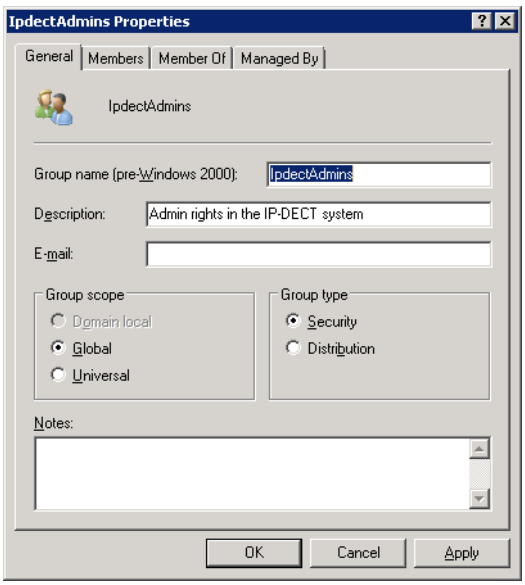
To determine the SID of a group, do as follows:
1. Start Windows Command Prompt (cmd.exe). To find Windows Command Prompt, enter "cmd.exe" in Windows Start Menu search field.
2. In Windows Command Prompt, enter "whoami /groups". This command displays the group information of the user logged in to the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

21. 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.
- **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, IPBS2 and IPBL (the client):

22. Select General > Admin.
23. 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.
24. In the *Address* text field, enter the IP address of the AD server.
25. Click "OK".

Log in using Kerberos cross-realm authentication

1. Make sure 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.

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/IPBL as a secondary Kerberos server, do the following:

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

2. Select General > Kerberos Server.
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".
    1. The secondary Kerberos server is enabled. Enter the realm name in the Realm field.
    2. 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 Configure LDAP Server on page 96.
    3. Select the Enable check box.
    4. Click "OK".
    5. Click "OK" again to perform the LDAP replication.

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

5. Select General > Admin.
6. Go to the Authentication Servers section.
7. In the Secondary Address text field of the Kerberos server, 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 Port text field is filled out automatically.
8. Click "OK".

Delete a user or trusted realm

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

1. Select General > Kerberos Server.
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:

4. Select General > Kerberos Server.
5. In the Trusted Realms section select the Delete check box for the realm to be deleted.
6. 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/IPBL is no longer a member of the realm it is not possible to access the IPBS/IPBL in any other way.

7. Select General > Admin.

8. In the Delegated Authentication section clear the Disable local authentication check box.
9. Click "OK".

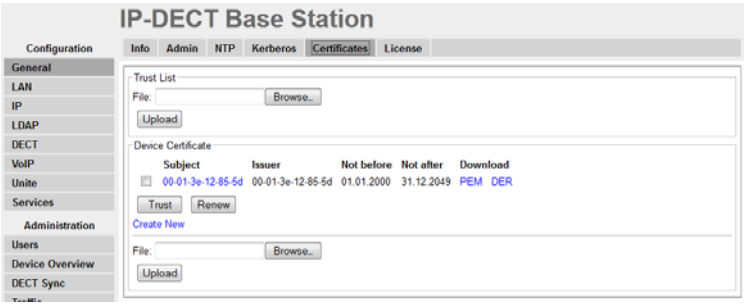
To deactivate the Kerberos membership for a client, do the following:

10. Select General > Admin.
11. Go to the Kerberos section and click on the blue text link "Leave realm".
12. 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".

Certificates

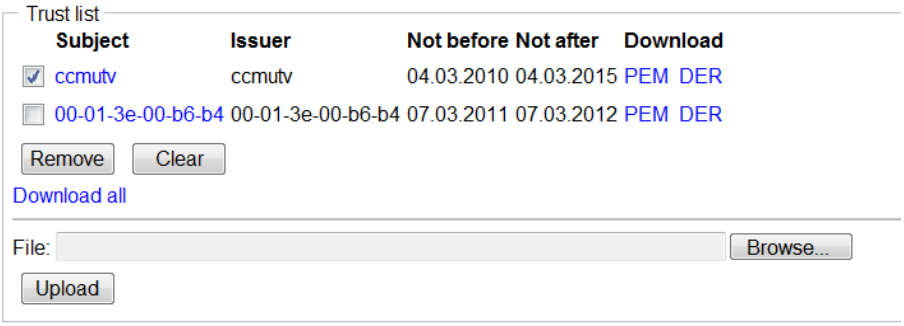
The Certificates tab is part of IP Security in IP-DECT. For more information on IP Security, see chapter IP on page 95.

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).



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 Certificates on page 84, there are three possible certificate options:

1. Default device certificate, see Default Device Certificate on page 86.
2. Self-signed certificates, see Self-signed Certificates on page 87.
3. Certificates signed by a Certificate Authority (CA), see Certificate Signing Request (CSR) on page 88

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 87 • Certificate Signing Request (CSR) on page 88
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 Device Management on page 111.

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.

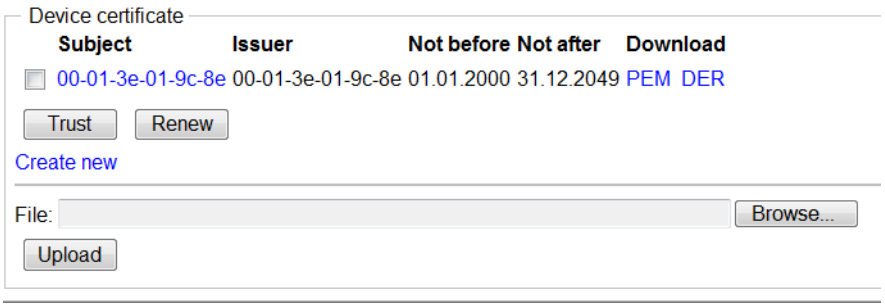
The default certificate is a self-signed certificate. This means that certificates cannot be verified and thus the user/administrator will be prompted by the web browser to accept the certificate before it can be used. From this point on within the browser session (as long as the certificate is not changed) 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 TLS Certificates on page 33.

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 TLS Certificates on page 33. This will be the most common options for IP-DECT systems. For more information on CSRs see Certificate Authorities on page 31.

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.
6. 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.
7. When the CSR file has been generated it is visible in the Signing Request section of the Certificates page.
8. Download the CSR file by clicking the "PEM" or "DER" link in the Signing Request section.
9. Send the CSR file to your CA.
10. If successful your CA will send back a digitally signed certificate file. This file should now be uploaded.
11. Select the certificate file.
12. 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.

Provisioning

Provisioning makes it easy to manage IP-DECT users from the IP-PBX without using the IP-DECT GUI. Provisioning is mainly configured in the IP-PBX but it must be enabled in the IPBS/IPBL. If provisioning is enabled user records in the IPBS/IPBL cannot be modified since all user data is mapped from the IP-PBX to the IPBS/IPBL.

> **Note:** Local users created in the IPBS/IPBL will be deleted when provisioning is enabled if no corresponding user exists in the IP-PBX.

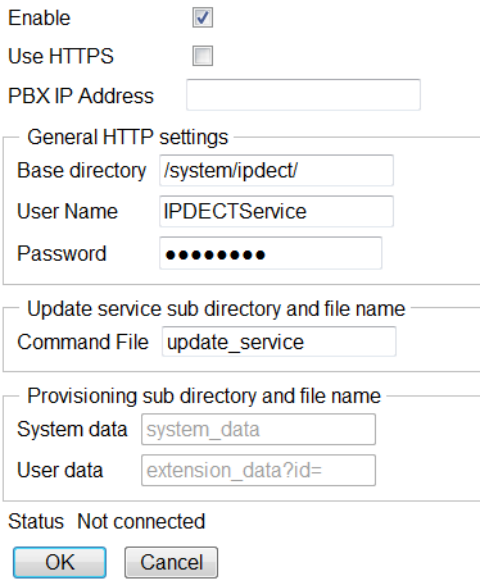


Figure 24. Configure Provisioning

To enable provisioning do the following:

1. Select General > Provisioning.
2. Select the Enable check box.
3. The communication between the IPBS and the IP-PBX can be encrypted using https. Select the Use HTTPS check box to enable the encryption.
4. Specify the IP address of the IP-PBX in the PBX IP Address field.
5. The other values on the page are default values and filled out automatically.
6. Click "OK".
7. Reset the IPBS/IPBL to make the changes take effect, see Reset on page 141.

If the https protocol is used the IPBS/IPBL downloads a certificate from the IP-PBX to ensure a secure transaction. The IPBS/IPBL does not initially trust the certificate so it must be added manually to the trust list of the IPBS/IPBL. 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:

8. Select General > Certificates.
9. In the Rejected certificates section select the check box of the certificate you want to trust.
10. Click "Trust".

For more information about certificate handling, see Public Key Certificates (Digital Certificates) on page 31.

Provisioning Modes

There are three different modes.

Active	The connection is up.
Inactive	Provisioning is not enabled for the currently viewed IPO PBX or the connection is used for the other IPO PBX.
Not connected	Provisioning is enabled for the currently viewed IPO PBX but the connection cannot be established or the connection is being established.

LAN

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

- Set DHCP mode
- Set IP static address
- Set dynamic IP address
- Set link type
- Configure VLAN
- View LAN statistics
- Deactivate LAN port (only for IPBL)

> **Note:** The IPBL has two LAN ports. LAN1 port must be used in the IP-DECT system (LAN2 port is for administration only). This is not applicable when RSTP is used, see Enable RSTP (only for IPBL) on page 94.

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 E: Configure DHCP Options on page 168.

Set DHCP Mode

The IPBS/IPBL can have different DHCP modes, see the table below.

Disabled	Used if the IPBS/IPBL should have a static IP address.
Client	The IPBS/IPBL 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/IPBL will act as a DHCP client on power up. If the IPBS/IPBL 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. On the IPBS: Select LAN > DHCP.
   On the IPBL: Select LAN1 > DHCP.
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 Reset on page 141.

Set a Static IP Address

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

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

1. On the IPBS: Select LAN > DHCP.
   On the IPBL: Select LAN1 > DHCP.
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 IPBS: Select LAN > IP.
   On the IPBL: Select LAN1 > IP.
6. Enter "IP Address", "Network Mask", "Default Gateway" and "DNS Server" addresses provided by the network administrator in the text fields.
7. 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.
8. Click “OK”.
9. Reset in order to make the changes take effect, see Reset on page 141.
10. Start the web-based configuration, using the static IP address.

Dynamic IP address using DHCP

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

1. On the IPBS: Select LAN > DHCP.
   On the IPBL: Select LAN1 > DHCP.
2. Select “Client” in the *Mode* drop-down list.
3. Click “OK”.
4. Reset in order to make the changes take effect, see Reset on page 141.

> **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.

Link

1. On the IPBS: Select LAN > Link.
2. On the IPBL: Select LAN1 > Link.

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

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/IPBL, otherwise it will not be possible to access the IPBS/IPBL.

> **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.

View LAN Statistics

To view statistics of LAN events:

1. On the IPBS: Select LAN > Statistics.
2. On the IPBL: Select LAN1 > Statistics.

To reset the ethernet statistics counters, click "Clear".

Enable RSTP (only for IPBL)

The RSTP (Rapid Spanning Tree Protocol) function is provided for IPBLs connected to a redundant bridged network when an IPBL must stay operational even if a network port or a bridge in the network fails. If RSTP is enabled LAN1 is assumed to be the primary port and LAN2 the backup port. RSTP packets are sent over both ports. From received RSTP packets it is learned which port shall be used for data traffic. The port to be used for data traffic may change whenever the network topology changes, i.e. when a link between bridges goes down or up or a bridge is added. On each such change the IP stack is moved to the selected port without disruption of data traffic.

Before RSTP can be enabled the following preconditions must be met:

- The bridges in the network should support RSTP.
- LAN1 and LAN2 should be connected to RSTP enabled bridge ports.
- LAN1 and LAN2 should be connected to different bridges.
- LAN1 must be configured for a static IP address. See Set a Static IP Address on page 92.
- Select LAN1 > IP. Make sure that the *Check ARP* and the *Disable* check boxes are unchecked.
- Select LAN2 > IP. Select the *Disable* check box.
- Select LAN2 > DHCP. Select *disabled* in the *Mode* drop-down list.
- Select LAN1 > VLAN. Check that VLAN is not enabled.
- Select LAN2 > VLAN. Check that VLAN is not enabled.

To enable RSTP:

1. Select LAN1 > RSTP.
2. Select the *Enable* check box.
3. To trace events triggering RSTP state machine actions and the associated events: Select the *Trace Actions* check box.
4. Click “OK”.

Deactivate LAN Port (only for IPBL)

To deactivate LAN port:

1. Select LAN2 > IP.
2. Select the Disable check box.
3. Click “OK”.

The LAN2 port is for administration only and it is the port you in normal case are interested in deactivating.

IP

Configure IP Settings

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

ToS priority, RTP Data and VoIP Signalling:	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 Signalling[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 32767 will be used.

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

1. Select IP > 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 Signalling* 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".

Routing

View the IP routing by Select IP > Routing.

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/IPBLs in the system have access to the database, one of the IPBSs/IPBLs 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

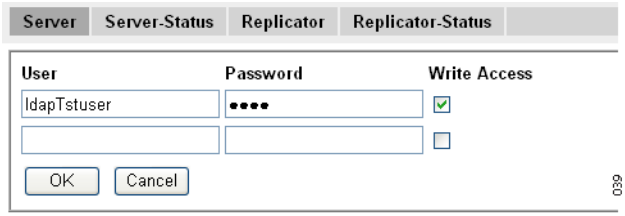
Configure LDAP Server

The IP-DECT system needs an LDAP server. If the PBX is set up as an LDAP server, the Master should be set up as an LDAP Replicator. If the Master is set up as an LDAP Server, the Standby Master could be set up as an LDAP Replicator, see Configure LDAP Replicator on page 97.

Setup the IPBS/IPBL 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".



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

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 PBX to the Master. The replicator is configured on the Master (Full Directory Replication)

Configure Full Directory Replication

1. Select LDAP > Replicator.
2. Select the Enable check box.
3. Enter the IP address to the LDAP server in the Server text field.
4. Enter the IP address to the alternative LDAP server in the Alt. Server text field.
5. NOTE: If this IPBS/IPBL is configured as an alternative/standby LDAP server, enter "0.0.0.0" in the Alt. Server text field.
6. 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.

Check LDAP Replicator Status

1. Select LDAP > Replicator-Status.

The following information is displayed:

- Server - The IP address and port of the LDAP server.
- 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

Expert tool

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

DECT

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

- Change System Name and password
- Change Subscription Method
- Configure Authentication Code
- Set Default Language
- Set Frequency Band
- Enable/Disable Carriers

- Enable/Disable Early Encryption
- Configure Coder
- Configure Supplementary Services
- Select Master Mode
- Configure Trunks
- Enable/Disable Radio
- Multiple Radio Configuration
- Assign PARI
- Enter SARI
- Configure Air Synchronization

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/IPBLs throughout the system. Reset in order to make the changes take effect, see Reset on page 141.

1. Select DECT > System.
2. Note: To access the System tab, the Master mode has to be activated, see Select Mode on page 103.
3. Write a system name in the System Name text field.
4. Enter a new password in the Password text field. Repeat the password.
5. Click "OK".

Note: It is recommended to create a backup of the IPBS configuration when the password has been changed, see Backup on page 132.

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.

2. Note: To access the System tab, the Master mode has to be activated, see Select Mode on page 103.
3. Select subscription method in the Subscriptions drop-down list.
4. Click "OK".

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

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.
2. Note: To access the System tab, the Master mode has to be activated, see Select Mode on page 103.
3. Enter an authentication code in the Authentication Code text field.
4. Click "OK".

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.
2. Note: To access the System tab, the Master mode has to be activated, see Select Mode on page 103.
3. Choose language in the Default Language drop-down list.
4. Click "OK".

Set Frequency Band

The IPBS/IPBL can operate in the following frequency bands:

- 1880 - 1900 MHz, Europe, Africa, Middle East, Australia, New Zealand and Asia
- 1910 - 1930 MHz, South America
- 1920 - 1930 MHz, North America

1. Select DECT > System.
2. NOTE: To access the System tab, the Master mode has to be activated, see Select Mode on page 103.

3. Select frequency area in the Frequency drop-down list.
4. Click "OK".

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

Enable Carriers

The IPBS/IPBL has 5 carriers for the North American 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.
2. NOTE: To access the System tab, the Master mode has to be activated, see Select Mode on page 103.
3. Select/clear the Enabled Carriers check boxes.
4. Note: For Brazil, the following carriers shall be selected only: 0, 1, 2 and 3.
5. Click "OK".

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 Select Mode on page 103.

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

   Note: The *Early Encryption* check box will not be visible if the IPBS GUI is set to simplified mode. (About simplified mode, see Simplified GUI on page 62.) The *Early Encryption* check box will be disabled (greyed out) when Provisioning is enabled in the IPBS/IPBL. (About Provisioning, see Provisioning on page 89.)

3. Click "OK".

Note: *When using IPBL and the early encryption feature is enabled*: The RFPs will startup only if they support this feature.

4. 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).

Configure Coder

Select the preferred coder, and enter the desired frame length. If exclusive is selected for the coder the IPBS/IPBL 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.
2. Note: To access the System tab, the Master mode has to be activated, see Select Mode on page 103.
3. Choose the applicable coder in the Coder drop-down list.
4. Enter the sample time in milliseconds in the Frame text field.
5. Choose Exclusive enabled or disabled by selecting/clearing the Exclusive check box.
6. Choose Silence Compression enabled or disabled by selecting/clearing the SC check box.
7. Click "OK".

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.

1. Select DECT > System.

Note: To access the System tab, the Master mode has to be activated, see Select Mode on page 103.

2. To enable SRTP: Select in the Secure RTP drop-down list a cryptographic suite. The numbers in the list refer to key-length/sha1 hash-length.
3. To disable SRTP: Select in the Secure RTP drop-down list the empty row at top.
4. Click "OK".
5. Select DECT > Trunks.
6. In the *Password* text field, enter the same SRTP password as in the IP-PBX.
7. Click "OK".

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 Select Mode on page 103.

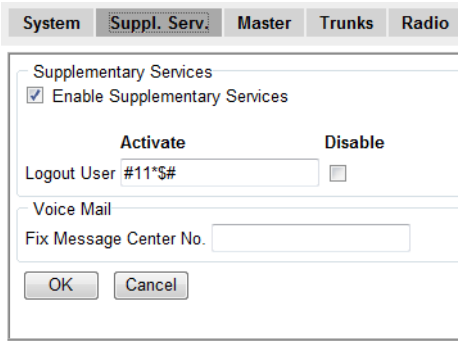
2. Select the Enable Supplementary Services check box to activate the supplementary services below. The default Activate feature code is preset.

   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*$#

   Note: To disable a specific service, select the Disable check box to the right.

3. Click "OK".
4. Reset in order to make the changes take effect, see Reset on page 141.



Select 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.

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

- "Off", if this IPBS/IPBL is not a Master.

- "Active", if this IPBS/IPBL is the Master.
- "Standby", if this IPBS/IPBL 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/IPBL is the Mirror. For information about Mirror devices, see the system description for IP-DECT.

2. If you have selected the "Standby" mode enter the primary Master IP address in its text field.
3. If you have selected the "Mirror" mode 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.
4. Click "OK".
5. Reset in order to make the changes take effect, see Reset on page 141.

Configure Gatekeeper

Only applicable on the Master.

1. Select DECT > Master
2. Set Master ID
3. NOTE: The ID for the Master and the Standby Master must be identically.
4. Select PBX.

   Note: If a redundant trunk shall be configured for connection to IPO PBX, select the *PBX Resiliency* check box.
   The *PBX Resiliency* check box will be disabled (greyed out) when Provisioning is enabled in the IPBS/IPBL. About Provisioning, see Provisioning on page 89.
5. Select Protocol.
6. Enter ARS Prefix. For example, 00 for external calls.
7. Enter International CPN Prefix. For example, 0046 for Sweden.
8. Enter National CPN Prefix. For example, 031 for Gothenburg.

9. Click "OK".

Configure Trunks

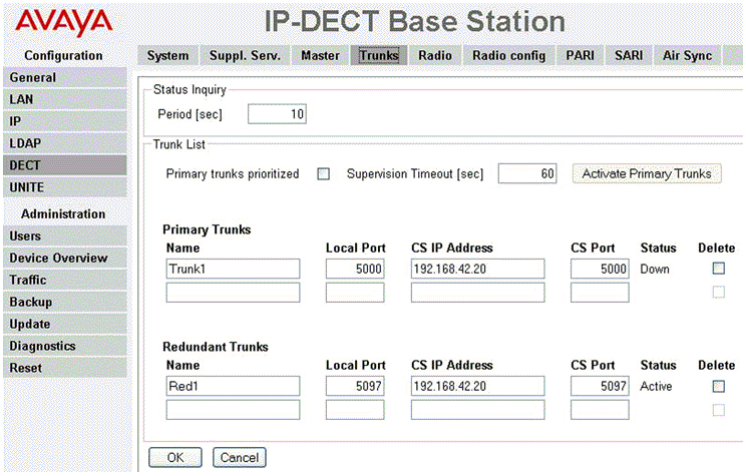
Note: Trunks cannot be configured (configuration sets will be greyed out) in the IPBS/IPBL when Provisioning is used with IPO PBX. However, it will still be possible to activate a primary trunk manually (see Activation of Primary Trunks on page 106). About Provisioning, see Provisioning on page 89.

A shared trunk is used for connection between the IP-DECT system and an PBX which can be an ACM PBX or an IPO PBX.

There are two kinds of trunks; primary and redundant. One or more primary trunks can be configured. They are used in the first place. One or more redundant trunks can also be configured. They are only used if none of the primary trunks are in "Active" mode. That is, all primary trunks must be in "Down" mode.
Note: Only one primary and one redundant trunk can be configured for the IPO PBX.

1. To configure primary and redundant trunks, do as follows:
2. Select DECT > Trunks.
3. To determine the status of the trunks towards the IP-PBX, enter in the *Period (sec) field* how often the IPBS/IPBL shall send status inquiry messages to the IP-PBX.
4. Enter the IP Address of the IP-PBX in the CS IP Address field and the port of the IP-PBX in the CS Port field.
5. Enter port address of the IPBS in the Local Port field.

Note: If a redundant trunk shall be configured for connection to the IPO PBX, make sure that the *PBX Resiliency* check box has been selected (DECT > Master).
The *PBX Resiliency* check box will be disabled (greyed out) when Provisioning is enabled in the IPBS/IPBL. About Provisioning, see Provisioning on page 89.



Load Balancing

Note: This section does not apply for the IPO PBX.

There are possibilities to configure several primary trunks to get a good load balancing in the system. This means that call setups alternate between the active primary trunks. The first active primary trunk has the highest priority.

If no load balancing is desired in the network, only one primary trunk should be configured and all calls are set up on this trunk if it is in "Active" mode.

Trunk Modes

There are four different modes for a primary and redundant trunk.

Note: A primary trunk can never be set to Standby.

Active	The trunk is up and accepts traffic.
Up	The trunk is up but does not accept traffic as it is not set to "Active" mode.
Down	The trunk is down and not working.
Standby	The trunk is ready to be used for redundant purpose.

A trunk that is "Active" or "Up" is correctly configured and correctly attached. A trunk that is "Down" has a fault. Either in the configuration or the hardware (broken cable).
Fault finding can be to check that the IP-address is correct as well as to check the PCB and the cable.

Redundant Trunks

Commonly one redundant trunk is configured as a backup. It is used if all of the primary trunks are down.

If all primary trunks are "Down", the redundant trunks starts working. The redundant trunk will get the status "Active" or "Down" depending if it works or not. If it gets the status "Active" the calls will go through the redundant trunk until the primary trunks are activated again.

Activation of Primary Trunks

There are two ways of activating the primary trunk; Manual and Automatic:

- Manual

  Click on the "Activate Primary Trunks" button. (This button is only available if there is any primary trunk in "Up" mode.)

  The primary trunks then enters "Active" mode and the redundant trunks cease to be active and go to "Standby" mode". (New calls go through the primary trunks and ongoing calls go through the redundant trunks until the call is finished).

- **Automatic**
  Note: Automatic activation cannot be configured if Provisioning is used. About Provisioning, see Provisioning on page 89.

  1 Select the "Primary trunks prioritized" check box.

  2 Set the "Supervision Timeout" to desired time. The primary trunks are automatically changing from "Up" mode to "Active" mode when the timer is elapsed.

  Example:
  If the timeout is set to 600 seconds, it means that the system waits 600 seconds (10 minutes) until it is automatically up and running again (on active primary trunks). This is the amount of time to fix any problems.

  During the Supervision Timeout, there is a continuous condition check of the trunk connection. The timer states the time it must take until a successful connection is established in the system.

Enable the Radio

If the IPBS/IPBL shall not be used as a radio, for example only be used as a Master, it can be disabled by marking the Disable check box.

Tip: To assign a Master, see PARI on page 108.

- Select DECT > Radio.
- Clear the Disable check box.

Enter IP Address to the Master and the Standby Master

All IPBS/IPBL need to know the IP address of the Master and the Standby Master.

1. Select DECT > Radio.
2. Enter the name for the Master in the Name text field.
3. Enter the password for the Master in the Password text field.
4. Enter the address to the Master in the Master IP Address text field. If this is the Master, enter 127.0.0.1.
   Note: The Master can be configured as Active or Mirror.
5. Enter the address to the Standby Master in the Alt. Master IP Address text field. If this is the Standby Master, enter 127.0.0.1.
   Note: The Standby Master can be configured as Standby or Mirror.
6. Click "OK".
7. Reset in order to make the changes take effect, see Reset on page 141.

Multiple Radio Configuration

The 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.
2. Configure alarm and event forwarding, see Forward Alarms and Events on page 115.
3. Configure automatic firmware update, see Certificates on page 84.
4. Configure NTP settings, see Trust List on page 84.
5. Configure IP settings, see Configure IP Settings on page 95.
6. Click "OK".
7. Click "OK".

PARI

The PARI is a part of the broadcast identity, which uniquely identifies an IPBS/IPBL. This PARI is automatically assigned to each IPBS/IPBL in the system. But if more than one Avaya 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 Avaya IP-DECT systems within the coverage area, perform an RFP scan, see RFP Scan on page 140.

1. Select DECT > PARI.
2. Select a number between 1 and 292. If this is not done, the IPBS/IPBL will randomly select a number.

   Note: The number of system IDs will affect how many IPBSs/IPBLs that can be used per Master in an installation, as shown below:

   System ID = 1 to 36:
   Max. 1023 IPBS per Master or max. 240 IPBL per Master.

   System ID = 37 to 292:
   Max. 127 IPBS per Master or max. 127 IPBL per Master.
3. Click "OK".
4. Reset in order to make the changes take effect, see Reset on page 141.

SARI

The SARI is the broadcast identity, which uniquely identifies an IP-DECT system. The SARI is added in the Master.

1. Select DECT > SARI.
2. Enter the license number delivered by your supplier in the SARI text field.
3. Click "OK".
4. Reset in order to make the changes take effect, see Reset on page 141.

Configure Air Synchronization

This section only applies to the IPBS.

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. The 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 the Master. The Master informs the IPBS sync slaves which sync candidate it shall synchronize to.

Mixed System

All IPBLs are synchronization masters in region 0. Any IPBS in this region will receive its synchronization over the air from the RFPs, which are connected to the IPBL.

Sync Regions

Sync regions are used when, for example, several buildings are located in the same coverage area and all radios are using same 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 Master. The 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 63 in the Sync Region text field.
5. Click "OK".

Configure Sync Master IPBS

Radios configured as sync master will report to the Master that it wants to be a sync master. The 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 63 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. Select Action at reference sync failure as one of the following:
   - Resynchronize on command (manually)

- Resynchronize every day (automatically)
- Resynchronize once per week (automatically)

7. If automatic resynchronization is selected, the master will restart the synchronization at the scheduled time if the synchronization to the reference system is lost. If manual resynchronization is selected, the administrator can manually restart the synchronization to the reference system if required.
8. Click "OK".

UNITE

Configure Messaging

If an AIWS2 is to be used in the IP-DECT system, enter the IP address following the steps below.

1. Select UNITE > SMS.
2. NOTE: To access the SMS tab, the Master mode has to be activated, see Select Mode on page 103.
3. Click "OK".
4. Reset in order to make the changes take effect, see Reset on page 141.

Configure Network Regions

It is possible to setup several Network Regions by configuring one Master Base Station for each Network Region.

Each Master Base Station is identified towards the AIWS2 by a unique number. The AIWS2 is supporting 100 Network Regions. It is recommended to set a number between 1 and 100.

1. Select UNITE > SMS.
2. NOTE: To access the SMS tab, the Master mode has to be activated, see Select Mode on page 103.
3. Enter a number identifying the Network Region in the Region ID field.
4. Click "OK".

Device Management

Note: To access the Device Management tab, the Master mode has to be activated, see Select Mode on page 103.

If a specific Device Manager (for example AIWS2) 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 Service Discovery on page 112.

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.
3. The IP address for the Device Manager that the Master is currently connected to is shown under Active Settings.
4. 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.
3. The IP address for the Device Manager that the Master is currently connected to is shown in the Unite Address text field.
4. Enter the Resource Identity/Service in the Resource Identity text field. The default is IPDECT.
5. Click "OK".

Service Discovery

If no Device Manager (for example AIWS2) has been selected to be used in the IP-DECT system, see Device Management on page 111, 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.
2. NOTE: To access the Service Discovery tab, the Master mode has to be activated, see Select Mode on page 103.
3. 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.
4. 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.

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).

Services

Configure Automatic Firmware Update

The IPBS/IPBL 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 153.

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.

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/IPBL 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/IPBL 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 Master (DECT > Radio config) or locally as described below.

7. Select Services > Logging.
8. If the HTTP server destination requires HTTPS then select "HTTPS" in the Type drop-down list.
9. Enter the IP Address of the IPBS/IPBL where you want to have an overview of all faults in the External HTTP Server Address text field.
10. Enter the HTTP server port in the External HTTP Server Port text field. The default value is 80.

Configure the HTTP settings

Traditionally IPBS/IPBL has been administered over the network via the http protocol (default port 80).

In a secure system (see the IP Security chapter) IPBS/IPBL 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/IPBL 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.

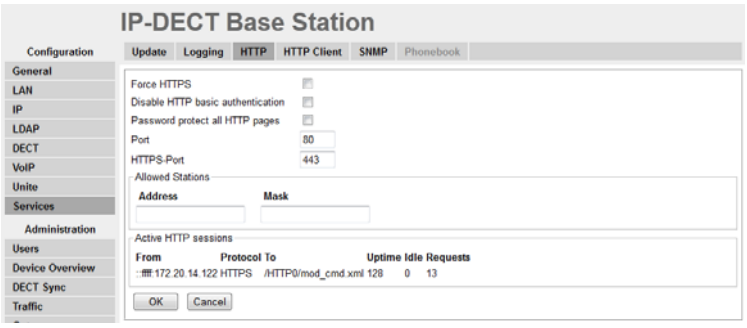


Figure 25. Configure the HTTP Settings

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.
- Enter "Port number" in the Port text field. The IPBS/IPBL 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/IPBL 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".

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.

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/IPBL, the relationship between the manager and the agent must be defined.

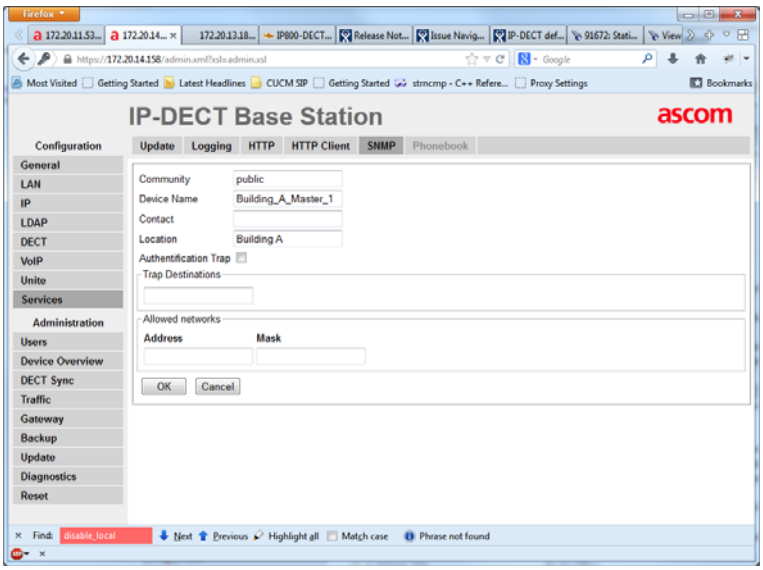


Figure 26. Configure SNMP Settings

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".

Phonebook

Note: This section applies only when using IPO PBX.

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.

Note: If the phonebook functionality in the IPBS/IPBL is enabled, then the SMS feature in the AIWS2 is disabled. If an AIWS2 is connected, the central phonebook should be located in the AIWS2 instead of the IPBS/IPBL.

Import Entries to the Central Phonebook

Note: When importing new entries to the central phonebook, existing entries will be overwritten.

In the Master, do as follows:

1. Select Services > Phonebook.
2. Select the Enable check box.
3. Enter the phonebook number in the *Phonebook Number* field, i.e. the phonebook number the DECT handsets are using to access the phonebook. Check that the phonebook number does not conflict with any of the DECT handsets in the system. The default phonebook number is 999999.
4. Enter the IP address to the TFTP server (IPO PBX) in the *Server IP Address* field.
5. In the *External Directory File* field, enter the path to the IPO PBX's external phonebook.
6. In the *Internal Directory File* field, enter the path to the IPO PBX's internal phonebook.
7. In the *Synch. Interval [min]* field, enter the database synchronization interval in minutes. A value between 10 and 30000 can be entered.
8. Click "OK".
9. If a Standby Master is used, repeat the above steps for the Standby Master also.

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 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.

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 name or number to search for in the text field. It is possible to enter only the beginning of the name or number.
3. Click "show".

Add a User

For information on how to add Users to the IP-DECT system, see Add Users on page 68.

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 Ascom 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.

Add a User Administrator

For information on how to add user administrator to the IP-DECT system, see Managing User Administrators on page 61.

Import Users from a csv file

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. This is the name presented in a called party´s display, unless this is configured in the IP-PBX.	30
Display Name	Optional, will be shown in the handset display when the handset is idle.	30
Name	Optional, the user name.	30
Number	Mandatory, the phone number extension, need to be unique throughout the system.	30
Password	Optional, is used for registration towards the gatekeeper.	15
IPEI / IPDI	The unique identification number of the handset.	
Auth. Code	Optional, the individual authentication code for this user. Automatically created by default. Can be modified manually.	

The csv file may have the following format:

Long Name;Display Name;Name;Number;Password;IPEI/IPDI;Auth Code;

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 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 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 Show all Registered Users in the IP-DECT System on page 119.

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.

Show Anonymous

The IPEI / IPDI number is displayed on anonymous registered handsets.

1. Select "Users".
2. Select "Anonymous".

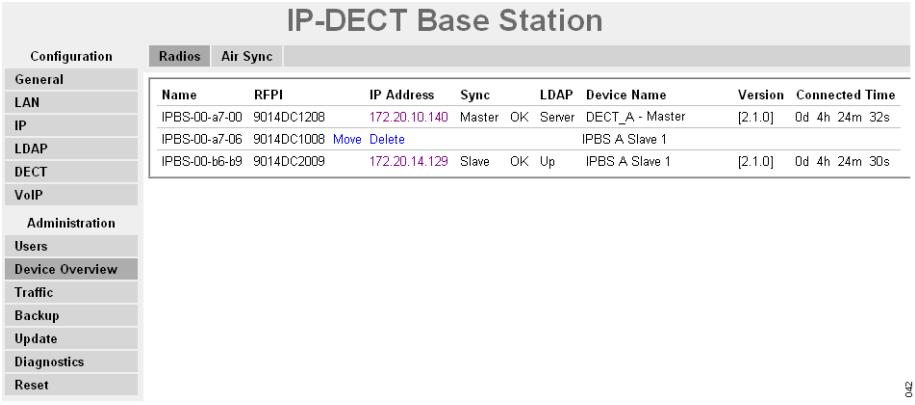
Device Overview

Radios

Information about the devices in the IP-DECT system.

1. Select Device Overview > Radios.

I



Name	The unique identification name. The name syntax is ipbs-xx-xx-xx (IPBS1), ipbs2-xx-xx-xx (IPBS2) or ipbl-xx-xx-xx (IPBL), 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/IPBL.
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 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 Master only.

Delete Radios

In the Static Registrations section, initialized Radios no longer registered to the 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 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 Master.

1. Connect the replacing device.
2. Add the Radio to the Master, see Add Radios on page 122.
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.

RFPs

This section only applies to the IPBL.

Information about the DECT devices connected to the IPBL. For explanation on the information, see the table below.

1. Select Device Overview > RFPs.
2. Click the applicable port to open the RFP details pop-up window.
3. The following actions are available:
   - Click "OK" to save your settings and close the pop-up window.
   - Click "Cancel" to close the pop-up window.

- Click "Refresh" to update the information.
- Click "Reset" to reset the RFP.

RFP Logging

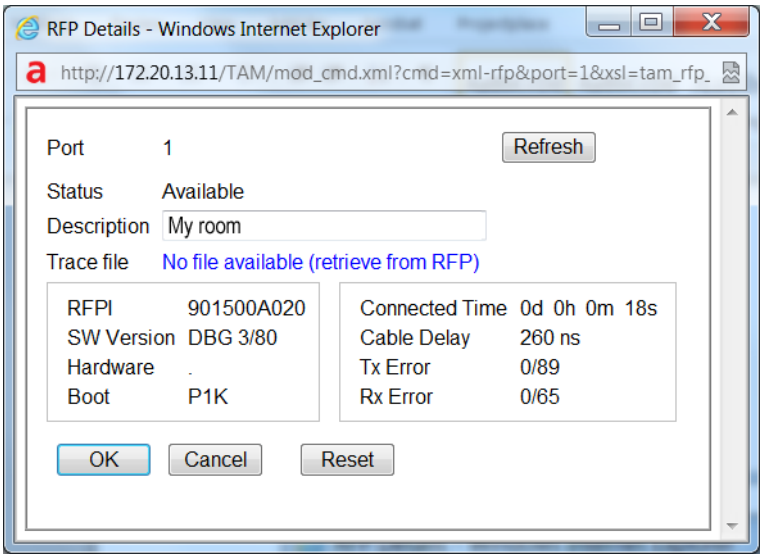
An IPBL can retrieve logs from connected DB1s. A DB1 continuously produce logs by default, but during normal operation there will be few logs. Detailed logs will be produced if the DB1 experience a major event, such as an unexpected restart.

Retrieving an RFP Log

To retrieve a log, do as follows:

1. Select Device Overview > RFPs.
2. Click the applicable port (blue text link) to open the RFP details pop-up window.
3. Click on the blue retrieval text link "No file available (retrieve from RFP)" (see figure on page 125). The log is being prepared for download which may take up to 3 to 4 minutes (figure 27). The retrieval link will thereafter turn into the blue text link "Download" (figure 28).
4. Click on the blue text link "Download" and open or save the log.

Note: The log can only be downloaded once. It is removed from the RFP after download. Logs are stored in the volatile memory and will be lost if the RFP loses power for whatever reason.



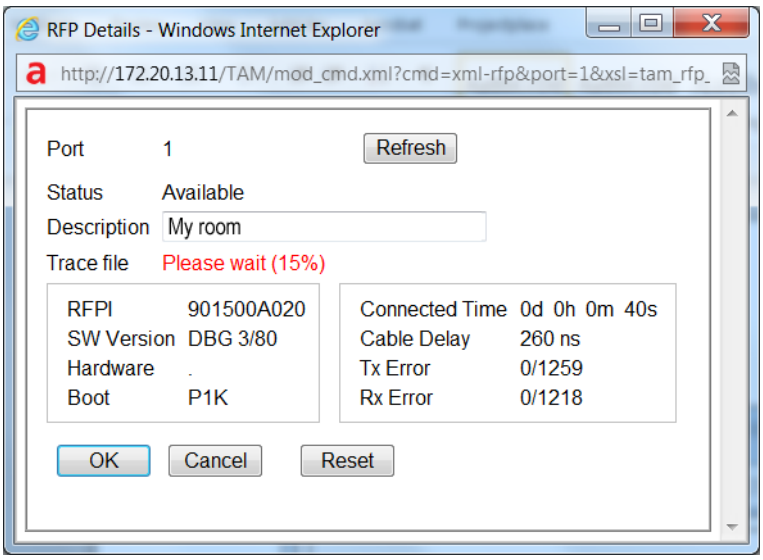


Figure 27.

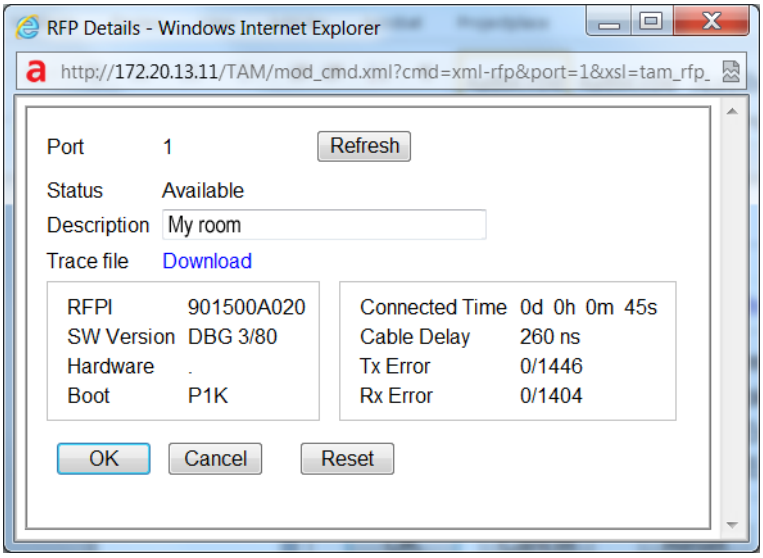


Figure 28.

Halted Logs

At certain major events, such as an unexpected restart, the logging will be halted so that the major event can be investigated. When the logging has been halted, the blue RFP link on the RFP overview (Device Overview > RFPs) will turn red (see figure 29). The logging will be restarted after the log has been downloaded.

Note: An unexpected RFP restart will be indicated by the fault code 0x000e000a under Diagnostics > Events.

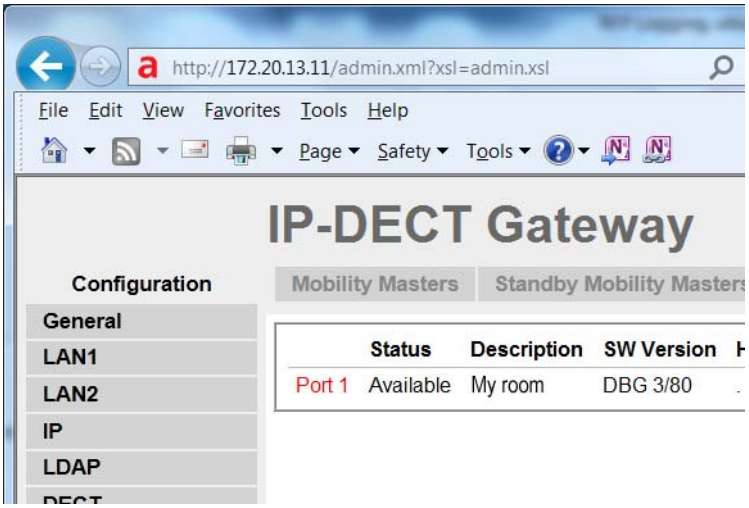


Figure 29.

Sync Ring

This section only applies to the IPBL.

A wire map of the synchronization ring is available in the GUI. The identities (IPBL-xx-xx-xx) of the IPBLs and the position in the ring is displayed. If the ring is broken it is possible to locate where. Click the IP address to access another IPBL.

1. Select DECT Sync > Sync Ring.

Sync Ports

This section only applies to the IPBL.

Displays the current status of the synchronization ports.

1. Select DECT Sync > Sync Ports.

Status	The current status of the port.
Sync Offset	The synchronization offset for the IPBL.
Cable Delay	The delay caused by the cable.
Sync Lost Counter	The number of times synchronization lost.
Communication	The present status of communication.
Connected to	The IP address of the IPBL connected.
Tx Error	The number of transmitting errors.
Rx Error	The number of receiving errors

Air Sync

This section only applies to the IPBS.

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%. Should be below 80% to be able to keep the synchronization.

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 127, 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.

DECT Sync

Air Sync Overview

This section only applies to the 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 30. 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.

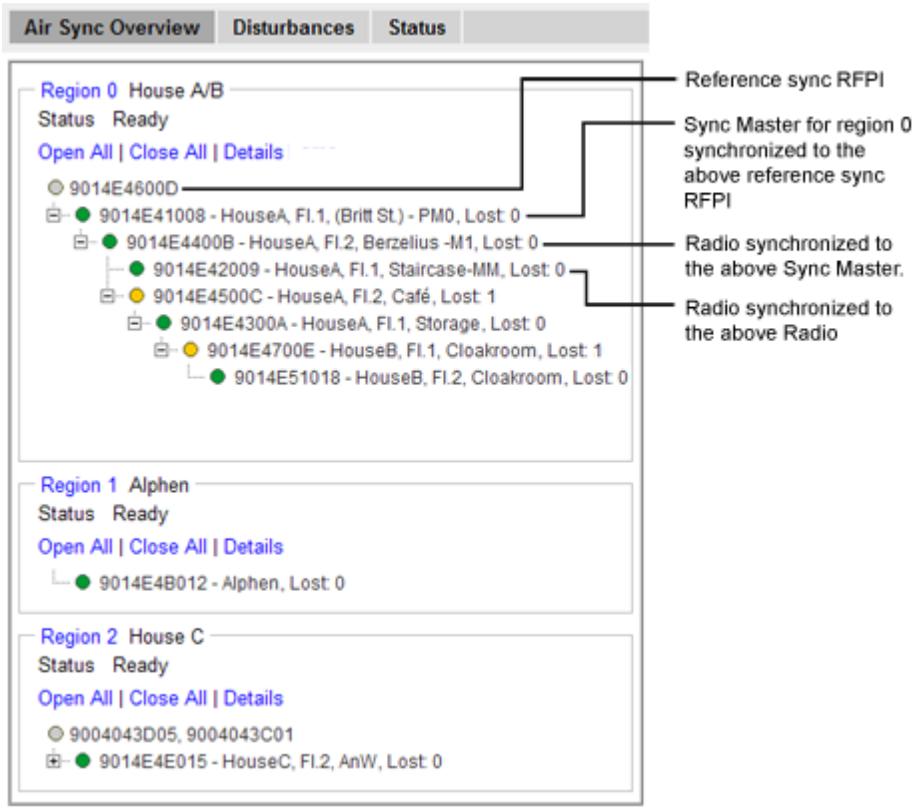


Figure 30. The sync trees for region 0, 1 and 2 where region 0 is fully expanded.

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.
   To clear the counters, click "Clear".

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.

Disturbances

This section only applies to the 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.

Status

This section only applies to the IPBS.

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%. Should be below 90% to be able to keep the synchronization.

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).

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.

Display Calls

All calls on an IPBS/IPBL 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 Canceled	The number of failed handovers in the Radio. NOTE: There can be several reasons for uncompleted handovers occuring. This will in most cases not cause dropped or disconnected calls.

Handover

During call, all ongoing handovers in the IP-DECT system can be displayed by selecting Traffic > Handover in the Master.

Backup

The IPBS/IPBL configuration can be downloaded and saved on a disc or a server. This is useful when identical configuration should be applied to several IPBSs/IPBLs, for example when configuring the Radios in a system. For information on how to load a saved configuration on the IPBS/IPBL, see System Downgrade for IPBS2 and DB1 on page 132.

1. Select Backup > Config.
2. Click "download".
3. Click "download with standard password" to save the configuration with the default system password.
4. Click "Save" in the dialogue window and browse to the place where the configuration should be saved.
5. Click "Save".

System Upgrade from Software Version 4.x.x to 5.0.x

Radios with software version 4.x.x will not be able to connect to a Master with software version 5.0.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 Master.

System Downgrade for IPBS2 and DB1

This section applies only to IPBS2 and DB1 with the following article numbers that can be found on the label on the backside of the device:

- IPBS2-**A
- DB1-**A

Note: When downgrading, minimum version of the software that runs on IPBS2 is 7.2.11 and on DB1 it is R3E.

Update

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

- Update Configuration
- Update Firmware
- Update the Boot File
- Update the RFPs

Update Configuration

A previously saved configuration can be loaded and activated on the IPBS/IPBL. See Backup on page 132 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 Reset on page 141.

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. Both IPBS1 and IPBL have "big-endian" CPUs compared to IPBS2 which have "little-endian" CPU. Hence, IPBS1 and IPBL are compatible.

If a device (e.g. IPBS2) is configured and the configuration is taken from another type of device (e.g. IPBS1), some lines in the configuration will be skipped by the configured device (IPBS2). 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).

Update Firmware

Updated software files are distributed by your supplier.

There are two ways to update the firmware:

- Using an update server, see Appendix A: How to Configure and Use the Update Server on page 153.
- 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 Reset on page 141.

Update the Boot File

Updated software files are distributed by your supplier.

There are two ways to update the boot file:

- Using an update server, see Appendix A: How to Configure and Use the Update Server on page 153.
- 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 Reset on page 141.

Update the RFPs

This section only applies to the IPBL.

Updated software files are distributed by your supplier.

There are two ways to update the RFPs:

- Using an update server, see Appendix A: How to Configure and Use the Update Server on page 153.
- Manual update, see below.

To update manually:

In the RFP status list, information on connected RFPs are displayed.

1. Select Update > RFPs.
2. Click "Browse..." and browse to the RFP update file.
3. Click "Upload".

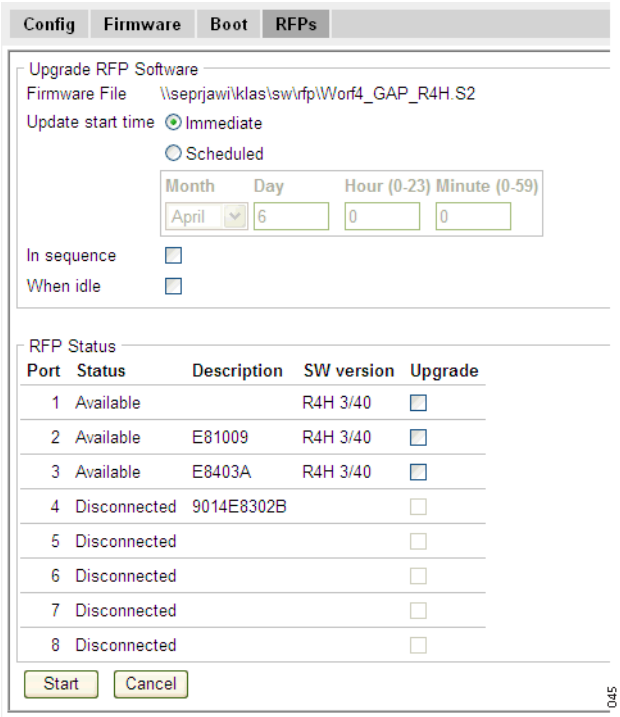


Figure 31. Upgrade the RFP.

4. Select "Immediate" or "Scheduled" update.
5. Select "In sequence" check box to update the selected RFPs one by one.
6. Select "When idle" check box to start the update when the RFP is idle.
7. Mark the applicable RFPs to be updated.
8. Click "Start" to upgrade the selected RFPs.

The RFP restarts after the upload is finished.

Diagnostics

Logging

The IPBS/IPBL 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 Enable the Radio on page 107. 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.
DECT Master	Logs generated by the Master software component in the IPBS/IPBL.
DECT Radio	Logs generated by the Radio software component in the IPBS/IPBL.
DECT Stack	A low level DECT log, intended for support departments.
Config Changes	Logs generated upon configuration changes in the IPBS/IPBL or the IP-DECT system.

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.

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.
3. The Trace check box in the Remote PCAP section is mainly used by the R&D department to follow the desired network attributes.
4. Select the TCP/UDP Traffic check box in the IP section to capture traffic information.
5. Click "OK".

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 Fault Code Descriptions on page 145.
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.

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 Fault Code Descriptions on page 145.
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.

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 etc. 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.
Temperature (only for IPBL)	Shows the temperature of the cabinet.
Voltage (only for IPBL)	Shows the power supply voltage level. An alarm warning about high voltage will be sent at 54 V. An alarm warning about low voltage will be sent at 42 V. The IPBL will shut down when the voltage drops below 36 V or goes above 60 V.

1. Select Diagnostics > Performance
2. Select the checkbox(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.

Config Show

Under Diagnostics > Config Show, the configuration is displayed as a text output.

Ping

The ping function is used to determine the response time from the IPBS/IPBL to a certain IP address. It can be used to analyse the connection between the IP-DECT system components.

1. Select Diagnostics > Ping.
2. Enter an IP address in the IP Address text field.
3. Press "Enter" on the keyboard.

Traceroute

The traceroute function displays how packets travel from the IPBS/IPBL 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.

Environment

This section only applies to the IPBL.

The environment tab gives information power supply and consumption. It also display temperature and fan status.

1. Select Diagnostics > Environment.
2. The following information is available in the Power section:
   - Power supply - AC or DC power port.
   - Voltage - input voltage.
   - Current consumption - total consumption for the IPBL an the connected RFPs.
     – Max 4,0 A when supplied with AC power port
     – Max 5,2 A when supplied with DC power port
3. The following information is available in the Environment section:
   - Temperature - °C
   - Fan status - OK, not OK

RFP Scan

This section only applies to the IPBS.

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"

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.

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/IPBL.
- Immediate reset - clears all calls and resets the IPBS/IPBL.

Idle Reset

1. Select Reset > Idle Reset.
2. Click "OK".
3. The IPBS/IPBL will reset when there are no active calls.

Immediate Reset

1. Select Reset > Reset.
2. Click "OK".
3. The IPBS/IPBL will terminate all active calls and reset.

TFTP Mode

Note: When the IPBS/IPBL is in TFTP mode it can only be reached using the gwload utility. This mode should not be used during normal operation.

Boot

When the IPBS/IPBL 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".

Reset Using the Reset Button

It is possible to do a hardware reset of the IPBS and IPBL by pressing the reset button. The button is accessed through a hole in the back of the IPBS (IPBS1: figure 1 on page 10, IPBS2: figure 2 on page 13) and on the front of the IPBL (figure 4 on page 17).

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 and IPBL 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.

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.

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.

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.

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.

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.

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.

Troubleshooting

Load Firmware Using the Gwload Tool

If the firmware is corrupt, for example if firmware download is interrupted the IPBS/IPBL 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/IPBL 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/IPBL in TFTP-mode by performing a medium (~3 sec) hardware reset, see Reset Using the Reset Button on page 142.
3. Start a command window.
4. 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
   - **IPBL:**
     gwload /setip /i <ipaddress> /gwtype 4001 /prot <..path/firmwarefilename> /go
5. If there is more than one IPBS/IPBL in TFTP mode, select the unit to update and press enter.

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
The LDAP replicator is not connected (Users)	0x00030001	IPBS/ IPBL		X	
CPU resources are not available (Radio)	0x00030101	IPBS/ IPBL			X

Standby master active (Master)	0x00030201	IPBS/ IPBL		X	
User registration failure (Master)	0x00030202	IPBS/ IPBL		X	
Connection to Radio lost (Master)	0x00030204	IPBS/ IPBL		X	
Primary/redundant trunk is down (Master)	0x00030205	IPBS/ IPBL		X	
Master active (Master) This event is generated when the Mirror becomes active.	0x00030206	IPBS/ IPBL			X
Master inactive (Master) This event is generated when the Mirror becomes inactive.	0x00030207	IPBS/ IPBL			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/ IPBL		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 signaling problem (media negotiation).	0x00050001	IPBS/ IPBL		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/ IPBL		X	
Wrong payload type received (RTP) Caused by signaling/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/ IPBL		X	
Stun failed (RTP)	0x00050004	IPBS/ IPBL		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/ IPBL		X	
Status inquiry (H323)	0x00060002	IPBS/ IPBL		X	

Signaling TCP failed (H323) The signaling transport connection could not be established. This usually means, the destination (IP) is not reachable. Check network connectivity.	0x00060003	IPBS/ IPBL		X	
Signaling timeout (H323) A signaling timer expired. The reason for this could be a network problem or an interop problem.	0x00060004	IPBS/ IPBL		X	
Invalid URL (WebMedia)	0x00080001	IPBS/ IPBL		X	
Coder missing in URL (WebMedia)	0x00080002	IPBS/ IPBL		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/ IPBL		X	
Unexpected message (TLS)	0x000c010a	IPBS/ IPBL			X
Unexpected message (TLS)	0x000c020a	IPBS/ IPBL			X
Bad MAC (TLS)	0x000c0114	IPBS/ IPBL			X
Bad MAC (TLS)	0x000c0214	IPBS/ IPBL			X
Decryption failed (TLS)	0x000c0115	IPBS/ IPBL			X
Decryption failed (TLS)	0x000c0215	IPBS/ IPBL			X
Record overflow (TLS)	0x000c0116	IPBS/ IPBL			X
Record overflow (TLS)	0x000c0216	IPBS/ IPBL			X
Decompression failure (TLS)	0x000c011e	IPBS/ IPBL			X
Decompression failure (TLS)	0x000c021e	IPBS/ IPBL			X
Handshake failure (TLS)	0x000c0128	IPBS/ IPBL			X
Handshake failure (TLS)	0x000c0228	IPBS/ IPBL			X
No certificate (TLS)	0x000c0129	IPBS/ IPBL			X
No certificate (TLS)	0x000c0229	IPBS/ IPBL			X

Bad certificate (TLS)	0x000c012a	IPBS/ IPBL			X
Bad certificate (TLS)	0x000c022a	IPBS/ IPBL			X
Unsupported certificate (TLS)	0x000c012b	IPBS/ IPBL			X
Unsupported certificate (TLS)	0x000c022b	IPBS/ IPBL			X
Revoced certificate (TLS)	0x000c012c	IPBS/ IPBL			X
Revoced certificate (TLS)	0x000c022c	IPBS/ IPBL			X
Expired certificate (TLS)	0x000c012d	IPBS/ IPBL			X
Expired certificate (TLS)	0x000c022d	IPBS/ IPBL			X
Unknown certificate (TLS)	0x000c012e	IPBS/ IPBL			X
Unknown certificate (TLS)	0x000c022e	IPBS/ IPBL			X
Illegal parameter (TLS)	0x000c012f	IPBS/ IPBL			X
Illegal parameter (TLS)	0x000c022f	IPBS/ IPBL			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/ IPBL			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/ IPBL			X
Access denied (TLS)	0x000c0131	IPBS/ IPBL			X
Access denied (TLS)	0x000c0231	IPBS/ IPBL			X
Decode error (TLS)	0x000c0132	IPBS/ IPBL			X
Decode error (TLS)	0x000c0232	IPBS/ IPBL			X
Decryption error (TLS)	0x000c0133	IPBS/ IPBL			X
Decryption error (TLS)	0x000c0233	IPBS/ IPBL			X

Export restriction (TLS)	0x000c013c	IPBS/ IPBL			X
Export restriction (TLS)	0x000c023c	IPBS/ IPBL			X
Protocol version (TLS)	0x000c0146	IPBS/ IPBL			X
Protocol version (TLS)	0x000c0246	IPBS/ IPBL			X
Insufficient security (TLS)	0x000c0147	IPBS/ IPBL			X
Insufficient security (TLS)	0x000c0247	IPBS/ IPBL			X
Internal error (TLS)	0x000c0150	IPBS/ IPBL			X
Internal error (TLS)	0x000c0250	IPBS/ IPBL			X
User cancelled (TLS)	0x000c015a	IPBS/ IPBL			X
User cancelled (TLS)	0x000c025a	IPBS/ IPBL			X
No renegotiation (TLS)	0x000c0164	IPBS/ IPBL			X
No renegotiation (TLS)	0x000c0264	IPBS/ IPBL			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/ IPBL		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/ IPBL		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/ IPBL		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/ IPBL			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/ IPBL			X
RFP disconnected (TAM)	0x000e0001	IPBL		X	
RFP malfunctioning (TAM)	0x000e0002	IPBL		X	
RFP disabled (TAM)	0x000e0003	IPBL		X	
RFP software download (Dwl)	0x000e0004	IPBL		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 110. To resynchronize manually, see Reference Synchronization on page 129.	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	
High temperature (TAM)	0x000f0001	IPBL	X		
High power consumption (TAM)	0x000f0002	IPBL	X		
Supply voltage low (TAM)	0x000f0004	IPBL	X		
Supply Voltage High (TAM)	0x000f0008	IPBL	X		
Fan failure (TAM)	0x000f0010	IPBL		X	

Synchronization ring broken (Sync)	0x00100001	IPBL		X	
Reference synchronization signal lost (Sync)	0x00100002	IPBL		X	
Synchronization lost (Sync)	0x00100004	IPBL		X	
Unsynchronized to reference (Sync)	0x00100008	IPBL		X	
Interface down (ipproc)	0x00110000	IPBS/ IPBL		X	
Interface not configured (ipproc)	0x00110001	IPBS/ IPBL			X
DHCP server not responding (ipproc)	0x00110002	IPBS/ IPBL		X	
Invalid UDP-RTP port base/range (ipproc)	0x00110019	IPBS/ IPBL		X	
Invalid UDP-NAT port base/range (ipproc)	0x0011001a	IPBS/ IPBL		X	
Invalid NAT port base/range (ipproc)	0x0011001b	IPBS/ IPBL		X	
ARP poisoning detected (ipproc)	0x00110041	IPBS/ IPBL		X	
Out of TCP/NAT ports (ipproc)	0x00110046	IPBS/ IPBL		X	
Out of TCP ports (ipproc)	0x00110047	IPBS/ IPBL		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/ IPBL		X	
Out of UDP/RTP ports (ipproc)	0x00110050	IPBS/ IPBL		X	
Out of UDP ports (ipproc)	0x00110051	IPBS/ IPBL		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/ IPBL		X	
No route to destination (ipproc)	0x0011005a	IPBS/ IPBL		X	

No route to destination, if down (ipproc) The IP routing process failed to deliver a packet explicitely 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/ IPBL		X	
No route to destination, if unknown (ipproc)	0x0011005c	IPBS/ IPBL		X	
No route to destination, if unconfigured (ipproc)	0x0011005d	IPBS/ IPBL		X	
No route to destination, no gateway (ipproc)	0x0011005e	IPBS/ IPBL		X	
No route to destination, loop (ipproc)	0x0011005f	IPBS/ IPBL		X	
Memory Low (box) This alarm indicates that there is less then 200000 bytes of memory available for allocation	0x00120001	IPBS/ IPBL	X		
Radio busy for speech (Dect)	0x00140001	IPBS			X

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 UP1 to perform the requested updates.

UP0 can also receive commands from the "Update clients" page of the PBX Administration user interface.

A.2 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.3 Installation

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.

Since all HTTP requests are performed unauthenticated, the website used must allow anonymous read (and potentially write) access. You may want to restrict access to that site to certain network address ranges.

Configure a Microsoft IIS URL to allow PUT commands:

1 Create a directory where you want to save configurations to

2 Create a virtual directory in Microsoft's IIS manager

3 Select "read" and "write" access

No installation is needed on the IPBS/IPBLs.

A.4 Configuration in IP-DECT

See *Configure Automatic Firmware Update* on page 113 on how to configure the IPBS/IPBLs 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.5 Setting the UP1 Parameters

The applet saves the configuration in a line starting config change UP1.

The full syntax is:

```
config change UP1 /url <url> [/poll <slow>] [/poll-fast <fast>]
[/disc]
```

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 is "http://1.2.3.4/configs/", it is expanded to "http://1.2.3.4/configs/update-IPBS.htm".

	Config filename
IPBS1	update-IPBS.htm
IPBS2	update-IPBS2.htm
IPBL	update-IPBL.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 maintenance 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 maintenance 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. You can change this initial polling interval using the /poll-fast <fast> parameter (this is not recommended).

The /disc parameter can be specified to force the device to close the http sessions used immediately.

When the maintenance 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 maintenance 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 canceled.

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 12,23,1,2,3,4
```

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.6 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	ipbs.bin
IPBS2	ipbs2.bin
IPBL	ipbl.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: http://192.168.0.10/firm/ipbs.bin
IPBS2: http://192.168.0.10/firm/ipbs2.bin
IPBL: http://192.168.0.10/firm/ipbl.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	boot_ipbs.bin
IPBS2	boot_ipbs2.bin
IPBL	boot_ipbl.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: http://192.168.0.10/firm/boot_ipbs.bin
IPBS2: http://192.168.0.10/firm/boot_ipbs2.bin
IPBL: http://192.168.0.10/firm/boot_ipbl.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

A.7 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.8 Setting the RFP_UPDATE0 Parameter

To perform a RFP firmware update, use the following commands.

```
mod cmd RFP_UPDATE0 firmware http://192.168.0.10/
Worf4_GAP_R4H.s2
```

The command above specifies the url to the RFP firmware to use.

```
mod cmd RFP_UPDATE0 select 0x2753
```

Specifies which RFPs to update using a hex-encoded bit-mask. Each bit represents an RFP port starting with port 1 at the LSB (0x0001) up to port 16 (0x8000).

0x2753 specifies RFP "1,2,5,7,9,10,11,14" to be updated.

```
mod cmd RFP_UPDATE0 schedule DD.MM.YYYY-HH:MM
```

Specifies when the update shall start. If no date is provided, the update will be immediate when the start command is issued.

```
mod cmd RFP_UPDATE0 start /idle
```

Starts the update or activates the schedule. Normally the /idle command is selected and an update starts only if the RFP is idle.

If multiple RFPs are selected for update, they will be updated one at a time If /sequence command is used.

Example Update RFP Firmware

This example shows an "update file" for the IPBL.

```
mod cmd UP1 check ser 20070316-1

mod cmd RFP_UPDATE0 firmware http://172.20.8.125/ascom/rfp/
Worf123.S2

mod cmd RFP_UPDATE0 select 0xffff

mod cmd RFP_UPDATE0 start /idle
```

A.9 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/IPBL, 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

- Must be a Windows 2008 R2 server containing Microsoft IIS ver. 7.5.

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.

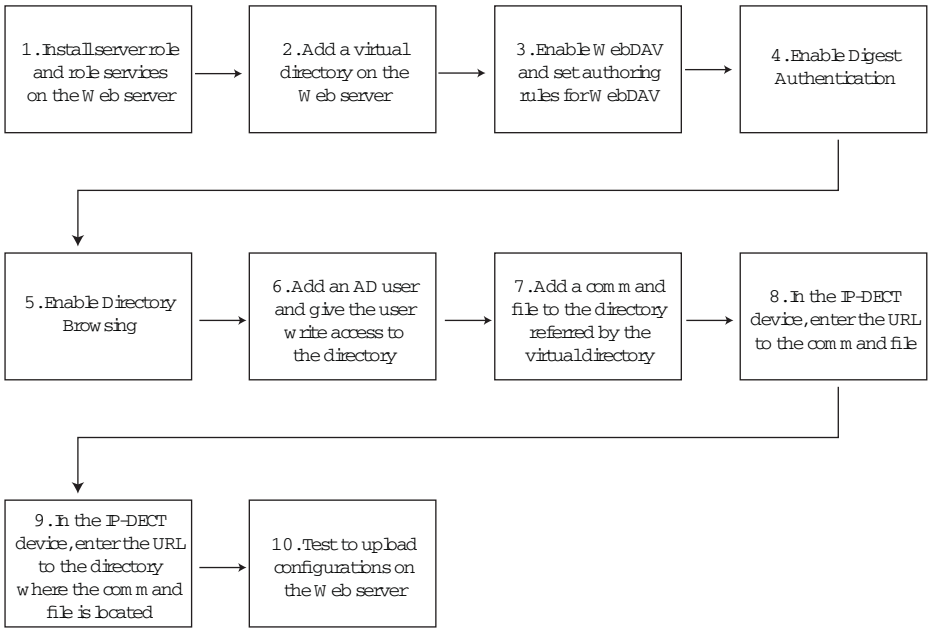


Figure 32. To configure Microsoft IIS as an Update Server.

1. Install server role and role services on the Web server

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 Make sure 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".

2. Add a virtual directory on the Web server

10 In "Internet Information Services (IIS) Manager": Right-click on "Default Web Site" and select "Add Virtual Directory..." (menu item). The "Add Virtual Directory" window is shown.

11 In the *Alias* text field, enter a name for the virtual directory.

12 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.

13 Close the "Add Virtual Directory" window, click "OK".

3. Enable WebDAV and set authoring rules for WebDAV

14 In "Internet Information Services (IIS) Manager": Left-click on "Default Web Site".

15 Left-double click on "WebDAV Authoring Rules"

16 Left-click on "Enable WebDAV" (link).

17 Left-click on "Add Authoring Rule..." (menu item)". The "Add Authoring Rule" window is shown.

18 In section *Allow access to this content to:*, select the *All users* option.

19 In section *Permissions*, select the *Read*, *Source* and *Write* check boxes.

20 Click "OK".

4. Enable Digest Authentication

Note: Digest Authentication requires that the Web server is joined to a domain.

21 Left-click on the virtual directory.

22 Left-double click on "Authenticaton" and left-click on "Enable" (link).

5. Enable Directory Browsing

23 Left-click on the virtual directory.

24 Left-double click on "Directory Browsing" and left-click on "Enable" (link).

6. Add an AD user and give the user write access to the directory

Note: This section requires an existing Active Directory (AD) user.

25 Right-click on the virtual directory and left-click on "Edit Permissions..." (menu item). The *Properties* window for the virtual directory is shown.

26 Click on the *Security* tab.

27 Click on "Edit..." (button). The "Permissions for *virtual directory name*" window is shown.

28 Click on "Add" (button). The "Select Users, Computers, Service Accounts, or Groups" window is shown.

29 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.

30 Click "OK".

31 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.

32 Click "OK".

33 Click "OK".

7. Add a command file to the directory referred by the virtual directory

34 Add a command file to the directory referred by the virtual directory. For information on the command file syntax, see A.6 *Setting the UP0 Parameters* on page 155.

8. In the IP-DECT device (IPBS/IPBL), enter the URL to the command file

35 See *Configure Automatic Firmware Update* on page 113 on how to configure the IPBS/ IPBLs for automatic update.

9. In the IP-DECT device (IPBS/IPBL), enter the URL to the directory where the command file is located

36 Select Services > HTTP Client.

37 In section *Authenticated URLs*, enter in the *URL* text field the URL to the directory.

38 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 159.

39 In the *Password* text field, enter the password.

10. Test to upload configurations on the Web server

40 During the test period, set the poll interval to 1 minute.

41 When the command file has been run, check that the label data in the IPBS/IPBL (select Services > Update) is the same as in the command file.

42 Check that the configuration file is located in the directory.

Appendix B: 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 C: Install Certificate in the Web Browser

To access the GUI for an IPBS/IPBL using secure web access (https), the certificate for the IPBS/IPBL 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 *C.1 Create a Certificate*.

Step 2. Install the certificate in the web browser. See *C.2 Install the Certificate*.

C.1 Create a Certificate

Note: Make sure the name you use to access the IPBS/IPBL 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 87.

- 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) or Certification Request* on page 32.

C.2 Install the Certificate

The instructions below apply for Internet Explorer version 8 and may 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 an IPBS/IPBL. A security warning window will appear when using secure web access (https) to access the GUI.

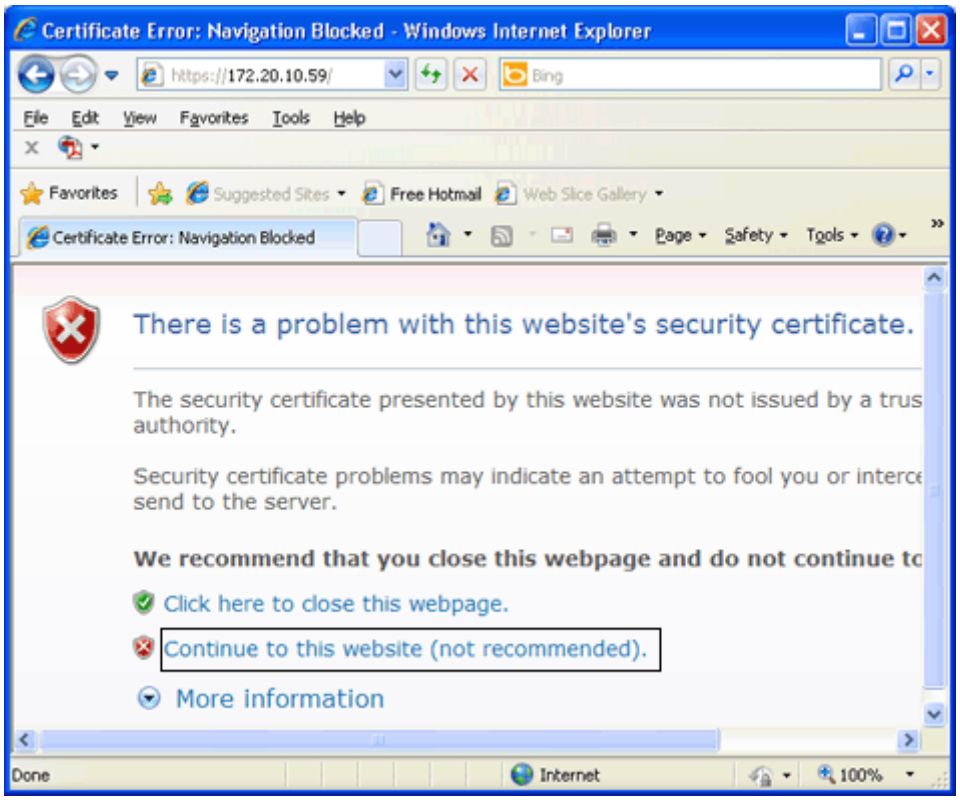


Figure 33. Security warning window.

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 34. The Security Report window will appear,

see Figure 35.

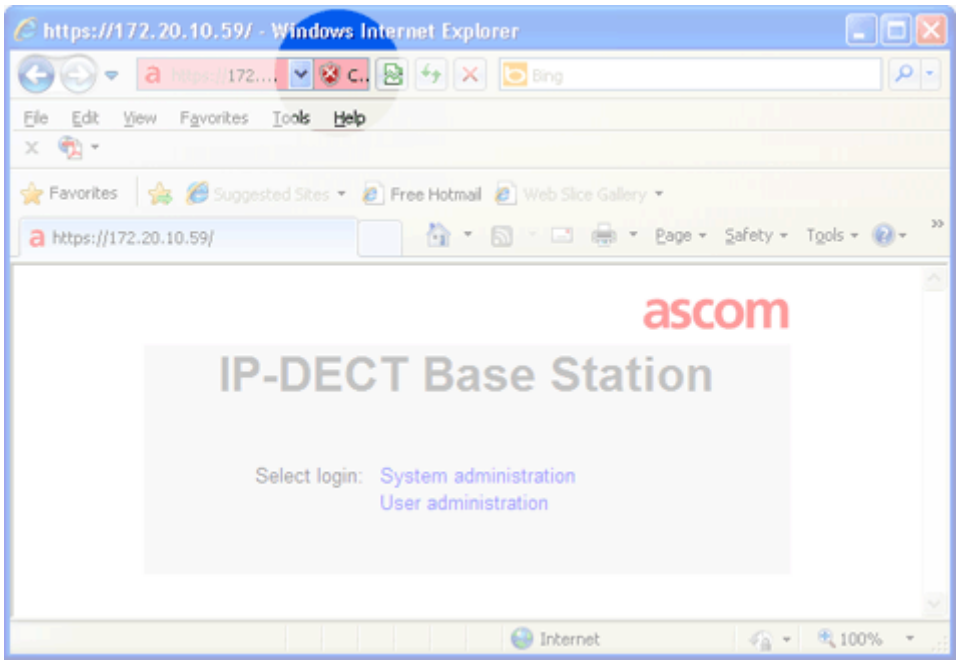


Figure 34. Sceen shot of the login window, with the "Security Status bar highlighted.

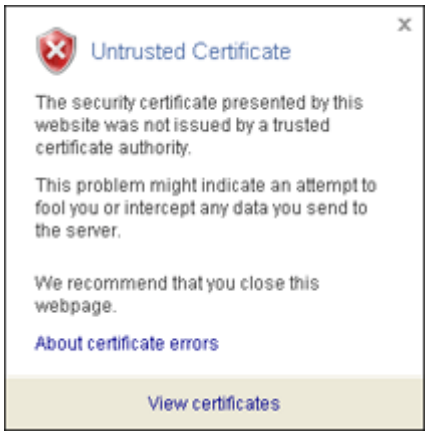


Figure 35. The Security Report window.

4 In the Security Report window, click on the blue text link "View certificates". The Certificate window will appear.

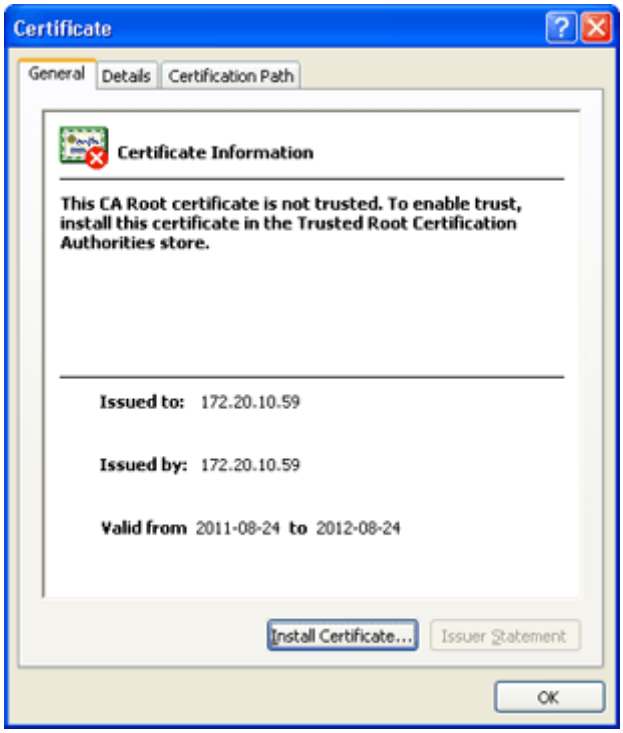


Figure 36. The Certificate window.

5 In the Certificate window, click on the button "Install Certificate...". The Certificate Import wizard is started.

6 Click on "Next".

7 Make sure that option "Automatically select the certificate store based on the type of certificate" is selected, see Figure 37. Click on "Next".

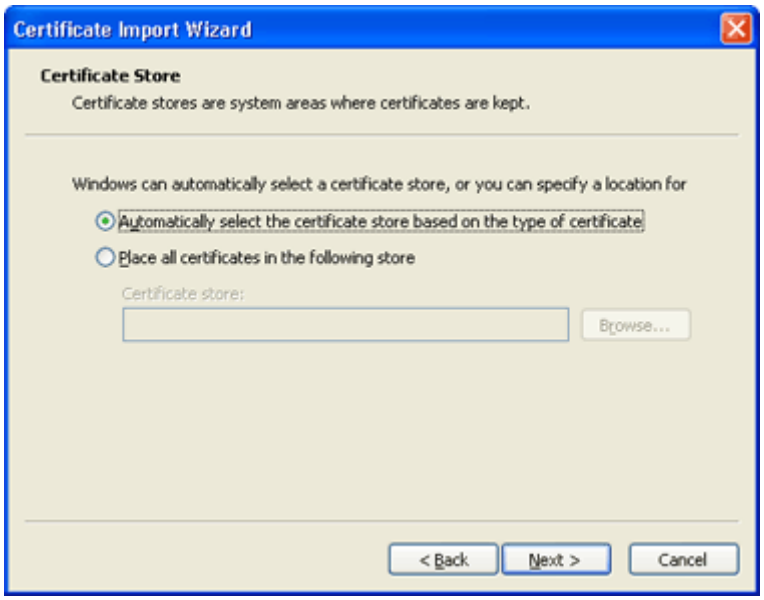


Figure 37. The Certificate Import wizard.

8 Click on "Finish" to complete the Certificate Import wizard. The Security Warning window will appear.

9 Click on "Yes" to install the certificate".

Appendix D: Used IP Ports

Port	TCP/UDP	Protocol	Comment
68	UDP	DHCP	
80	TCP	HTTP	Configurable
88	UDP	KERBEROS	
123	UDP	NTP	
161	UDP	SNMP	
389	TCP	LDAP	
636	TCP	LDAPS	
443	TCP	HTTPS	Configurable
464	UDP	KERBEROS	
1716-1717	TCP	H.323	Master
1718-1719	UDP	H.225	Master, Radio
1718-1719	TCP	H.323	Radio
1722-1723	TCP	H.323	Master
1724-1727	TCP	H.323	Radio
1814-1817	TCP	UNITE	Messaging
3217	UDP	UNITE	IP-DECT Device Management, Fault Reporting, Service Discovery
12346	TCP	UNITE	Portable Device Management
16384-32767	UDP	RTP	Media (port range is configurable)

Appendix E: Configure DHCP Options

IPBS/IPBL include a DHCP client which allows the IP interface to be configured from a DHCP server. In addition to that, IPBS/IPBL also allow configuring a number of settings via special DHCP vendor options.

E.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.

E.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.

E.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-signalling 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 signalling 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

E.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.

E.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.

E.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.

E.7 VLAN set with LLDP

From version 7.1.X, VLAN is also set with LLDP if provided by the switch. See *Configure VLAN* on page 93.

E.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.