Avaya DECT R4 System Description

21-604149
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)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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.

Introduction

Avaya IP-DECT is an IP-based cordless telephony and messaging system to connect to private telephone exchanges.

The IP-DECT system supports the DECT standard which gives a full integration of messaging and voice functions. You can also integrate the DECT-system with external applications such as different alarm systems. This system gives features such as; messages to telephone, alarm from telephone, message acknowledgment, and absent handling.

Abbreviations and Glossary

AIWS2	Avaya In-Building Wireless Server:. An application suite running on an Elise3 server. It enables wireless services to and from handsets and chargers.
CKI	The CKI, Cipher Key Index, is stored in both the handset and in the system and is used for Early Encryption. It uniquely identifies a DefCK and is used for Early Encryption.
DECT	Digital Enhanced Cordless Telecommunications: global standard for cordless telecommunication.
DefCK	The DefCK, Default Cipher Key, is stored in both the handset and in the system and is used for Early Encryption.
GAP	Generic Access Profile: communication protocol standard within DECT, that guarantees compatibility of systems and components.
IP	Internet Protocol: global standard that defines how to send data from one computer to another through the Internet
IPBS	IP-DECT Base Station
IPBL	IP-DECT Gateway
ISDN	Integrated Services Digital Network
LAN	Local Area Network: a group of computers and associated devices that share a common communication line.
LDAP	Lightweight Directory Access Protocol
OAP	Open Access Protocol: XML based protocol used to create customized applications for Unite access.
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.

PSTN	Public Switched Telephone Network
RFP	Radio Fixed Part. DECT base station part of the DECT Infrastructure. TDM-DECT base station connected to an IPBL or the local RFP part in an IPBS.
Roaming	The procedure of moving the handset from one IPBS/IPBL to another and still be able to place outgoing and receive incoming calls.
External Handover	The procedure of moving an active call from one IPBS/IPBL to another.
QSIG	Q-signalling: a set of standards defined by ECMA, ESTI and ISO for connection PBX to PBX in networks.
SMS	Short Message Service: global protocol for sending messages between cordless telephones.
VoIP	Voice over IP

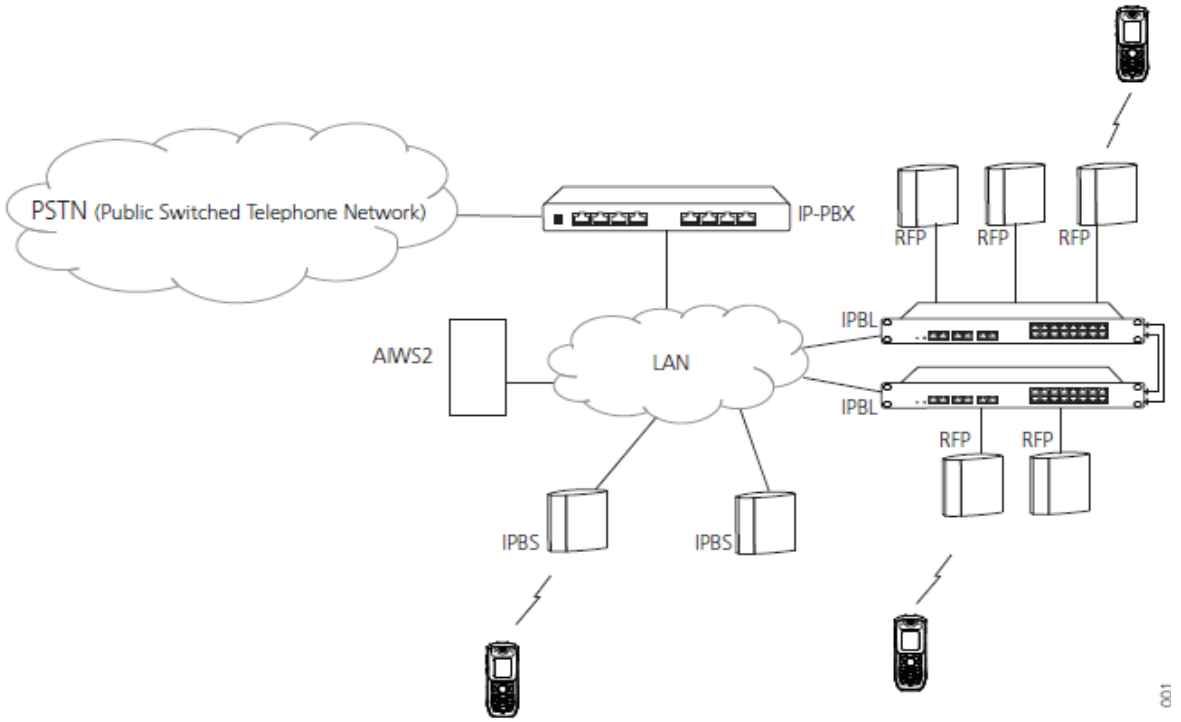
System overview

Avaya IP-DECT System is a wireless communication system that is cost efficient with modularity up to very large installations. Avaya IP-DECT system is a feature-rich distributed system that can be installed at local office or on-site and a wide variety of connection possibilities.

Avaya IP-DECT system components:

- DECT Cordless Handsets
- IP-DECT Base Station (IPBS), or Compact IP-DECT Base Station
- IP-PBX
- IP-DECT Gateway (IPBL)
- Radio Fixed Part (RFP)
- Avaya In-Building Wireless Server (AIWS2)

Figure 1: IP-DECT System Overview



IP-DECT System Overview

Supported Standards

- H.323 XMobile incl. H.450
- G.711 (a-law and mu-law)
- G.723-53
- G.729-A/AB

System functions

Avaya IP-DECT system is designed to enable voice traffic, messaging, and alarms between cordless telephones within an enterprise LAN. For details see *Function Description Document, Avaya IP-DECT System*.

DECT functions

DECT is a digital wireless technology that originated in Europe, but is now being adopted increasingly worldwide, for cordless telephones, wireless offices, and even wireless telephone lines to the home. DECT has been designed and specified to interwork with many other types of network, such as the PSTN, ISDN, and GSM.

Common IP-DECT functions are handled entirely within the IP-DECT system.

Roaming and handover

The IP-DECT system supports roaming between all base stations and gateways in the system. The IP-DECT system also supports handover if there is overlapping speech coverage.

Enhanced DECT Security

The enhanced DECT security feature is a mechanism to enhance DECT security by introduction of early encryption and re-keying during an ongoing call. It also addresses the security risk of staying permanently open for registration.

Early Encryption

This procedure is used for encryption of each DECT link, directly after establishment. The purpose is to protect data like caller ID and dialed digits, exchanged before encryption with the handsets private cipher key can start.

When a handset that supports early encryption is registered, a CKI with a corresponding DefCK is allocated/calculated and stored both in the handset and in the IP-DECT system. The CKI uniquely identifies the corresponding DefCK for each handset within the system. Later at each DECT link establishment this CKI is used to identify the DefCK to be used for early encryption of the link. The handset will release the connection in case early encryption activation is rejected.

Re-keying

This procedure periodically modifies the handsets private cipher key used for encryption of an ongoing call. The purpose is to protect against any attempts to crack the ciphering e.g. like super-computing.

Subscription Requirements

This procedure is used to control if registration is allowed or not. A system that permanently allows registration will make it possible for an attacker to do over-the-air subscriptions using exhaustive testing of AC-codes.

The subscription method “With System AC”, used to allow anonymous registrations, will permanently allow subscription attempts.

Therefore, for safety reasons, when the anonymous registration is finished change the Subscription Method to "Disable"or "With User AC".

With the subscription method “With User AC”, the system will allow subscription attempts only after activation in the IPBS/IPBL web GUI. The system will thereafter remain in enabled subscription mode for a maximum time of two minutes. After successful registration of the activated IPEI, the system will not allow registrations any longer.

LAN/WAN

Several vendors provide components needed to deploy a LAN or WAN. For optimal performance for IP-DECT the following is recommended:

- Administer Quality of Service (QoS)
- Connect the infrastructure to a switched network. (i.e hubs or repeaters should be avoided)
- Use a backbone of least 100 Mbps depending on the network size.

LDAP

The LDAP protocol is used in the IP-DECT system between two or more Master IPBSs/IPBLs if different network regions shall be used.

Supported third-party functions

IP-PBX are examples of third-party products required when setting up the DECT infrastructure. The Avaya developed products are designed to work in system provided by different vendors.

IP-DECT System

The major parts of the Avaya IP-DECT system are the IP-DECT Base Station (IPBS) and IP-DECT Gateway (IPBL) consisting of the software components DECT Radio (interface) and DECT Master.

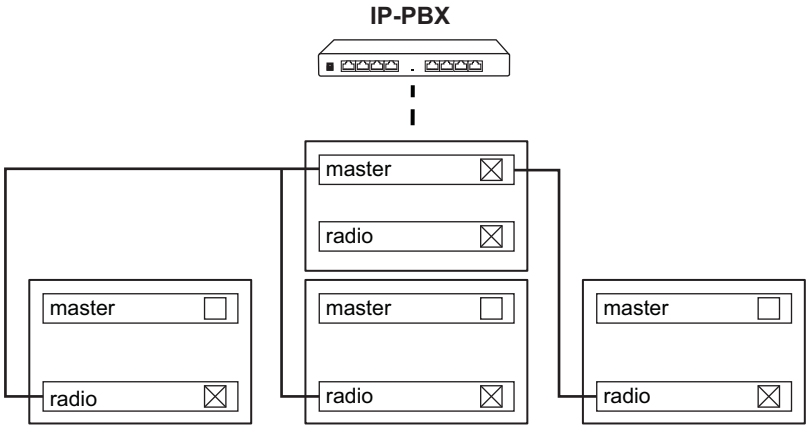
There is only one DECT Master in a single site IP-DECT system. In a multiple site IP-DECT system, each site is connected with the PBX through an own DECT Master and an H.323 XMobile trunk.

The IPBS/IPBL is connected to an IP network through the LAN interface, which provides connectivity to the IP-PBX.

System layout

All IPBSs/IPBLs are connected to the LAN, but it is only the DECT Master that have a logical connection to the IP-PBX. It is a flat layout where all DECT Radios are logically communicating directly to the DECT Master, see figure 2 on page 10.

Figure 2: Logical connections of the software components DECT Master and DECT Radio



DECT Master

The DECT Master is a software interface between the IP-DECT system and the IP-PBX. The DECT Master is responsible for all DECT handsets in the system.

The DECT Master knows which DECT Radio the handsets are located to, that is which DECT Radio in the system that received the latest location registration message from the handset. A call to a handset is directed only to the DECT Radio where the handset is located. Thus limiting the H.323 XMobile and DECT load in the system.

DECT radio

The DECT Radio is a software interface between DECT and H.323 XMobile. A DECT Radio always communicates with one DECT Master. The DECT Radio only has information of the DECT handset which currently are on the same radio channel.

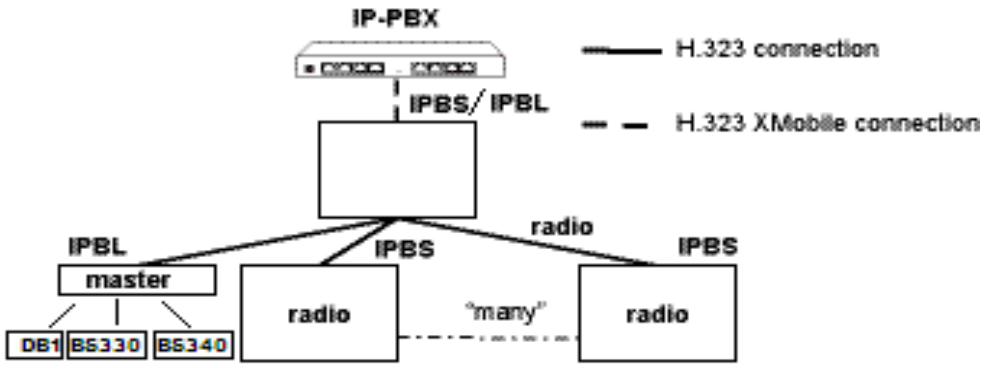
Single Site Installation Example Layout

Customers who require a single-site installation can use the layout in figure 3 for installation.

The system capacity for a single-site layout is:

- Up to 1000 users
- If the number of system IDs used in the installation is between 1 to 36:
  - Max. 1023 IPBS / Master
  - Max. 240 IPBL / Master
- When the number of system IDs used in the installation is between 37 to 292:
  - Max. 127 IPBS / Master
  - Max. 127 IPBL / Master

Figure 3: Single site layout with one IP-DECT Master



In figure 3, the lines that connect Communication Manager (IP-PBX), DECT Master, and DECT Radios indicate the logical connection between the software modules.

Note:

The figure 3 shows the software components. An IPBS includes both the software components DECT Master and DECT Radio.

Assign the role of master to one IP base station or gateway. The IPBS/IPBL can also act as a DECT Radio and have an active DECT Radio and an active DECT Master software component. All other IPBS/IPBLs will only have the software component "DECT Radio" active. The software component "DECT Master" will only be active in the Master, in all other cases it will be deactivated.

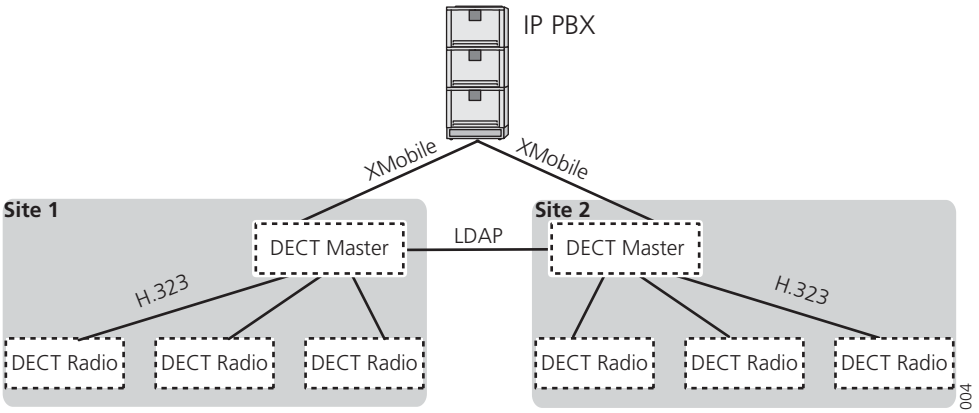
Multiple-site installation

You can use the single site layout for installation on several sites. The sites may have one DECT Master per site and one or several base stations at each site. Communication Manager is centrally located (may be one of the sites), see figure 4.

The system capacity for a multiple-site layout is:

- Up to 1000 users
- When the number of system IDs used in the installation is between 1 to 36:
  - Max. 1023 IPBS / Master
  - Max. 240 IPBL / Master
- When the number of system IDs used in the installation is between 37 to 292:
  - Max. 127 IPBS / Master
  - Max. 127 IPBL / Master

Figure 4: Multiple site layout with one IP-DECT Master per site



The lines displayed between the Communication Manager, the respective DECT Master and the DECT Radios in figure 4 are used to indicate the logical connection between the software modules.

Note:

An IPBS/IPBL includes both the software components DECT Master and DECT Radio.

External handover is only possible to do within each site, not between sites.

Each IP-DECT Master must be assigned an unique master identity to update the IP-PBX with correct information about the handset's location when it is roaming between different sites. See the following example for more information.

Example:

The identity for each IP-DECT Master is set according to the table below.

Site	IP-DECT Master ID
Site 1	1
Site 2	2

A handset being on Site 1 and Master 1 has indicated to the IP-PBX that Master 1 shall be used for incoming calls to the handset. When the handset is entering Site 2, the LDAP database will be updated with the new location of the handset, in this case, Master 2 shall be used for incoming calls to the handset.

Standby Devices

It is recommended to have Standby devices in an IP-DECT system. When a Master goes down the corresponding Standby Master takes over.

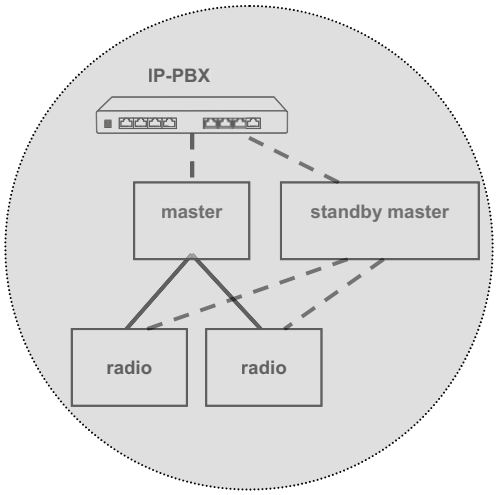


Figure 5. An IP-DECT system with a Standby Master.

Mirror Devices

For redundancy purposes, the Master can act in two ways: As Standby Master and Mirror. However, there are some limitations when using Standby Masters and in these cases using Mirror Masters can be a solution.

Description of Mirror Mode

Mirror Masters are configured in pairs in the same way as Active and Standby Masters are. A Mirror Master can act in both the two previous modes, Active and Standby. One Mirror will initially take the Active role while the other Mirror becomes the Standby. Both the previously used modes "Active" and "Standby" can now instead be set to "Mirror". It is not possible to mix the Mirror mode with any other modes, both masters must be set to Mirror.

The administrator decides which Mirror that initially should be the active one by clicking on the "Activate mirror" link in that device. When the active Mirror fails, the Mirror acting as the standby will automatically become the active Mirror. When the failing Mirror is in operation again it will take the role as the standby and stay inactive.

The administrator can, when both Mirrors are in operation, switch the active role by clicking on the "Switch active mirror" link. This should then be done within a maintenance window as all ongoing calls will be lost.

In the special case where both Mirrors become active due to a network error between the Mirrors, conflicts might arise when the connection between the Mirrors is established again. In this case the Mirror that became active most recently will "win" and changes made to the other mirror will be lost.

The LDAP replication of the user database between Mirrors will be done automatically when needed and no configuration of this is necessary when using the Mirror mode.

If LDAP replication is also used towards an IP6000 or an Active Directory this must be configured at both Mirrors. This replicator will be disabled automatically when the Mirror is inactive.

The Mirror mode will not affect the communication towards the IP-PBX except for the change of master IP address after a fail over.

Benefits With Mirror Mode Compared to Standby Mode

Note:

For new installations we recommend to use the Mirror mode.

The functionality will not be limited when failing over to the Mirror that has acted as Standby. It will still be possible to add/edit/delete users, login/logout shared phones and subscribe new handsets. With the Standby mode this is not possible.

When the failing Mirror becomes available again the system will not automatically fall back to this Mirror and this is not necessary from a functional point of view. If the administrator anyway wants this to happen it is possible to manually switch back to the previously active Mirror. This should then be done at an appropriate time as ongoing calls will be lost. With the Standby mode the fallback is uncontrolled and can be brutal as ongoing calls are lost.

The LDAP replication of users will be done automatically when needed and no configuration of this is necessary with the Mirror mode.

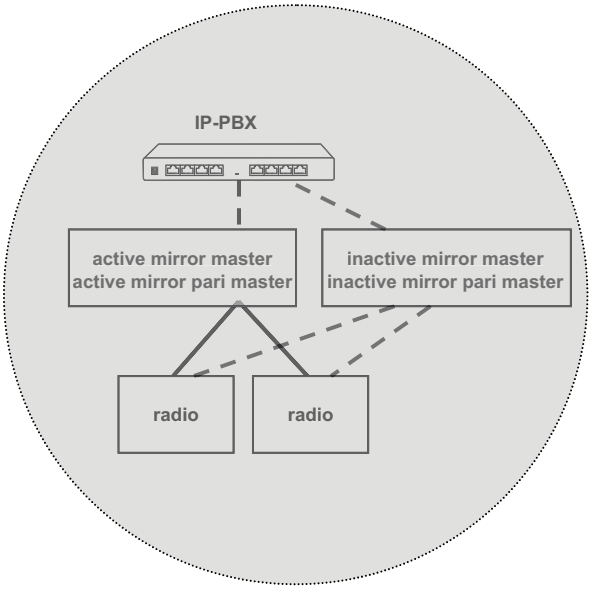


Figure 6. An IP-DECT system with Mirror Masters.

Messaging in Multiple Site Systems

For messaging purposes, the IP-DECT system can be connected to one or several Avaya In-Building Wireless Server (AIWS2). To have messaging functionality for all handsets in a multiple site system, each Master with handsets assigned must have a connection to an AIWS2

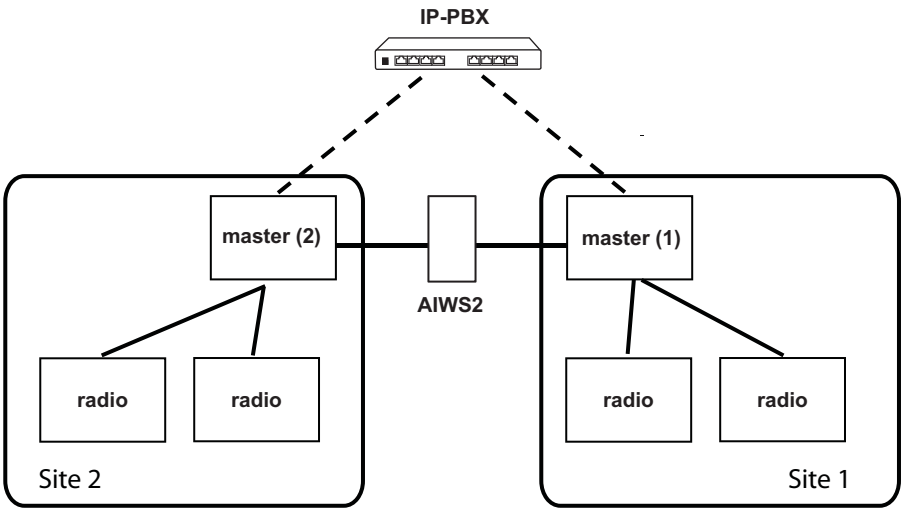


Figure 7. Messaging in Multiple Site Systems.

Example

A handset with extension 1111 is located at Site 1. In this case, the AIWS2 is configured to route all messages to handsets with extensions between 1000-1200 via the Master 1. The AIWS2 will route all messages to handsets with extensions between 1201-1300 via Master 2.

Device Management

A Device Manager (included in the AIWS2) is an application for managing handsets and chargers in wireless systems.

The Device Manager supports software downloads to handsets. The table below shows approximately download times for DECT handsets 3720, 3725 and 3745 when done over-the-air.

	IPBS	***IPBL***
3720	approx. 17 min.	approx. 102 min.
3725, 3745	approx. 25 min.	approx. 189 min.

The software downloads capacity is depending on call traffic in the following way:

IPBS: 0-4 simultaneous downloads depending on call traffic, see below.

Number of calls	*Number of possible simultaneous downloads*
0	4
1	3
2	2
3	1
4 or more	0

IPBL: 0-4 simultaneous downloads depending on call traffic. Same limitations as for IPBS, see above.

AIW2: Max. 10 simultaneous downloads (max. 20 when using an external web server).

There are a number of factors that affect the software download time:

- The number of base stations.
- The number of handsets per base station.
- How much the handsets are moving between the base stations. When moving between RFPs there will be a 1-2 minute break in the software download.
- Speech calls will delay the software download.

Device Management in Multiple Site System

If a handset is moved between several system/sites, it is possible to determine on which site/system the handset shall synchronize with the Device Manager.

For example, a handset with extension number 1111 is registered in System A. When the handset is present in this system, it will synchronize with Device Manager. If the same handset is registered with number 2222 in System B, no synchronization will be performed.

In this case, the System A is considered as the handset's "home" system and it can only be synchronized within this system and only when present in this system.

See the handset's Configuration Manual for more information about the settings.

Synchronization

Synchronization within the IP-DECT system is done by:

- Air synchronization (IPBS)
- Ring Synchronization (IPBL)

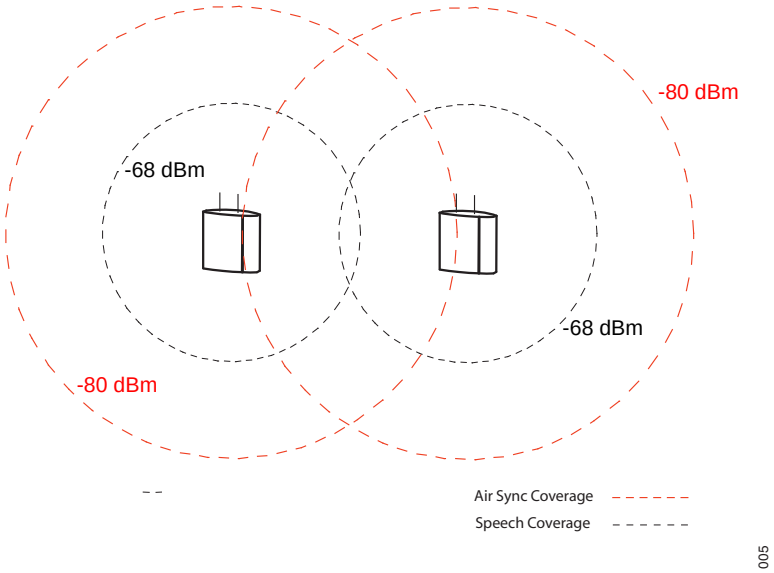
Air synchronization

IP-DECT base stations use the DECT air interface to synchronize to each other. This makes it possible to fulfill the Common Alerting Protocol (CAP) standard and to use the existing portables.

Configure one IPBS as a synchronization master. From this sync master all other IP base stations adjust their internal crystal oscillator to have the same frequency drift as the master. All base stations need not be within coverage of the master base, a IPBS running in slave mode can synchronize to another IPBS in slave mode.

You need not configure which IPBS to synchronize to. This is handled automatically by introducing a proprietary message called "air sync hop" that is sent from the IPBSs.

Figure 8: Air and speech sync radius.



A single IPBS failure may spread to other IPBSs. Therefore, for critical systems you need to install the IPBSs within coverage of at least two alternative IPBSs to sync with.

It is also possible to configure one backup sync master in case of failure of the sync master.

Speech radius: The radius of the circle (circular radiation patterns of the IPBS antennas are assumed), around a particular IPBS, in which portable parts can communicate with that IPBS. See figure 8: Air and speech sync radius.

Note:

The signal strength must be at least -68 dBm for good speech quality. The -68 dBm circles must overlap to ensure seamless handover between 2 base stations (The handset should receive the next base station with -62 dBm at the -68 dBm circle of the first base station).

Sync radius: The radius of the circle, around a particular IPBS, in which other IPBSs lose synchronization with that IPBS with a given synchronization loss probability. The size of the sync radius depends on requested probability of losing synchronization. See figure 8: Air and speech sync radius.

Note:

A value of -80 dBm is a recommendation to ensure good sync conditions.

Ring synchronization

Each synchronization port sends and receives synchronization signals. Each IPBL has two ports *in* and *out* for ring synchronization and two ports *in* and *out* for reference synchronization.

The ring synchronization can be made in two different ways:

- Redundant (preferred)
- Non-redundant

Each synchronization ring dynamically assigns a sync master.

IP-DECT System Management

Onsite management

To manage IPBS and IPBL, use the web GUI that can be accessed over the LAN.

Remote management

The IPBS and IPBL have support for remote setup and configuration over the Internet using a VPN client.

IP administration security

All IP administration is based on secure IP. IPBS and IPBLs are password protected in order to prevent unauthorized access.

IPBS,IPBL, AIWS, and AIWS2 offer a set of default passwords for several user accounts in a factory fresh installation. During installation, you must change the default password for all existing accounts according to the described installation process for each particular device.

Software upgrade

IPBS and IPBL support:

- Software download using the web interface.
- Software upgrade using the web interface.
- Automatic firmware update from a web server or a TFTP server.

VoIP signalling protocols

The protocol used for VoIP signalling is H.323 XMobile which is a proprietary extension of H.323. H.323 was the first standard and is in fact a set of protocols designed to enable multimedia traffic in single LANs. One protocol of many in the set of protocols defined in H.323, is H.450, which is a series of protocols which defines Supplementary Services for H.323.

H.323

The International Telecommunications Union (ITU) developed H.323 from a telecommunications perspective. Ratified in 1996, H.323 has become a common choice for interoperability among VoIP equipment. H.323 is a standard that provides specifications for computers, equipment, and services for multimedia communication over networks that do not provide guaranteed QoS.

H.323 equipment can carry real-time video, audio, and data, or any combination of these elements. The H.323 standard includes H.225, H.245, and the IETF protocols RTP and RTCP, with additional protocols for call signalling and data and audiovisual communications.

Benefits of using H.323 products and services:

- Products and services developed by multiple manufacturers under the H.323 standard can interoperate without platform limitations. H.323 conferencing clients, bridges, servers, and gateways support this interoperability.
- H.323 provides multiple audio and video codecs that format data according to the requirements of various networks, using different bit rates, delays, and quality options. Users can choose the codecs that best support their computer and network selections.

H.323 XMobile

The protocol between the IP-PBX and the Master IPBS is based on H.323 with some minor differences called XMobile, such as:

- No need to register the DECT Wireless Terminal with the Gatekeeper. No RAS procedure necessary.
- Shared trunk between the IP-PBX and the Master IPBS where all telephony signalling is going

QSIG

- QSIG is a standardised signalling protocol, that is mainly used for signaling between traditional PBXs. This allows interoperability between communications platforms provided by different vendors.

- QSIG has two layers, called BC (basic call) and (GF) generic function. QSIG BC describes how to set up calls between PBXs. QSIG GF provides supplementary services for large-scale corporate, educational, and government networks, such as line identification, call intrusion and call forwarding. Thus for a large or very distributed company that requires multiple PBXs, users can receive the same services across the network and be unaware of the switch that their telephone is connected to. This greatly eases the problems of management of large networks.

IP-DECT planning and deploying

Each unit of IP-DECT provides radio access within a pre-defined area called a cell. To enable seamless handover for the mobile devices, cell planning is important when deploying the IP-DECT System. See the documentation from the DECT supplier if you are using a 3rd party DECT system.

Avaya IP-DECT system components

The Avaya IP-DECT system is created using Avaya developed products, as well as third-party products. This section gives a brief description of the components needed.

DECT cordless handsets

The DECT Cordless Handsets are available in a number of versions. From handsets with basic functionality suitable in office environments to handsets suitable in environments with needs like supervision, alarm functions and EX-classification.

The IP-DECT system has support for all DECT Cordless Handsets. No changes of the handset is needed.

Handset installation on the DECT System/I55 System

Note:

The handset to be installed must not have any previous valid registrations. If it has a valid registration, unsubscribe the handset

Installation of Handsets

Subscribing a handset

1. Assign an extension number for the handset in the DECT/I55 system. See the corresponding manual for the DECT/I55 system.
2. Subscribe the handset towards the DECT/I55 system. The subscription procedure is described in the handset's User Manual.

During the subscription procedure, the handset's User ID will automatically be set to the same as the extension number. The User ID is used to identify the handset when it is connected to PDM/Device Manager and will be visible in the Number column.

Tip:

The User ID can be viewed in the handset by navigating to the menu as follows: **Admin menu** > **Device info** > **User ID**

Handset Replacement with Device Manager in DECT/I55 System

Note:

The replacement handset must not have any previous valid registrations. If it has a valid registration, unsubscribe the handset.

1. Unsubscribe the old handset. If the unsubscribtion cannot be performed in the handset, unsubscribe the handset via the DECT/I55 interface. See the corresponding documentation for your system.
2. Subscribe the new handset with the same extension number as the old handset. The subscription procedure is described in the handset's User Manual. During the subscription procedure, the handset's User ID will automatically be set to be the same as the extension number.

Tip:

The User ID can be viewed in the handset by navigating to the menu as follows: **Admin menu** > **Device info** > **User ID**.

3. Insert the handset into a desktop charger or charging rack connected to Device Manager (not needed if an over the air connection is used). Navigate to the Numbers tab in the Device Manager.
   The new handset now has the same User ID as the old handset. It will automatically be synchronized and data and parameter settings from the old handset will be transferred to the new handset.
   The synchronization will take a while if the Contacts in the original handset contains a large number of contacts.

IPBS

The IP Base Station or the IPBS is available in two versions: IPBS1 and IPBS2. The IPBS has eight channels for speech and messaging and one channel which is reserved for broadcast messages. For more information on the IPBS, see IP-DECT System on page 10.

Compact IPBS

The Compact IPBS is identical to IPBS (see *IPBS*), but has only four channels used for speech. A basic administration interface is used for the Compact IPBS. For more information on the simplified interface, see *Installation and Operation Manual, IP-DECT Base Station and IP-DECT Gateway for Avaya, TD 92604EN*.

IPBL

You must use the IPBL (IP-DECT Gateway) if you plan to use legacy base stations (RFPs) with the IP-DECT system. Up to 16 RFPs can be connected to the IPBL. The IPBL has a total of 40 channels of which eight channels are used for each RFP for speech, message, and alarm. Two channels are reserved for messaging and alarm.

You can connect he following legacy DECT base stations to the IPBL in order to use them in an IP-DECT system:

- BS330-9131 with Internal antenna (EU)
- BS330-9134 with Internal antennas (US)
- BS340-9131 with External antenna (EU)
- DB1-C3 and DB1-C4

RFP

The following TDM-DECT base stations can be connected to the IPBL in order to use them in an IP-DECT system:

- BS330-9131 (EU) with Internal antenna
- BS330-9134 (US) with Internal antenna
- BS340-9131 with External antenna
- DB1-C3 (EU and US) with Internal antenna

- DB1-C4 (EU) with External antenna

IP-PBX

The IP-PBX is a private branch exchange that switches calls between VoIP users on local lines while allowing all users to share a certain number of external phone lines. The typical IP-PBX can also switch calls between a VoIP user and a traditional telephone user.

With a conventional PBX, separate networks are necessary for voice and data communications. One of the main advantages of an IP-PBX is the fact that it employs converged data and voice networks. This means that Internet access, as well as VoIP communications and traditional telephone communications, are all possible using a single line to each user. This provides flexibility as an enterprise grows, and can also reduce long-term operation and maintenance costs. Like a traditional PBX, an IP-PBX is owned by the enterprise.

Communication Manager

Avaya Aura(R) Communication Manager is a private branch exchange that transfers calls between VoIP users on local lines while all users share a certain number of external phone lines. Communication Manager can also move calls between a VoIP user and a traditional telephone user.

With Communication Manager, you do not require a separate network for voice and data communications. CM employs converged data and voice networks. Converged networks make Internet access, VoIP communications, and traditional telephone communications possible using a single line to each user.

Avaya In-Building Wireless Server (AIWS or AIWS2)

Avaya In-Building Wireless Server (AIWS) offers wireless services in IP-DECT such as SMS from cordless telephone to a cordless telephone, sending text messages from a web browser and access to a central phonebook. AIWS is also a messaging and alarm gateway between open messaging communication protocols and IP-DECT telephones.

The AIWS2 is based on Linux and runs on a highly reliable solid state appliance.

Available functionality (depending on activated licenses) are as follows:

- Sending messages handset to handset
- Access to built-in central phonebook
- Access to external directory over LDAP
- RS232-based messaging protocols

- IP-based messaging and alarm protocols
- NTP support (master and radio)
- Configuration fully web based
- Remote access over modem/PPP

Appendix A: System capacity

Max No. of Devices in an Avaya IP-DECT System

Cordless telephones	2000
IP-DECt Gateways (IPBLs)	100
IP-DECT Base Stations (IPBSs):	1000
Base Stations BS330/BS340	16 connected to an IPBL that is, total 1600 in an IP-DECT system
Compact IP-DECT Base Stations	5

Traffic Capacity

Speech calls:	10000/hour
SMS:	10000/hour

Speech Channels on each device

IP-DECT Base Station (IPBS)	8 simultaneous calls
IP-DECT Gateways (IPBLs)	40 simultaneous calls
Base Stations BS330/ BS340	8 simultaneous calls
Compact IP-DECT Base Stations	4 simultaneous calls

Appendix A: System capacity

Appendix B: Messaging capacity

Alarm Messages from DECT handset

Time until received in the Unite system:	*~ 2 sec*

No Highspeed Data to DECT handset 3720

Incoming Messages to DECT handset 3720

The time for a message to be delivered differ dependent on how many characters the message contain and if it is delivered to a single handset or a group of handsets.

Number of message characters:	*No of DECT handsets:*	*For **IPBL**: Time in seconds until **one handset** is paged:*	*For **IPBS**: Time in seconds until **one handset** is paged:*
20 characters	1	*~ 4*	*~ 3*
120 characters	1	*~ 5*	*~ 3*
240 characters	1	*~ 6*	*~ 4*
500 characters	1	*~ 9*	*~ 7*

Number of message characters:	*No of DECT handsets:*	*For **IPBL**: Time in seconds until **all handsets** are paged:*	*For **IPBS**: Time in seconds until **all handsets** are paged:*
20 characters	1 10 30 100	*~ 4* *~ 6* *~ 14* *~ 43*	*~ 3* *~ 4* *~ 11* *~ 32*
120 characters	1 10 30 100	~ 5 *~ 7* *~ 17* *~ 56*	~ 3 *~ 4* *~ 13* *~ 39*

Incoming Messages to DECT handset 3725/3745

The time for a message to be delivered differ dependent on how many characters the message contain and if it is delivered to a single handset or a group of handsets.

Number of message characters:	*No of DECT handsets:*	*For **IPBL**: Time in seconds until **one handset** is paged:*	*For **IPBS**: Time in seconds until **one handset** is paged:*
20 characters	1	*~ 4*	*~ 3*
120 characters	1	*~ 5*	*~ 3*
240 characters	1	*~ 6*	*~ 3*
500 characters	1	*~ 9*	*~ 3*

Number of message characters:	*No of DECT handsets:*	*For **IPBL**: Time in seconds until **all handsets** are paged:*	*For **IPBS**: Time in seconds until **all handsets** are paged:*
20 characters	1 10 30 100	*~ 4* *~ 6* *~ 14* *~ 43*	*~ 3* *~ 3* *~ 6* *~ 23*
120 characters	1 10 30 100	~ 5 *~ 7* *~ 17* *~ 56*	~ 3 *~ 3* *~ 9* *~ 27*