

SYSTEM DESCRIPTION

Mitel IP-DECT System

Abbreviations and Glossary

CKI	Cipher Key Index. Used for Early Encryption and is stored both in the handset and in the system. The CKI uniquely identifies a DefCK.
Cover Radius	The radius of the circle (circular radiation patterns of the base station antennas are assumed), around a particular base station, in which portable parts can communicate with that base station.
DECT	Digital Enhanced Cordless Telecommunications Global standard for cordless telephony.
DefCK	Default Cipher Key Used for Early Encryption and is stored both in the handset and in the system.
Device	A device can be an IPBS, IPBL, or IPVM.
External Handover	The procedure of moving an active call from one IPBS to another.
Handover Domain	Handover domain defines the Radios to which external handover is allowed. Handover domain is defined by the System ID.
IPBL	IP-DECT Gateway
IPVM	IP-DECT Virtual Appliance
WSM3	Wireless Service Messaging gateway WSM3 is a gateway handling communication interfaces for DECT and VoWiFi systems and other basic messaging services, such as web messaging and messaging handset to handset (SMS). The WSM3 is installed on a reliable solid state hardware.
CPDM3	Central Portable Device Manager Unite module that enables messaging to and from the connected cordless telephone system.
IP	Internet Protocol Global standard that specifies the format of datagrams and the addressing scheme. This is the principal communications protocol in the Internet Protocol suite.
IPBS	IP-DECT Base Station or IPBS Base Station.
ISDN	Integrated Services Digital Network
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
Master ID	Master ID must be unique for each Master in a system. The Standby Master must have the same id as the Master.
MCD	Mitel Communications Director

SYSTEM DESCRIPTION

Mitel IP-DECT System

PBX	Private Branch Exchange A telephone system within an enterprise that switches calls between local lines, and allows all users to share a certain number of external lines. Also referred to as Call Manager.
PSTN	Public Switched Telephone Network.
QoS	Quality of Service Defines to what extent transmission rates, error rates, and so on are guaranteed in advance.
RAS	Registration, Admission, Status (H.323)
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.
RFPI	Radio Fixed Part Identity The broadcast identity which uniquely identifies a RFP geographically.
Roaming	The procedure of moving the handset from one IPBS/IPBL to another and still be able to place outgoing and receive incoming calls.
SIP	Session Initiation Protocol SIP is a signaling protocol used for initiating, maintaining, and terminating real-time sessions that include voice, video, and messaging applications. SIP is used for applications of Internet telephony for voice and video calls, in private IP telephone systems, in instant messaging over IP networks, and in mobile phones calling over LTE, Voice over LTE (VoLTE).
SMS	Short Message Service. Text messages sent over the cellular network.
Sync Coverage	A sync coverage is the air sync coverage areas for all base stations connected to the same sync Master.
Sync Domain	Sync domain defines the Radios to which automatic synchronization is allowed. Sync domain is defined by the System ID.
System ID	System ID in the PARI Master defines the sync domain and handover domain. Within the coverage area, the System ID must be unique from other IP-DECT systems.
Unite	Generic term for messaging system that unites different systems.
Virtual Appliance	A pre-built, pre-configured and ready-to-run software application that is packaged with the operating system inside a virtual machine.
VoIP	Voice over IP

Contents

1 Introduction	1
2 IP-DECT System Overview	2
2.1 Supported Standards.....	3
2.2 System Size	3
2.3 System Components	3
2.3.1 Handsets.....	3
2.3.2 IPBS	4
2.3.3 IP-DECT Virtual Master (IPVM)	4
2.3.4 IPBL.....	4
2.3.5 RFP	4
2.3.6 IP-PBX	4
2.3.7 Wireless Service and Message Gateway (WSM3)	4
2.3.8 Central Portable Device Manager (CPDM3)	5
2.4 LAN and WAN.....	5
3 IP-DECT System	6
3.1 Software Components	6
3.1.1 Radio	6
3.1.2 Master	6
3.1.3 PARI Master	7
3.1.4 Mobility Master	7
3.1.5 Crypto Master.....	7
3.2 Enhanced DECT Security	7
3.2.1 Early Encryption.....	7
3.2.2 Re-keying.....	7
3.2.3 Subscription Requirements	8
3.3 Wideband Audio	8
3.4 System Layout	8
3.4.1 One Master Systems	8
3.4.2 Multiple Master Systems	10
3.4.3 Multiple Mobility Master Systems.....	13
3.4.4 One Master Systems with Enhanced DECT Security	15
3.4.5 Multiple Master Systems with Enhanced DECT Security	16
3.4.6 Multiple Mobility Master Systems with Enhanced DECT Security	16
3.5 Standby Devices	17
3.6 Mirror Devices	18
3.6.1 Description of Mirror Mode	18
3.6.2 Benefits With Mirror Mode Compared to Standby Mode	18
3.7 Call Localization	19
3.8 Messaging in Multiple Master Systems	20
3.9 Broadcast Messaging in Multiple Master Systems.....	21
3.10 Hot Desking	21
3.10.1 Log in	21
3.10.2 Log out	21
3.11 Device Management	22
3.12 Fault Reporting	22
3.13 Load Balancing	22
3.14 Synchronization	23
3.14.1 Air Synchronization	23
3.14.2 Ring Synchronization.....	23

3.15	Channel Distribution	24
3.15.1	DB1/BS3x0 Connected to the IPBL.....	24
3.15.2	IPBS	24
3.16	System Management.....	25
3.16.1	On Site Management	25
3.16.2	Remote Management.....	25
3.16.3	IP Administration Security	25
3.16.4	Software Upgrade.....	25
4	VoIP Signalling Protocols	26
4.1	H.323.....	26
4.1.1	H.450 Supplementary Services for H.323.....	26
4.2	Session Initiation Protocol (SIP).....	26
4.2.1	IP-DECT System Internal Communication	26
5	Related Documents	28
6	Document History	29
Appendix A	Messaging Capacity	31
A.1	Alarm Messages from DECT handset	31
A.2	Data to DECT handset	31
Appendix B	Performance Considerations.....	32
B.1	When to Switch off the Base Station Radio	32
B.2	System Capacity	32

1 Introduction

The IP-DECT system supports the standard which gives a full integration of messaging and voice functions. The IP-DECT system can be integrated with external applications such as different alarm systems, networks and e-mail. This gives features such as: messages to handset, alarm from handset, message acknowledgement, and absent handling.

About this Document

This document gives a general description of the IP-DECT system, an IP based cordless telephony and messaging system for connection to private telephone exchanges.

2 IP-DECT System Overview

The IP-DECT system is modular. It is designed for small installations as well as large multi-site installations with remote offices.

The IP-DECT system is designed to enable voice traffic, messaging and alarm handling between handsets within an enterprise LAN. The IP-DECT system supports roaming and handover between all IPBSs and IPBLs in the system.

The IP-DECT system is built up by the following components:

- Handsets
- IP-DECT Base Station (IPBS) or IP-DECT Base Station v2 Compact
- IP-DECT Gateway (IPBL)
- IP-DECT Virtual Master (IPVM)
- Radio Fixed Part (RFP)
- IP-PBX
- Wireless Services and Message gateway (WSM3)
- Central Portable Device Manager (CPDM3)

Figure 1. IP-DECT System Overview with CPDM3

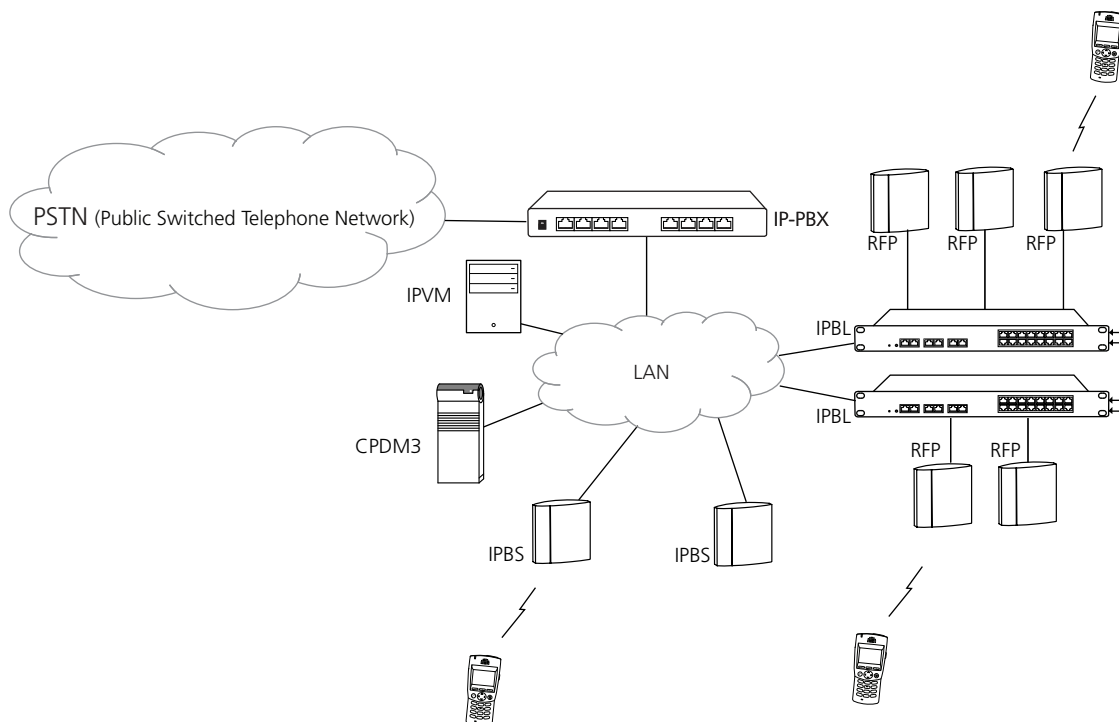
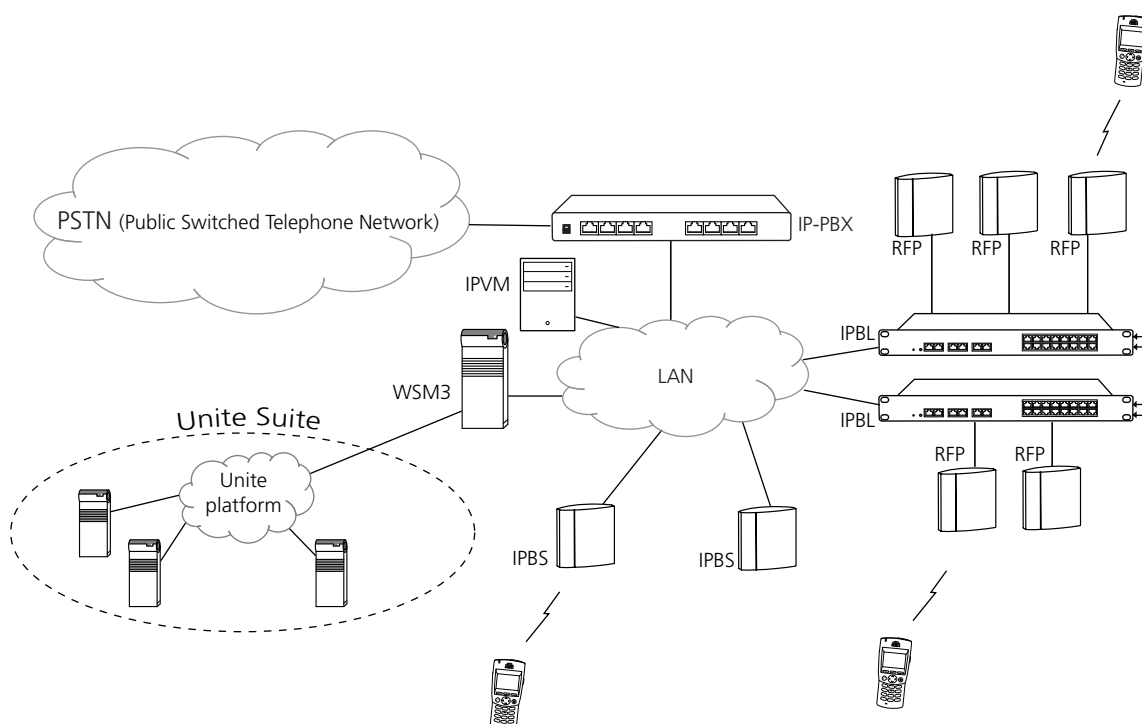


Figure 2. IP-DECT System Overview with WSM3



2.1 Supported Standards

- H.323
- SIP
- G.711 (a-law and μ -law)
- G.722.2 (Wideband audio)
- G.729-A/AB

2.2 System Size

The IP-DECT system is very modular and scalable. Systems for more than 100 000 users can be built.

2.3 System Components

2.3.1 Handsets

The Mitel IP-DECT system has support for the following Mitel DECT handsets:

- 5604
- 5607
- 5613
- 5614
- 5617
- 5619

No changes of these handsets are needed.

2.3.2 IPBS

IPBS contains all the functionality needed for a complete IP-DECT system, including a Radio module. It can be configured as a PARI Master, Mobility Master, Crypto Master, Kerberos Server, and so on.



IPBS1 can only be used as a radio from software version 9.1.X.

For more information about IPBS, see [3.15.2 IPBS, page 24](#).

2.3.3 IP-DECT Virtual Master (IPVM)

The IPVM is a virtual appliance that is compatible with VMware ESXi hypervisor. The IPVM offers the same functionality as the other IP-DECT devices except it does not have a Radio module. This means that the IPVM can work as a PARI Master, Mobility Master, Crypto Master, Kerberos Server, and so on. There are some functionality benefits by using VMware. Compared to IPBS and IPBL, the IPVM runs on a server hardware (host) which means there are more performance and memory available which allows for up to 4000 users on one IPVM. The number of possible users on one IPVM is license controlled.

VMware also comes with built in redundancy solutions like VMware High Availability which provides high availability for virtual machines by pooling them and the hosts they reside on into a cluster. Hosts in the cluster are monitored and in the event of a failure, the virtual machines on a failed host are restarted on alternate hosts.

2.3.4 IPBL

Up to 16 RFPs can be connected to the IPBL. The IPBL has eight channels for each RFP used for speech, messages and alarm. Totally the IPBL has 40 speech channels.

The IPBL will assign speech resources according to first come, first served. If all 40 speech resources are allocated, the RFPs connected to that IPBL will transmit the "Busy For Speech" flag, allowing handsets in need of establishing a speech call to roam to a different base station if available.

For more information about IPBL, see [3.15.1 DB1/BS3x0 Connected to the IPBL, page 24](#).

2.3.5 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

2.3.6 IP-PBX

The IP-DECT system is connected to the IP-PBX with standardized H.323 or SIP protocol.

2.3.7 Wireless Service and Message Gateway (WSM3)

The WSM3 contains a Device Manager which supports parameter and software download to portable devices. For more information, see *Installation and Operation Manual, WSM3, TD 92794EN*.

2.3.8 Central Portable Device Manager (CPDM3)

The CPDM3 contains support for messaging and alarm.

The CPDM3 contains also a Device Manager which supports parameter and software download to portable devices.

All features are license dependent.

2.4 LAN and WAN

There are several vendors providing components needed to deploy a LAN/WAN. In order to achieve optimal performance for IP-DECT the following is recommended:

- Quality of Service (QoS)
- The infrastructure should be connected to a switched network. (i.e hubs or repeaters should be avoided)
- Depending on network size, a backbone of at least 100 Mbps should be used.

3 IP-DECT System

The IP-DECT system is connected via one or several IP-PBXs to the PSTN. For messaging purposes the IP-DECT system can be connected to one or several WSM3 / CPDM3, see [3.8 Messaging in Multiple Master Systems, page 20](#).

The IP-DECT system has a modular structure that can be modelled as a number of network entities. The network entities defined are:

- the entity offering the H323-DECT gateway functionality will be referred to as **Radio**
- the entity acting as the proxy for the IP terminated DECT handsets within the coverage of the associated Radios will be referred to as **Master**
- the entity offering support for distribution of the DECT identity RFPI will be referred to as **PARI Master**
- the entity offering support for finding home location information will be referred to as **Mobility Master**
- the entity offering support for distribution of the CKI identity will be referred to as **Crypto Master**

3.1 Software Components

A Multiple Master system consists of the following entities which are software components which can be activated in a device:

- Radio (cannot be activated in an IPVM)
- Master
- PARI Master
- Mobility Master
- Crypto Master

For information on how to set these software components, see *Installation and Operation Manual for IP-DECT Base Station, TD 92682EN*.

3.1.1 Radio

The Radio is a software interface between DECT and H.323.

Location registration requests that cannot be resolved locally are forwarded to the Master acting as PARI Master. If the handset cannot be resolved locally in the PARI Master, the Mobility Master needs to be involved in the process of resolving the home location master, as it has knowledge of all DECT handsets in the system. The RAS channel will be established by the Radio for the first handset assigned to a Master and maintained until the last handset assigned to this Master has left the Radio. Thus, the Radio may have several concurrent RAS channels established to different Masters. Information for authentication of the handset will be sent by the home location master to the Radio.

3.1.2 Master

This software component is responsible for the communication to the IP-PBX. Translation between the internal H.323 to the DECT Radios and the external protocol (H.323 / SIP) to the IP-PBX is done by this component.

A Master is responsible for the DECT handsets that are assigned to it. When the Master has been notified about that a handset is within coverage it makes a registration to the IP-PBX. This registration is maintained by the Master until a notification is received that the handsets access rights has been terminated or the handset has detached. At startup the registration is done only for the handsets that notify themselves with the location registration message.

The Master will establish a RAS channel to any associated Mobility Master at startup. All DECT handsets in the HDB are sent to the Mobility Master, to be used in the home location master resolution process.

The Master is also responsible for the mapping of keypad information to supplementary PBX features. Some features are handled locally by the Master and some are communicated to the IP-PBX.

3.1.3 PARI Master

This software component is responsible for assigning RFPIs, being part of the same external handover domain, to the Radios associated. A Radio will always be given the same RFPI, based on the RFPI-MAC address association.

3.1.4 Mobility Master

The Mobility Master will establish a RAS channel to any associated Mobility Masters, for which roaming agreements have been configured. This ensures scalability to a world wide level by distributing the home location master information to local Radios and remote Mobility Masters in the system.

In an Enhanced DECT Security system, the Mobility Master will establish a RAS channel to the Crypto Master at startup. To guarantee that the assigned CKIs are system unique, all CKIs for the DECT handsets supporting Enhanced DECT Security are sent to the Crypto Master.

3.1.5 Crypto Master

This software component is responsible for assigning CKIs. The Crypto Master keeps track of all CKIs and allocates a new unique CKI whenever subscribing a new handset that supports Enhanced DECT Security in the system and frees values when unsubscribing. For more information about Enhanced DECT Security, see [3.2 Enhanced DECT Security, page 7](#).

3.2 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.

3.2.1 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.

3.2.2 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.

3.2.3 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 device 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.

3.3 Wideband Audio

Wideband audio is high definition voice quality for telephony audio. It extends the frequency range of audio signals, resulting in higher quality speech.

Wideband Audio media is supported by IPBS2 (software version 9.1.X or later) and IPBS3. The support for Wideband Audio is also dependent on what model of handset that is used and the type of PBX that is used in the system and if handsets from other manufacturers supports the same wideband coder. For more information, see the data sheet for the handset and the PBX test reports for interoperability.

If the handset supports wideband audio, when moving with the handset during a wideband audio call and a handover to an IPBS1 occurs, a renegotiation to narrowband is done. No renegotiation can then be done back to wideband. Once a call is narrowband it will remain so until the call is terminated.

3.4 System Layout

This section describes examples of different system layout sizes:

- One Master systems, see [3.4.1 One Master Systems, page 8](#).
- Multiple Master systems, see [3.4.2 Multiple Master Systems, page 10](#).
- Multiple Mobility Master systems, see [3.4.3 Multiple Mobility Master Systems, page 13](#).
- One Master systems with Enhanced DECT Security, see [3.4.4 One Master Systems with Enhanced DECT Security, page 15](#).
- Multiple Master systems with Enhanced DECT Security, see [3.4.5 Multiple Master Systems with Enhanced DECT Security, page 16](#).
- Multiple Mobility Master systems with Enhanced DECT Security, see [3.4.6 Multiple Mobility Master Systems with Enhanced DECT Security, page 16](#).

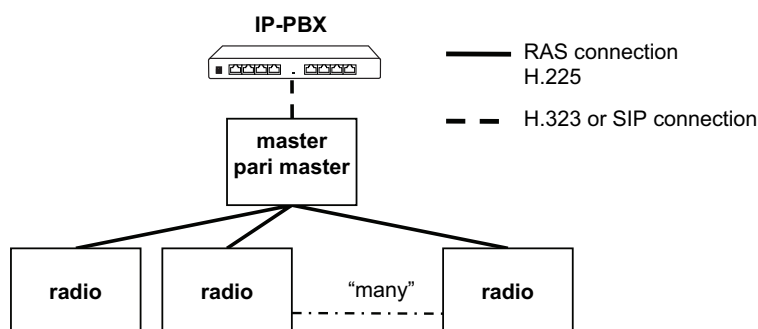
For details regarding the performance considerations and capacity of different systems, see [Appendix B Performance Considerations, page 32](#).

3.4.1 One Master Systems

Single Site Installation

The layout in [Figure 3. Example of a Single Site Installation, page 9](#) can be used for customers with a single site installation. The lines displayed between the IP-PBX, the Master, and the Radios in [Figure 3. Example of a Single Site Installation, page 9](#) indicate the logical connection between the software modules.

Figure 3. Example of a Single Site Installation



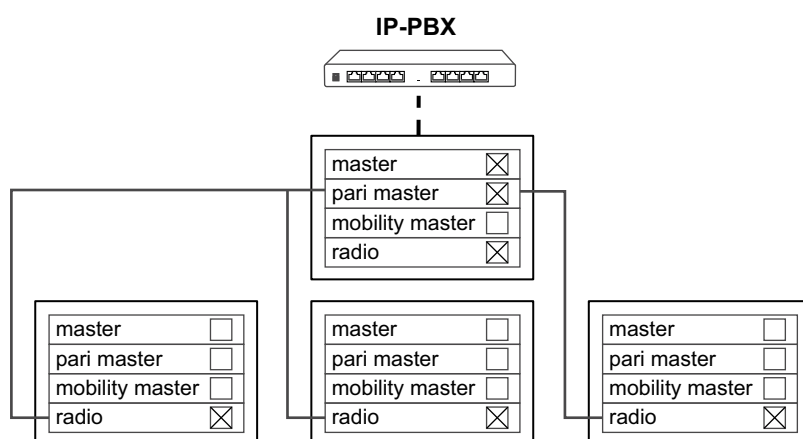
The [Figure 4. Distribution of Software Components, page 9](#) below shows the software components. A device includes all software components as described in [3.1 Software Components, page 6](#).



Radio is not included in IPVM.

In a single site installation, one of the devices will have an active Master and PARI Master software component, and optionally have an active Radio. All others will only have the software component Radio active.

Figure 4. Distribution of Software Components



Multiple Site Installation

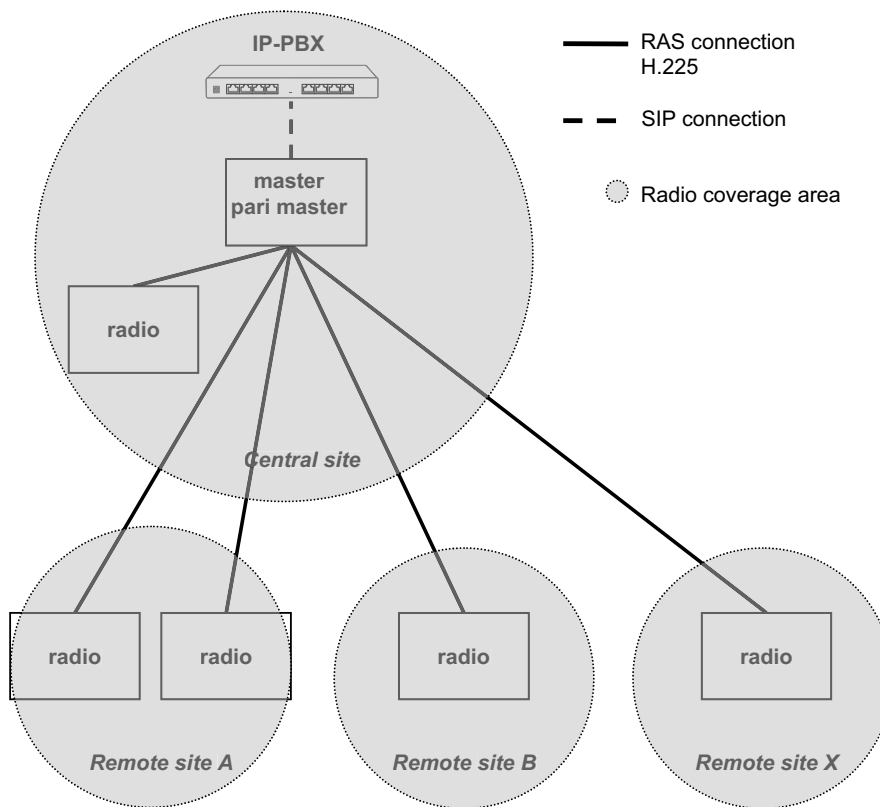
See [Figure 5. Multiple Site Installation, page 10](#).

This layout is chosen if there is no need for local functionality in remote sites.

The same layout as in a single site can also be used for customers with an installation on several sites. The sites may have one or several devices at each site. The IP-PBX and the PARI Master and Master are centrally located.

With this solution the handset will be able to roam to a different site and it will be possible to receive incoming and make outgoing calls.

Figure 5. Multiple Site Installation



3.4.2 Multiple Master Systems

Single Site Installation

See [Figure 6. Single Site Installation, page 11](#).

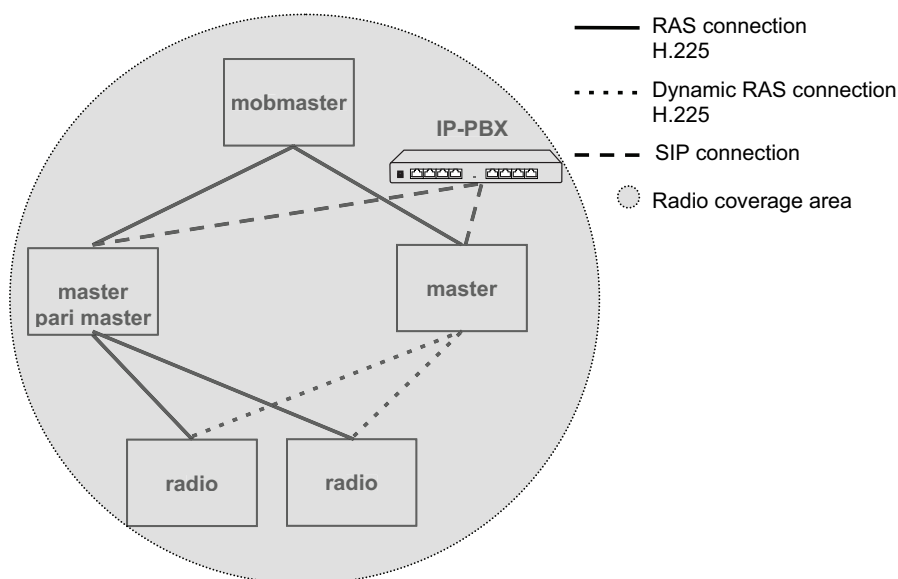
This layout may be used for customers with a large single site installation. Load must be distributed over a number of Masters to be able to cope with the load generated from a large number of handsets. It will be possible to do roaming and handover between all Radios.

The lines displayed between IP-PBX, Mobility Master, Master and Radios are only used to indicate the logical connection between the software modules.

Several Masters are logically connected directly to one or several IP-PBXs.

A Master makes SIP registrations to the IP-PBX for the respective handsets within coverage. After registration of a Master to the IP-PBX for a handset, all in- and outgoing speech calls will be routed directly to this Master.

Figure 6. Single Site Installation



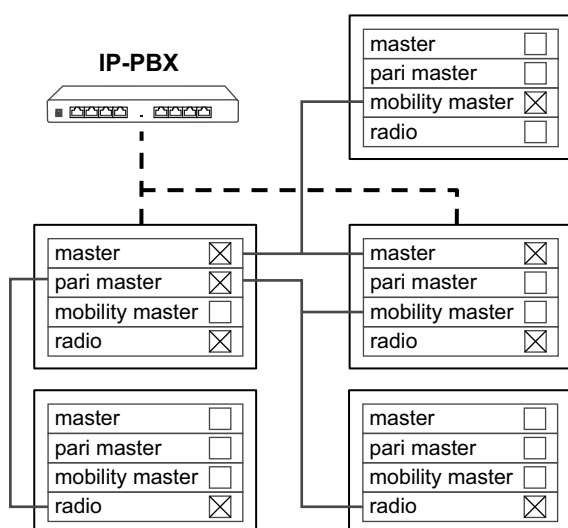
The [Figure 7. Distribution of Software Components](#), page 11 below shows the software components. A device includes all software components as described in [3.1 Software Components](#), page 6.



Radio is not included in IPVM.

In a single site installation, one or several of the devices will have an active Master software component, only one of the Masters will have an active PARI Master, and one device will have an active Mobility Master software component, and optionally have an active Radio. All others will only have the software component Radio active.

Figure 7. Distribution of Software Components



Multiple Site Installation

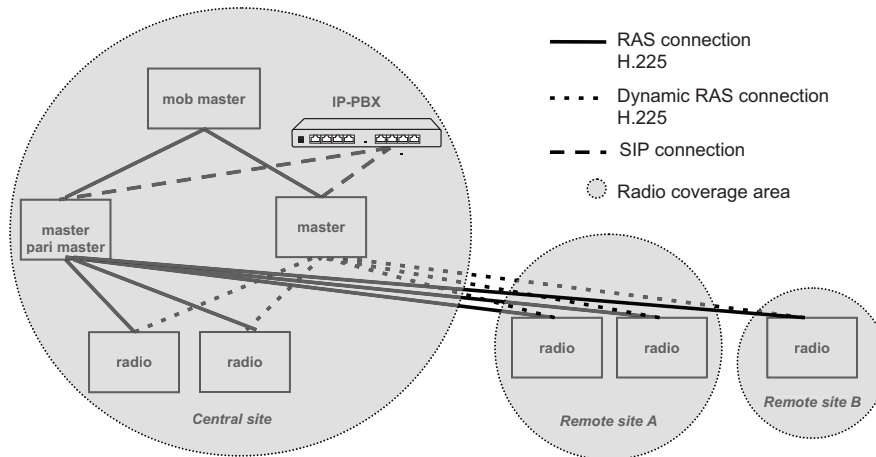
See [Figure 8. Multiple Site Installation with Central Master](#), page 12.

This layout is chosen if there is no need for local functionality in remote sites.

The same layout as in a single site can also be used for customers with an installation on several sites. The sites may have one or several base stations at each site. The IP-PBX and the PARI Master and Master are centrally located.

With this solution the handsets will be able to roam to a different site and it will be possible to receive incoming and make outgoing calls.

Figure 8. Multiple Site Installation with Central Master

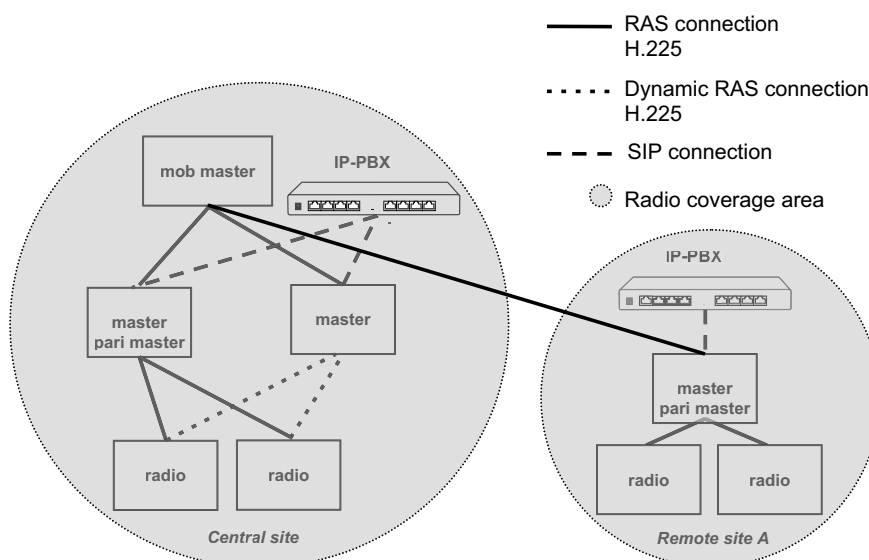


Multiple Site Installation with Local Functionality

See [Figure 9. Multiple Site Installation with Remote Master, page 12](#).

This layout is chosen if there is a need for local functionality in remote sites.

Figure 9. Multiple Site Installation with Remote Master



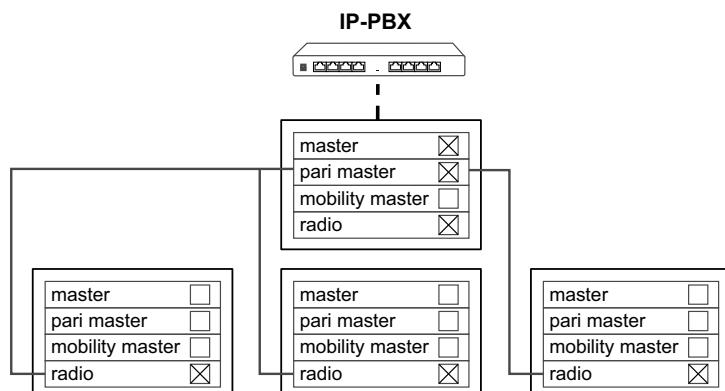
The [Figure 10. Distribution of Software Components in Remote Site A, page 13](#) below shows the software components. A device includes all software components as described in [3.1 Software Components, page 6](#).



Radio is not included in IPVM.

In site A, one of the devices will have an active Master and PARI Master software component, and optionally have an active Radio. All others will only have the software component Radio active, see [Figure 9. Multiple Site Installation with Remote Master, page 12.](#)

Figure 10. Distribution of Software Components in Remote Site A



3.4.3 Multiple Mobility Master Systems

See [Figure 11. Multiple Site Installation, page 14.](#)

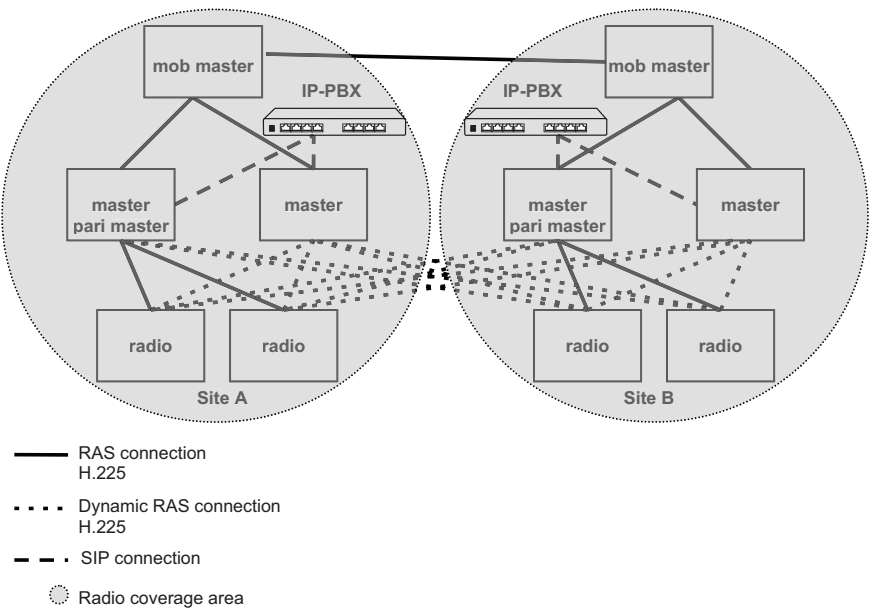
This layout is chosen if there is a need for local functionality in a site with several Masters. This layout may be used for customers with large multiple site installations. Load must be distributed over a number of Masters to be able to cope with the load generated from a large number of handsets in one site. It will be possible to do roaming and handover between all Radios within each site. It will be possible to do roaming to all other sites to which roaming agreements exists and it will be possible to receive incoming and make outgoing calls.

The lines displayed between IP-PBX, Mobility Master, Master and Radios are only used to indicate the logical connection between the software modules.

A system can consist of several Masters where each Master is logically connected to a specific IP-PBX.

A Master dynamically makes SIP registrations to the “home” IP-PBX for each of the handsets within its coverage. After registration of a Master to the IP-PBX for a handset, all in- and outgoing speech calls will be routed directly to this Master.

Figure 11. Multiple Site Installation



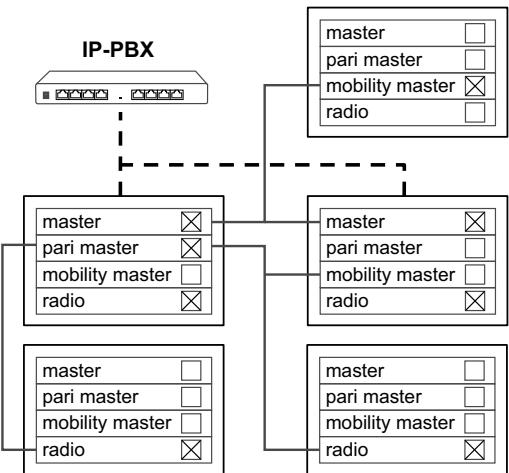
The [Figure 12. Distribution of Software Components in Site A and B, page 14](#) below shows the software components. A device includes all software components as described in [3.1 Software Components, page 6](#).



Radio is not included in IPVM.

In each site one or several of the devices will have an active Master software component, only one of the Masters will have an active PARI Master, and one device will have an active Mobility Master software component, and optionally have an active Radio. All others will only have the software component Radio active.

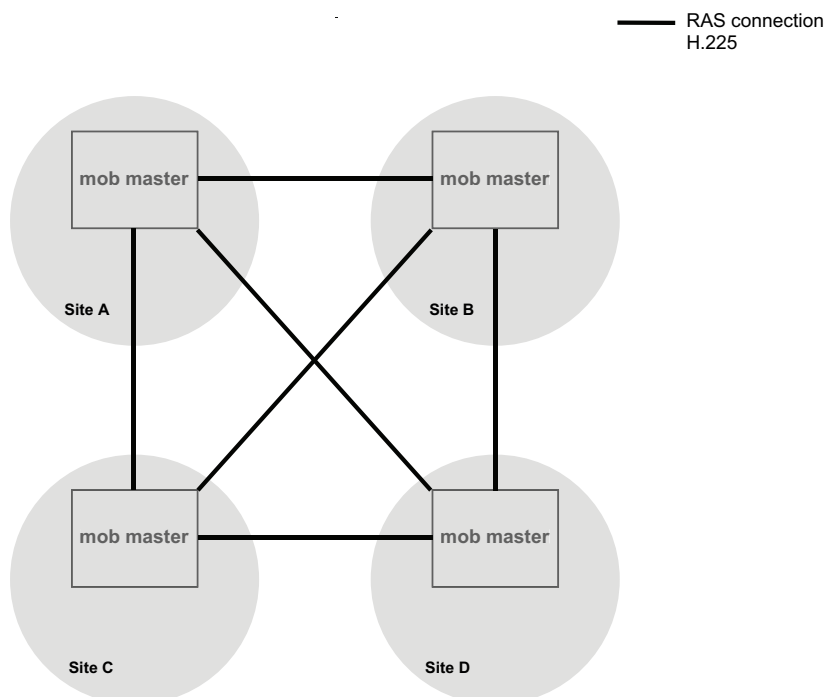
Figure 12. Distribution of Software Components in Site A and B



If more than two mobility masters are used in a system, all mobility masters must be connected to each other. Each connection implies a two-way communication, so, for example, if the mobility master in Site A points to the mobility master in Site B, the opposite direction does not need to be configured again.

[Figure 13. Four Mobility Master Site Installation, page 15](#) shows an example with four mobility masters.

Figure 13. Four Mobility Master Site Installation



The table below shows how four mobility masters, like in [Figure 13. Four Mobility Master Site Installation](#), [page 15](#), should be configured.

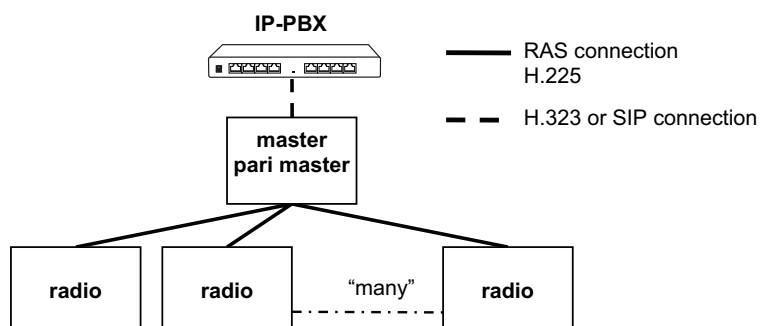
Mobility Master	Configure to other Mobility Masters
Site A	Site B, C, D
Site B	Site C, D
Site C	Site D
Site D	-

3.4.4 One Master Systems with Enhanced DECT Security



The Crypto Master function needed for encryption, will be automatically activated in the Master.

Figure 14. Enhanced DECT Security in a one Master System

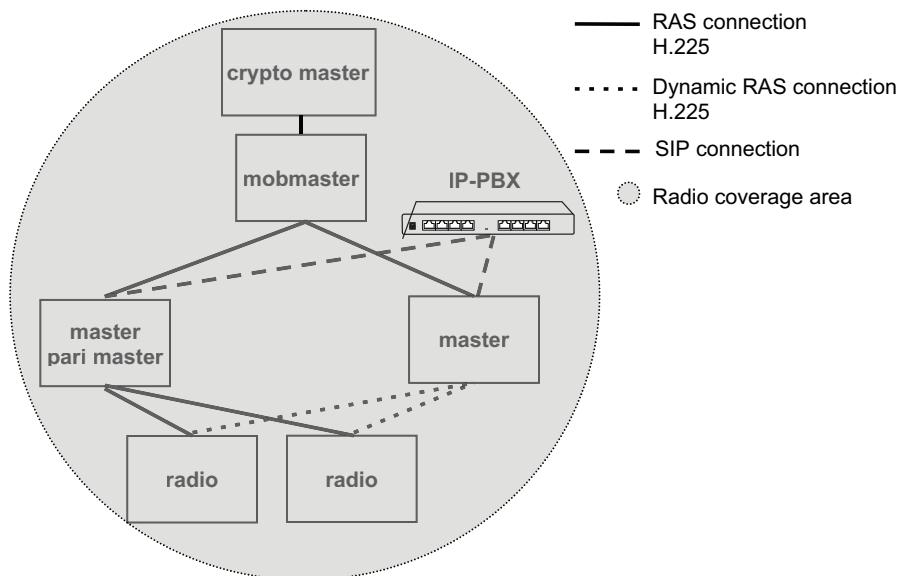


3.4.5 Multiple Master Systems with Enhanced DECT Security

In a system with a Mobility Master, the Mobility Master must be connected to a Crypto Master to enable the early encryption feature.

To guarantee that the assigned CKIs are system unique, all CKIs for the DECT handsets supporting Enhanced DECT Security are sent to the Crypto Master.

Figure 15. Enhanced DECT Security in a Multiple Master System



3.4.6 Multiple Mobility Master Systems with Enhanced DECT Security

In a system with multiple Mobility Masters, they must all be connected to the Crypto Master to enable the early encryption feature.

To guarantee that the assigned CKIs are system unique, all CKIs for the DECT handsets supporting Enhanced DECT Security are sent to the Crypto Master.



There can be only one Crypto Master.

Figure 16. Enhanced DECT Security in a Multiple Mobility Master System

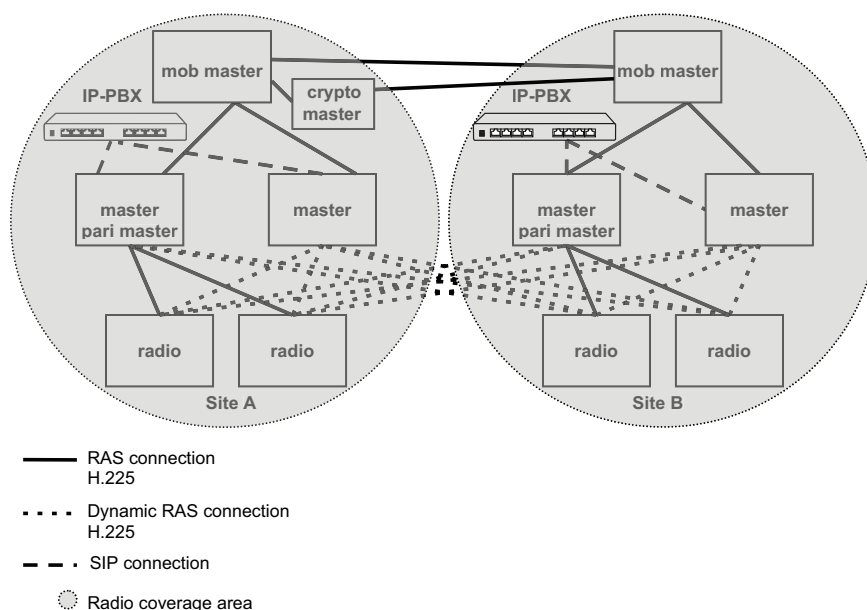
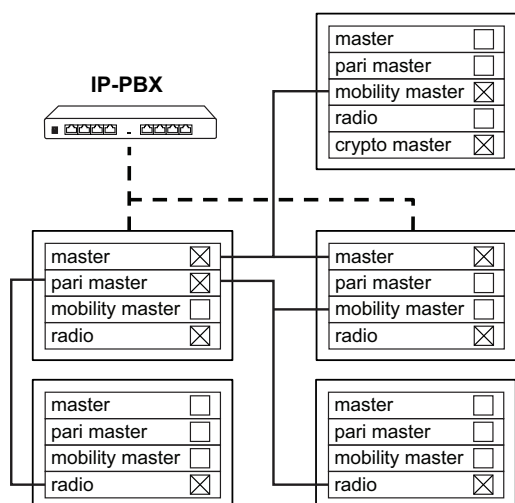


Figure 17. Distribution of software components in site A. Site B is the same but without Crypto Master

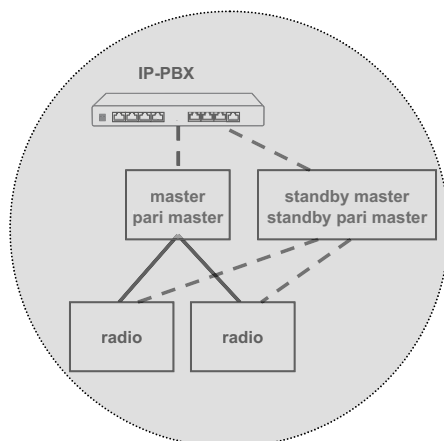


3.5 Standby Devices

It is recommended to have Standby devices in an IP-DECT system. Depending on how the IP-DECT system is configured, standby devices can be Standby Master, Standby PARI Master, Standby Mobility Master. When a Master goes down the corresponding Standby Master takes over.

Read also about Mirror devices, see [3.6 Mirror Devices, page 18](#).

Figure 18. An IP-DECT system with a Standby PARI Master



3.6 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.

3.6.1 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 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.

3.6.2 Benefits With Mirror Mode Compared to Standby Mode



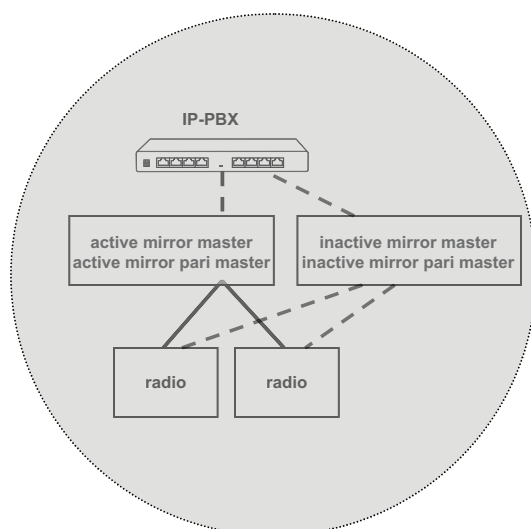
For new installations it is recommended to use the Mirror mode.

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, login/logout hot desk users 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 19. An IP-DECT system with Mirror Masters.



3.7 Call Localization

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

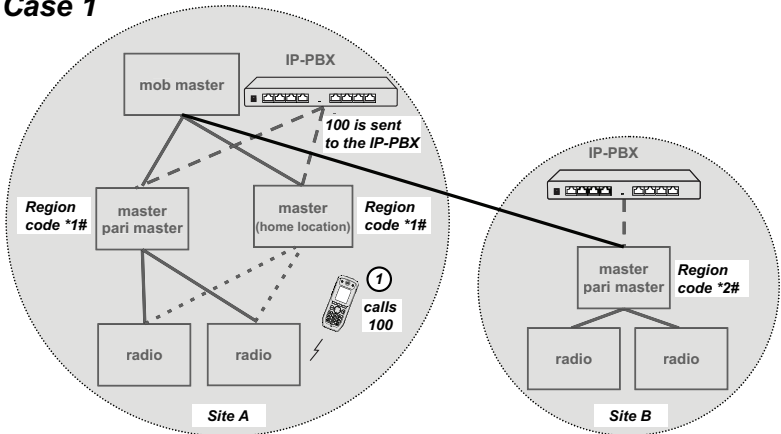
In each Master it is possible to configure a region code which can consist of numbers 0-9, * and #. Each radio will be assigned the same region code as the PARI Master the radio is connected to. When a call is placed, the Master responsible for that user will check if its region code is the same as the region code of the radio where the handset is located. If not, the region code of the radio will be added as a prefix to the dialed number.

Example (see the figure below): There are two sites (a PARI Master in each). Site A with region code *1# and site B with region code *2#.

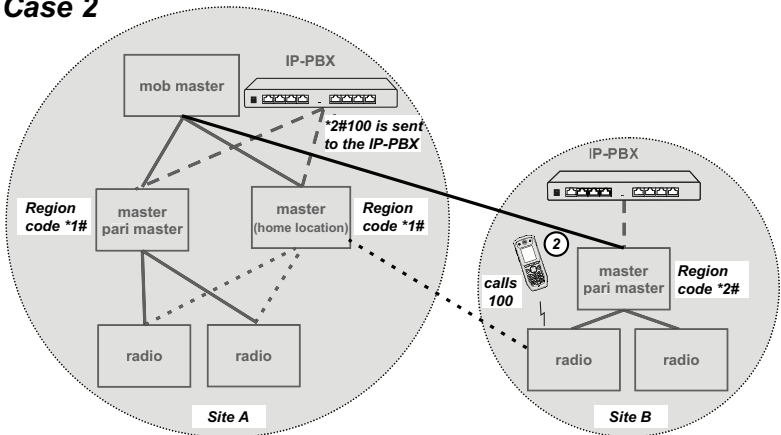
- **Case 1:** A user, configured in the site A Master and located on a radio in site A, calls number 100, then number 100 is sent to the IP-PBX.
- **Case 2:** If the same user moves to site B and calls number 100, then the number *2#100 is sent to the IP-PBX (case 2).

Figure 20. Call Localization using region codes.

Case 1



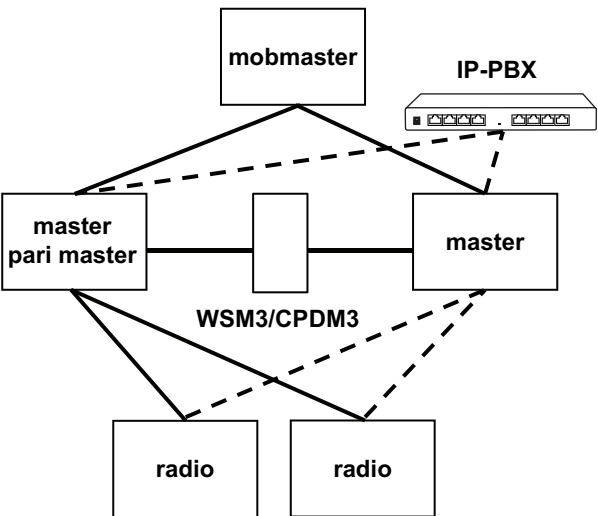
Case 2



3.8 Messaging in Multiple Master Systems

For messaging purposes the IP-DECT system can be connected to one or several WSM3CPDM3. To have messaging functionality for all handsets in a multiple master system, each Master with handsets assigned must have a connection to a WSM3/CPDM3.

Figure 21. Messaging in multiple Master systems



3.9 Broadcast Messaging in Multiple Master Systems

With broadcast messaging it is possible to deliver one message to all users in the system simultaneously. When a message is sent as a broadcast all handsets in the coverage area can receive the message. Broadcast messaging is not 100% proof since the system does not get a delivery receipt from the handsets, but the message is sent three times to increase the reliability of the transmission.

Message with broadcast (e.g. fire alarm) must be sent via a CPDM3/WSM3 connected to the PARI Master since the PARI Master is the only Master that is always connected to all Radios. The message will then be transmitted to all Radios that are connected to the PARI Master. All handsets within the coverage area of the system, will receive the message.

3.10 Hot Desking



This feature requires that hot desking is enabled in the DECT handset. See the DECT handset's Configuration Manual.

Following DECT handsets have support for hot desking:

- 5604
- 5607
- 5613
- 5614
- 5617
- 5619

The feature hot desking allows any hot desk user in the Mitel MCD to use a DECT handset. This feature does not require any administration of users in the IP-DECT system. When a DECT handset is configured for hot desking, the handset can be used by any hot desk user in the system.

3.10.1 Log in

When a user logs in to a hot desk extension with a hot desking handset, following will happen:

1. The user enters the desired hot desk extension and corresponding PIN-code. If the information is correct the user can make and receive calls otherwise the handset returns to logged out state again.
2. The handset's call history lists are updated from the MCD.



If the hot desk extension is already used by another device, for example a desktop phone or a DECT handset, the other device is automatically logged out by the MCD.

3.10.2 Log out

There are three ways to log out from a hot desk extension:

- Place the handset in charger.
- Manually with the handset.
- Automatically by the MCD. See step 3 in [3.10.1 Log in, page 21](#).

When a user logs out with a hot desking handset, the call history lists and message list are deleted.

For information on how to log in to/log out from a hot desk extension with a hot desking handset, see the handset's User Manual.

3.11 Device Management

A Device Manager (included in the CPDM/WSM3) is an application for managing handsets and chargers in wireless systems. The Device Manager can be connected to one or several Masters. It is also possible to have several Device Managers in the IP-DECT system.

The Device Manager supports software downloads to handsets.

The download time differs, and depends on handset model, number of simultaneous downloads, and call traffic load. The download time varies approximately from 20 minutes to several hours.



The download time is slower in IPBL than IPBS.

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.	
CPDM3/WSM3	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.

3.12 Fault Reporting

Faults that occur in the IP-DECT system are shown locally in the faulty device. The faults can be forwarded to a central point (the Master) in the IP-DECT system. The faults can also be forwarded to Messaging system and to an external SNMP manager.

3.13 Load Balancing

Load balancing can be used in an IP-DECT system when the number of handsets exceeds what an IP-PBX is able to register.

When load balancing, the traffic is distributed over several IP-PBXs which can be done in two ways using:

- fixed connections for users on each Master towards multiple IP-PBXs.

- dynamic connection for users on each Master towards IP-PBX network using DNS services.

For more information about load balancing, see *Installation and Operation Manual for IP-DECT Base Station, TD 92682EN*.

3.14 Synchronization

Synchronization within the IP-DECT system is done with the following methods:

- Air synchronization (IPBS)
- Ring synchronization (IPBL)
- Air and ring synchronization combined

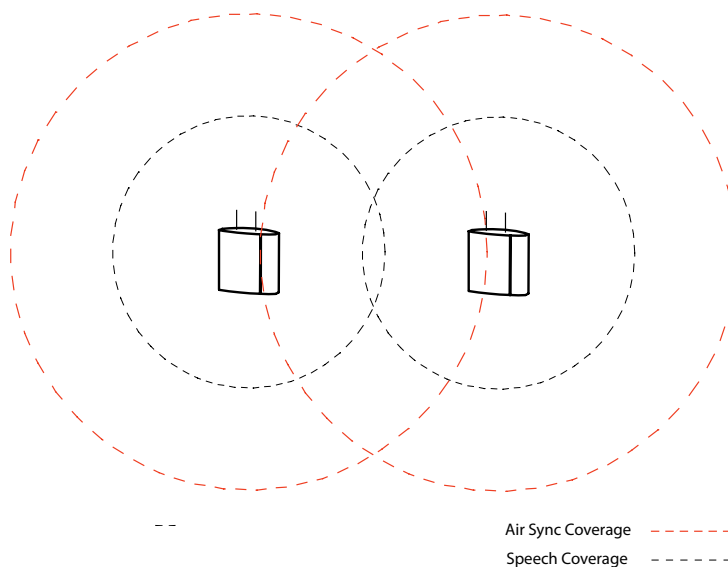
3.14.1 Air Synchronization

If the planned system shall have IPBS base stations, both speech coverage and air sync coverage have to be considered.

Speech coverage: the radius of the circle (circular radiation patterns of the IPBS antennas are assumed for reasons of simplicity), around a particular IPBS, in which portable parts can communicate with that IPBS, see [Figure 22. Air- and speech sync radius, page 23](#).

Sync coverage: the radius of the circle, around a particular IPBS, in which other IPBSs can synchronize with that IPBS with a given synchronization loss probability. This means that the size of the sync radius depends on requested probability of losing synchronization, see [Figure 22. Air- and speech sync radius, page 23](#).

Figure 22. Air- and speech sync radius



005

3.14.2 Ring Synchronization

Each synchronization port sends and receives synchronization signals. Each IPBL has two ports (in/out) for ring synchronization and two ports (in/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.

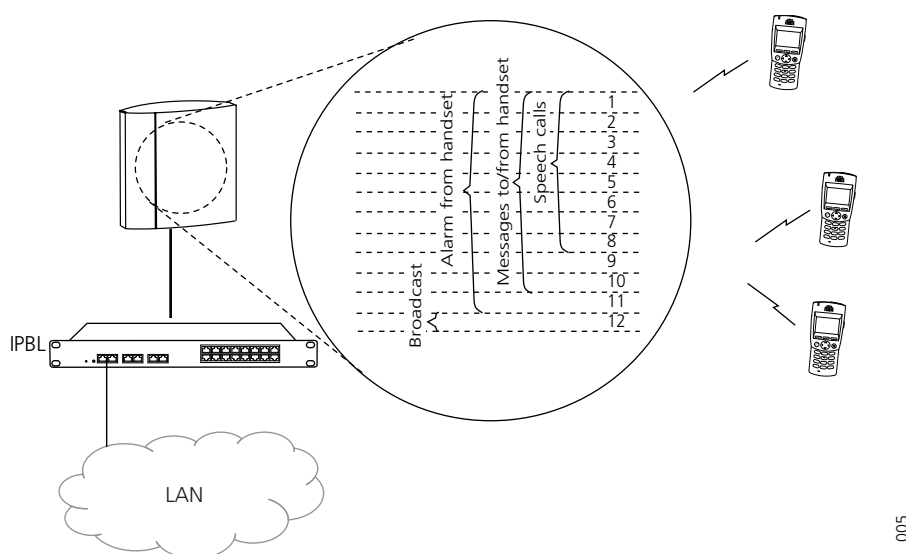
3.15 Channel Distribution

When a handset is used for speech, message, or alarm it always occupies one channel. However, when a handset is used for speech it can send or receive a message or an alarm on the same channel.

3.15.1 DB1/BS3x0 Connected to the IPBL

The DB1/BS3x0 that is connected to the IPBL has in total twelve channels. One channel is reserved for broadcast messages. Alarm from handset can occupy eleven channels. Messages to/from handsets can occupy ten channels but only eight speech calls can be handled simultaneously, see .

Figure 23. Channel distribution in the DB1/BS3x0 connected to the IPBL



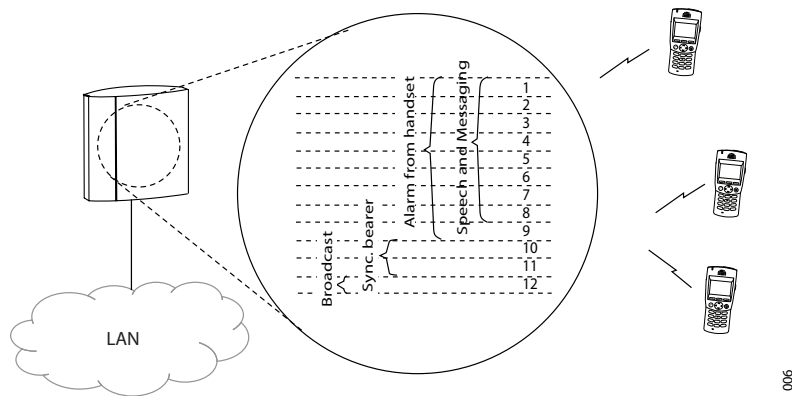
This means that even if a DB1/BS3x0 reports that it is busy i.e. fully occupied with speech calls and/or messaging, there are always channels free for alarm from handset and broadcast messages.

3.15.2 IPBS

The IPBS has in total twelve channels. One channel is reserved for broadcast messages and two channels are reserved for synchronization. Alarm from handset can occupy nine channels but only eight speech and/or messaging can be handled simultaneously, see [Figure 24. Channel distribution in the eight speech channel variant of IPBS](#), [page 25](#).

This means that even if a IPBS reports that it is busy, that is, fully occupied with speech calls and/or messaging, there are always channels free for alarm from handset and broadcast messages.

Figure 24. Channel distribution in the eight speech channel variant of IPBS



3.16 System Management

3.16.1 On Site Management

The device is managed using a web GUI accessed over the LAN.

3.16.2 Remote Management

The device can be managed over the Internet using a VPN client.

3.16.3 IP Administration Security

All IP administration is based on secure IP (HTTPS). All access to the device is password protected in order to prevent unauthorised access.

3.16.4 Software Upgrade

The device has support for software download and it is possible to do a software upgrade using the web interface. It also has support for automatic firmware update from a web server.

4 VoIP Signalling Protocols

Two of the protocols used for VoIP signalling are H.323 and SIP. 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 that defines Supplementary Services for H.323.

Like H.323, SIP can be used for VoIP but while H.323 is ISDN-based (Q. 931 and earlier H series), SIP is text-based. As opposed to H.323 which uses Abstract Syntax Notation number One (ASN.1), SIP encodes its messages as text, similar to HTTP and SMTP.

4.1 H.323

H.323 was developed by the International Telecommunications Union (ITU) and was designed from a telecommunications perspective. Ratified in 1996 it has become a defacto choice for interoperability among VoIP equipment. It is a standard that provides specification for computers, equipment, and services for multimedia communication over networks that do not provide a guaranteed QoS.

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

H.323 products and services offer the following benefits to users:

- 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.

4.1.1 H.450 Supplementary Services for H.323

H.450 is a series of protocols which are used to exchange signalling information to control the supplementary services such as, Call Transfer, Call Diversion, Call Waiting etc. over a LAN.

4.2 Session Initiation Protocol (SIP)

SIP is an application layer control (signalling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet multimedia conferences, Internet telephone calls and multimedia distribution. SIP is designed as part of the IETF standards.

SIP itself is not sufficient to set up a call and other IETF protocols such as RTP and SDP are required to support a VoIP call. However, the functionality and operation of SIP does not depend on any of these protocols.

4.2.1 IP-DECT System Internal Communication

The internal communication is based on H.323 but is always encrypted.

The Mobility Master listens to the following port:

- 1718–1719 UDP

The Master listens to the following ports:

- 1718–1719 UDP

- 1716–1717 TCP

The PARI Master listens to the following port (in addition to the Master ports above):

- 1722–1723 TCP

The Crypto Master listens to the following port:

- 1718–1719 UDP

The Radio listens to the following ports:

- 1718–1719 UDP
- 1718–1719 TCP
- 1724–1727 TCP

The Radio may also listen to 1728 and upwards (TCP) if in a Multiple Master system.

1718–1719 are used for connection with the PARI Master (TCP).

1724–1727 are used for DECT broadcast and multicast messaging (TCP).

Two additional ports starting at 1728 will be used for each dynamic master connection. The dynamic connections are created and destroyed when users from other Masters than their own PARI Master enters and leaves the coverage area of the Radio.

For example: In a system there are 4 Masters. One user from each Master is located on the same Radio. This Radio will then listen to ports 1718–1719 and 1724–1733 (TCP).

5 Related Documents

System Planning, IP-DECT System, TD 92683EN

Installation Guide, Base Station , TD 92988EN

Installation and Operation Manual for IP-DECT Base Station, TD 92682EN

Data Sheet, IP-DECT Base Station (IPBS), TD 92706GB

Data Sheet, IP-DECT Base Station (IPBS2), TD 92839EN

Data Sheet, IP-DECT Base Station (IPBS3), TD 93383EN

Data Sheet, IP-DECT Gateway (IPBL), TD 93670EN

Data Sheet, IP-DECT Virtual Appliance (IPVM), TD 93675EN

Installation and Operation Manual, WSM3, TD 92794EN

Installation and Operation Manual, Central Portable Device Manager (CPDM3), TD 92792EN

Data Sheet, Central Portable Device Manager (CPDM3), TD 92793EN

Installation and Operation Manual, CPDM ODBC, TD 92656GB

6 Document History

Version	Date	Description
A	2009-03-03	First version of the document
PB1	2011-06-29	Second preliminary version.
PB2	2012-09-26	New information about the feature Hot Desking and the feature Enhanced DECT Security feature.
B	15 January 2013	Have just removed the Preliminary stamp at top of pages.
C	10 January 2014	<p>Have added section 4.3 IP-DECT System Internal Communication on page 37.</p> <p>Updated sections 3.4.1 One Master Systems on page 9, 3.4.2 Multiple Master Systems on page 13 and 3.4.3 Multiple Mobility Master Systems on page 18 to reflect that 2047 IPBSs can now be used per PARI Master in an installation by setting the system ID to 293-296.</p> <p>Updated sections 3.9 Broadcast Messaging in Multiple Master Systems on page 30 regarding that broadcast messaging is not supported in large IP-DECT systems with more than 1023 IPBSs per PARI Master.</p> <p>Have added section 3.6 Mirror Devices on page 27 to reflect that a new DECT Master mode "Mirror" has been added to the currently available modes. Both the previously used modes "Active" and "Standby" can now instead be set to "Mirror".</p> <p>Have added section 3.7 Call Localization on page 28 which describes the new feature Call Localization. This feature is especially important for emergency calls when it is necessary to know the location of the calling party.</p> <p>Have updated section 3.9 Broadcast Messaging in Multiple Master Systems on page 30 to explain the concept of broadcast messaging and that it is not 100% proof.</p>
D	27 April 2015	<p>Have updated sections 3.9 Broadcast Messaging in Multiple Master Systems on page 30 regarding that broadcast messaging is now supported in large IP-DECT systems with more than 1023 IPBSs per PARI Master. Previously it was stated that broadcast is not supported in large IP-DECT systems</p> <p>Have updated the section 4.3 IP-DECT System Internal Communication on page 37 with IP ports: 1718-1719, 1722-1723, 1724-1727 and 1728.</p>

E	17 January 2019	<p>Updated and corrected 1.1 Abbreviations on page 1 and 1.2 Glossary on page 2.</p> <p>Updated section 2.2.2 IPBS on page 5 and 3.16.2 IPBS on page 34 regarding the use of IPBS1 as radio only.</p> <p>Added section 3.3 Wideband Audio on page 9 with a new function, wideband audio.</p> <p>Updated 3.4.3 Multiple Mobility Master Systems on page 18 with a four mobility master example.</p> <p>Updated 4.3 IP-DECT System Internal Communication on page 37 regarding IP ports.</p> <p>Updated Appendix A.2 regarding incoming messages.</p>
F	02 December 2019	<p>Added IPBS3 where it is applicable. Added Appendix B Performance Considerations, page 32.</p>
G — W		<p>Versions do not exist.</p>
X	16 May 2023	<p>B.2.1 Master, page 32: Updated limits for maximum number of users.</p> <p>General updates and editorial changes throughout the document.</p>
Y	03 September 2024	<p>Added IPBL and IPVM information throughout the document.</p> <p>Updated supported handset model information in 2.3.1 Handsets, page 3 and 3.10 Hot Desking, page 21.</p> <p>Minor editorial corrections.</p>

Appendix A Messaging Capacity

A.1 Alarm Messages from DECT handset

Time until received in the CPDM3/Unite system:	~ 2 sec
--	---------

A.2 Data to DECT handset

A.2.1 Incoming Messages to DECT handset

Number of message characters	For IPBL : Time in seconds until one handset is paged	For IPBS : Time in seconds until one handset is paged
20 characters	~ 4	~ 3
120 characters	~ 5	~ 3
240 characters	~ 6	~ 3
500 characters	~ 9	~ 3

A.2.2 Incoming Messages to DECT handsets in a Broadcast Group

Number of message characters	No of DECT handsets	For IPBL : Time in seconds until the group is paged	For IPBS : Time in seconds until the group is paged
20 characters	Unlimited	~ 4	~ 4
120 characters	Unlimited	~ 5	~ 5
240 characters	Unlimited	~ 13	~ 13
500 characters	Unlimited	~ 31	~ 31

Appendix B Performance Considerations

B.1 When to Switch off the Base Station Radio

B.1.1 Compulsary to Switch off the Base Station Radio

For systems with more than 1,000 Radios, the Radio in the Pari Master must be switched off.

Do not use the Pari Master for any other purpose, such as Kerberos server, to configure users on, Mobility Master, and so on.

B.1.2 Recommended to Switch off the Base Station Radio

It is recommended to switch off the Radio in the Pari Master in systems where SRTP is used under either or both of the following two circumstances:

- The number of users is more than 100.
- The number of Radios is more than 500.

B.2 System Capacity

B.2.1 Master

The system capacity for a Master is:

- For IPBS2: Up to 500 users for SIP over TCP or UDP; up to 250 users for SIP over TLS
- For IPBS3: Up to 1000 users for SIP over TCP or UDP; up to 500 users for SIP over TLS
- For IPBL: Up to 1000 users for SIP over TCP or UDP; up to 250 users for SIP over TLS
- For IPVM: Up to 4000 users

B.2.2 Pari Master

The system capacity for a Pari Master is:

- When the system ID used in the installation is between 1 and 36:
Max. 1023 IPBS per PARI Master or max. 240 IPBL per PARI Master.
- When the system ID used in the installation is between 37 and 292:
Max. 127 IPBS per PARI Master or max. 127 IPBL per PARI Master.
- When the system ID used in the installation is between 293 and 296:
Max. 2047 IPBS per PARI Master or max. 240 IPBL per PARI Master.
- For IPVM, when the system ID used in the installation is between 293 and 296:
Max. 3968 IPBS per PARI Master or max. 240 IPBL per PARI Master.

B.2.3 Mobility Master

The system capacity for a Mobility Master is:

- Max. 10 Mobility Masters per System
- Max. 100 Masters per Mobility Master

