IP DECT

SYSTEM DESCRIPTION

For MiVoice Business, MiVoice MX-ONE, and MiVoice Office 250

RELEASE 10.2
MARCH 14, 2019

Mitel®

NOTICE

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

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

TRADEMARKS

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

1 INTRODUCTION

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

The IP-DECT system supports the DECT 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.

1.1 ABBREVIATIONS

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.
HDB	Home location DataBase.
CPDM3/ WSM3	Mitel Central Portable Device Manager/Wireless Service Messaging. Unite module that enables messaging to and from the connected cordless telephone system.
IP	Internet Protocol: global standard that defines how to send data from one computer to another through the Internet.
IPBS	IP-DECT Base Station.
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.
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.
QoS	Quality of Service.
RAS	Registration, Admission, Status (H.323).
RFP	Radio Fixed Part. DECT base station part of the DECT Infrastructure. The local RFP part in an IPBS.
RFPI	The RFPI, Radio Fixed Part Identity, is the broadcast identity which uniquely identifies a RFP geographically.
SIP	Session Initiation Protocol.
Unite	Generic term for messaging system that unites different systems.
VoIP	Voice over Internet Protocol.

1.2 GLOSSARY

Roaming	The procedure of moving the handset from one IPBS 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 to another.
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.
Master ID	Master ID must be unique for each Master in a system. The Standby Master must have the same id as the Master.
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.
Sync Radius	The radius of the circle, around a particular base station, in which other Base Stations may synchronize with that Base Station.
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.
Handover Domain	Handover domain defines the Radios to which external handover is allowed. Handover domain is defined by the System ID.

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 built up by the following components:

- Handsets
- IP-DECT Base Station (IPBS)
- Radio Fixed Part (RFP)
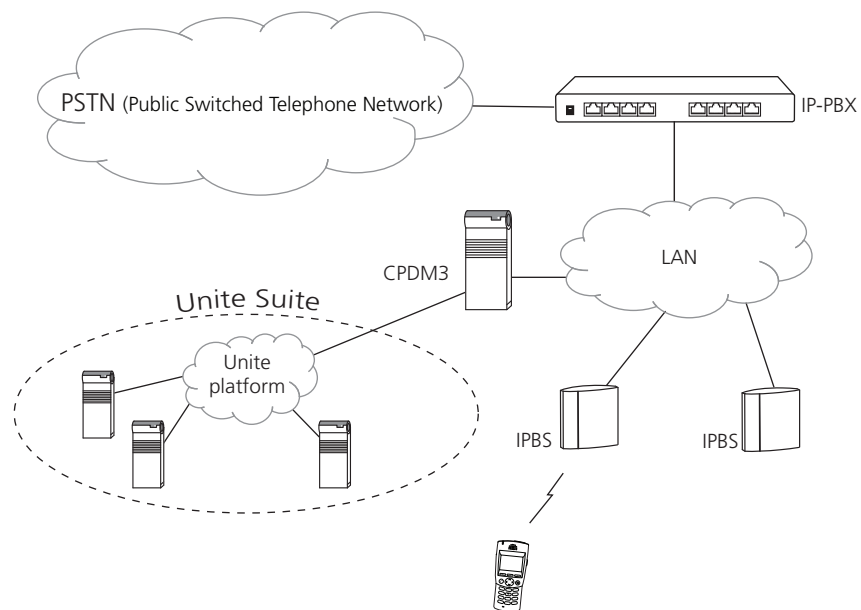- MiVoice MX-ONE, MiVoice Business, and MiVoice Office 250
- CPDM3/WSM3

Figure 1. IP-DECT System Overview

2.1 SYSTEM SIZE

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

2.2 SYSTEM COMPONENTS

2.2.1   HANDSETS

The Mitel IP-DECT system has support for Mitel DECT handsets, DT390, DT69x, DT4x3, Mitel 5603, 5604 5607, 5613, and 5614.

MiVoice MX-ONE supports DBCxxx, Mitel 5613, 5614, and 5624 models.

2.2.2   IPBS

The IPBS has eight channels used for speech, message and alarm. The IPBS also has one channel which is reserved for messaging and alarm.

2.2.3   IP-PBX

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

MiVoice MX-ONE supports CPDM3 and the 5613, 5614, 5624 and DT4x3 handsets.

MiVoice Business and MiVoice Office 250 supports WSM3 and 5613, 5614, 5607, 5624 handsets.

2.2.4   CPDM3/WSM3

The CPDM3/WSM3 contains support for messaging and alarm. This connects the IP-DECT system to the Unite platform.

The CPDM3/WSM3 contains also a Device Manager which supports parameter and software download to handsets. For more information, see the CPDM3/WSM3 documentation. These features are license dependent.

2.3 SYSTEM FUNCTIONS

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 in the system.

2.4 LAN/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 least 100 Mbps should be used.

2.5 SUPPORTED THIRD-PARTY FUNCTIONS

The developed products are designed to work in system provided by different vendors.

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 CPDM3/ WSM3 units, see 3.7 *Messaging in Multiple Master Systems* on page 27.

The IP-DECT system have 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

An Multiple Master system consists of the following entities which are software components which can be activated in an IPBS:

- Radio
- 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*.

3.1.1   RADIO

The Radio is a software interface between DECT and H323.

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 notifies itself 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 has 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*.

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 IPBS 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.

3.2.4   WIDEBAND AUDIO

Wideband Audio media is supported by IPBS2 only (software version 9.1.X or later). The support for Wideband Audio is also dependent on what model of handset that is used and the type of PBX that is used in the system and if handsets from other manufacturers supports the same wideband coder.

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

If the handset supports wideband audio, when moving with the handset during a wideband audio call and a handover to an IPBS1/IPBS4x0 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.

3.3   SYSTEM LAYOUT

This section describes examples of different system layout sizes:

- Multiple Master systems with Enhanced DECT Security, see 3.3.5 *Multiple Master Systems with Enhanced DECT Security* on page 22.
- Multiple Mobility Master systems with Enhanced DECT Security, see 3.3.6 *Multiple Mobility Master Systems with Enhanced DECT Security* on page 23.

3.3.1 ONE MASTER SYSTEMS

Single site installation

See figure 2.

The system capacity for this layout is:

- Up to 1000 users (Note: Up to 500 users if SIP over TLS is used.)
- When the system ID used in the installation is between 1 to 36:
  Max. 1023 IPBS per Pari Master
- When the system ID used in the installation is between 37 to 292:
  Max. 127 IPBS per Pari Master
- When the system ID used in the installation is between 293 to 296:
  Max. 2047 IPBS per Pari Master

This layout may be used for customers with a single site installation.

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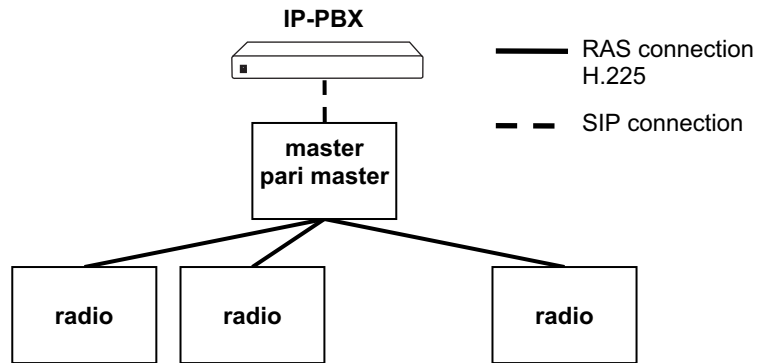

Figure 2. Example of a single site installation

The figure 3 below shows the software components. An IPBS includes all software components as described in 3.1 *Software Components* on page 9.

In a single site installation, one of the IPBSs 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.
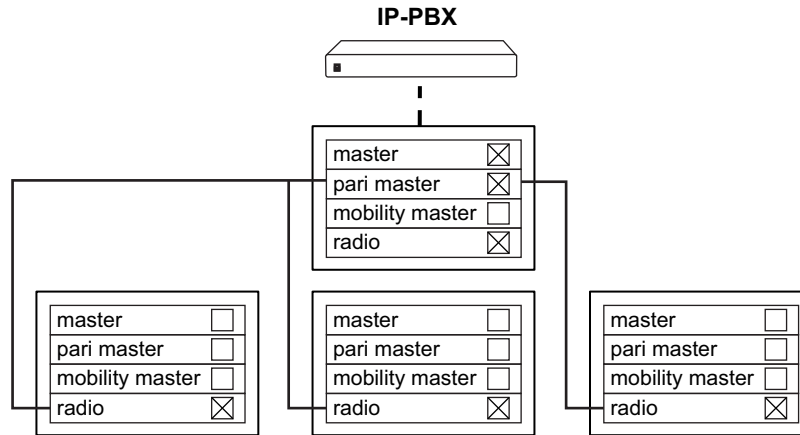

Figure 3. Distribution of software components

Multiple site installation

See figure 4.

The system capacity for this layout is:

*   Up to 1000 users (Note: Up to 500 users if SIP over TLS is used.)
*   When the system ID used in the installation is between 1 to 36:
    Max. 1023 IPBS per Pari Master
*   When the system ID used in the installation is between 37 to 292:
    Max. 127 IPBS per Pari Master
*   When the system ID used in the installation is between 293 to 296:
    Max. 2047 IPBS per Pari Master

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 IPBS 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.
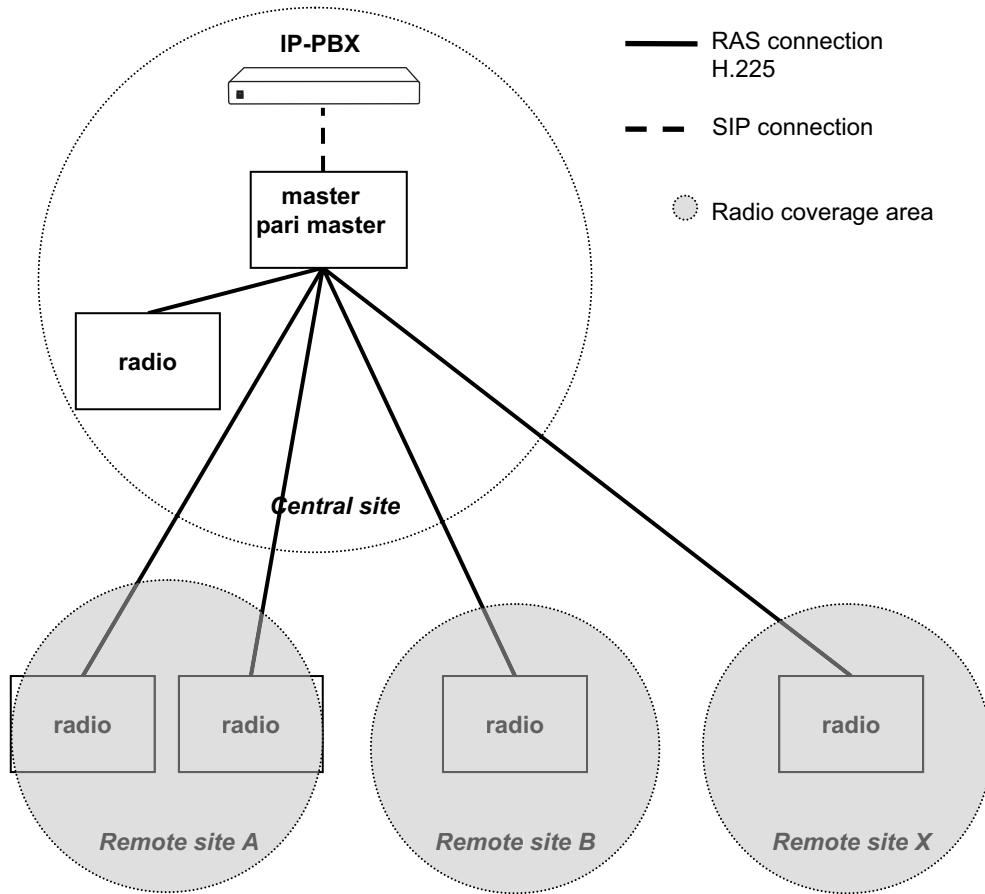
Figure 4. Multiple site installation

3.3.2   MULTIPLE MASTER SYSTEMS

Single site installation

See figure 5.

The system capacity for this layout is:

- Up to 1000 users per Master (Note: Up to 500 users per Master if SIP over TLS is used.)
- When the system ID used in the installation is between 1 to 36:
  Max. 1023 IPBS per Pari Master
- When the system ID used in the installation is between 37 to 292:
  Max. 127 IPBS per Pari Master
- When the system ID used in the installation is between 293 to 296:
  Max. 2047 IPBS per Pari Master
- Max. 100 Masters per Mobility Master

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.
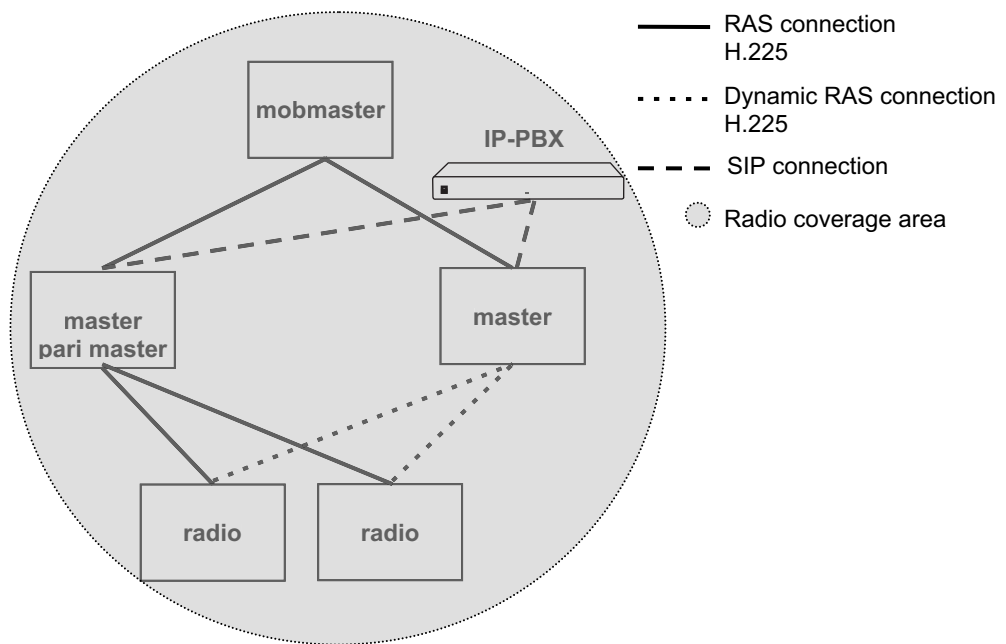

Figure 5. Single site installation

The figure 6 below shows the software components. An IPBS includes all software components as described in 3.1 *Software Components* on page 9.

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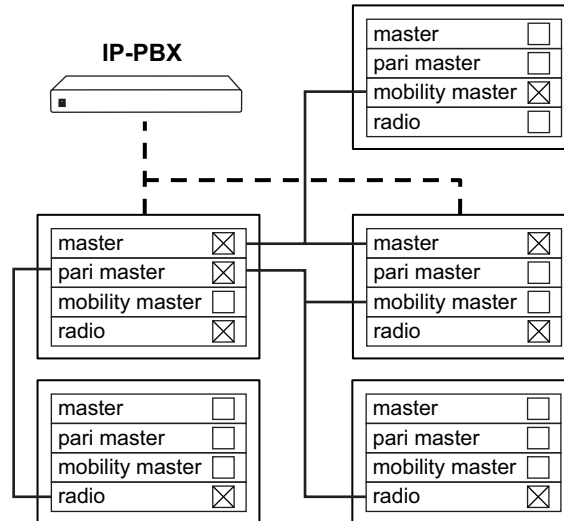

Figure 6. Distribution of software components

Multiple site installation

See figure 7.

The system capacity for this layout is:

- Up to 1000 users per Master (Note: Up to 500 users per Master if SIP over TLS is used.)
- When the system ID used in the installation is between 1 to 36:
  Max. 1023 IPBS per Pari Master
- When the system ID used in the installation is between 37 to 292:
  Max. 127 IPBS per Pari Master
- When the system ID used in the installation is between 293 to 296:
  Max. 2047 IPBS per Pari Master
- Max. 100 Masters per Mobility Master

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.
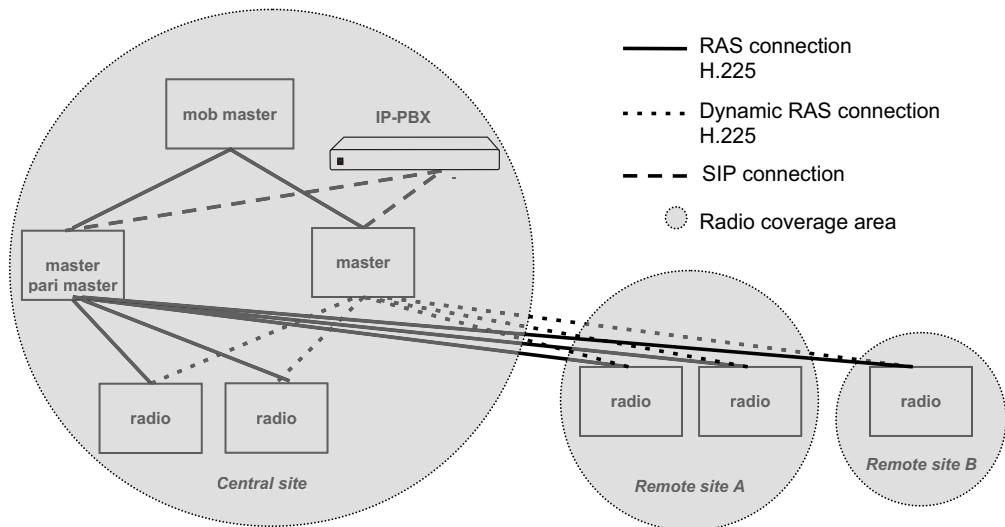

Figure 7. Multiple site installation with central Master

Multiple site installation with local functionality

See figure 8. The system capacity for this layout is:

- Up to 1000 users / Master (Note: Up to 500 users / Master if SIP over TLS is used.)
- When the number of system IDs used in the installation is between 1 to 36:
  Max. 1023 IPBS / Pari Master
- When the system ID used in the installation is between 37 to 292:
  Max. 127 IPBS per PARI Master
- When the number of system IDs used in the installation is between 293 to 296:
  Max. 2047 IPBS / Pari Master
- Max. 100 Masters / Mobility Master
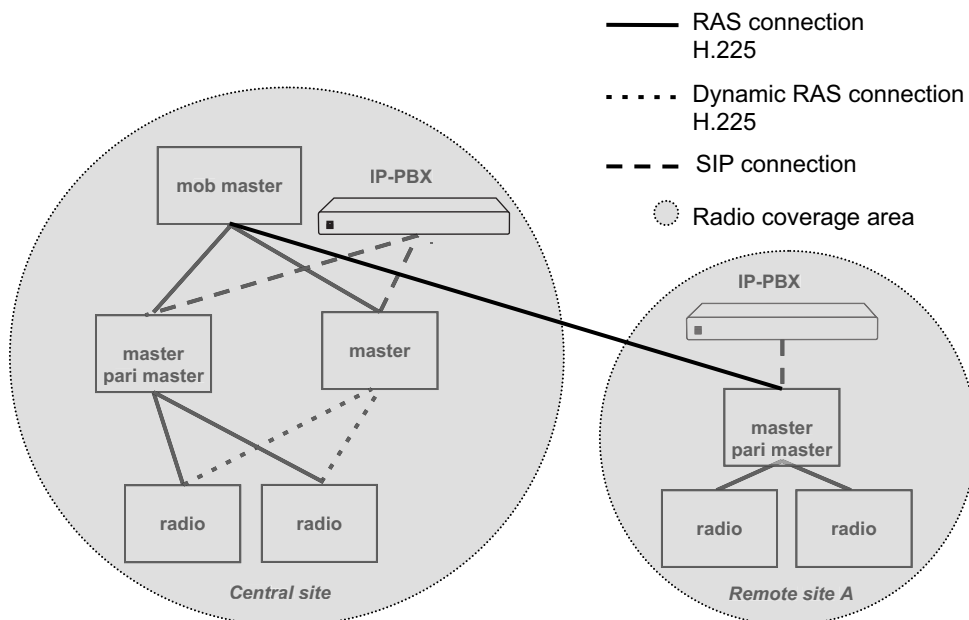 This layout is chosen if there is a need for local functionality in remote sites.

Figure 8. Multiple site installation with remote Master

The figure 9 below shows the software components. An IPBS includes all software components as described in 3.1 *Software Components* on page 9.

In site A, one of the IPBS 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 8.
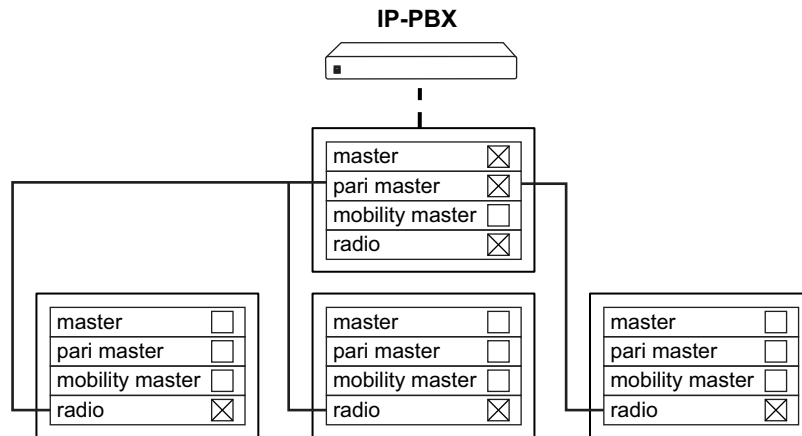
IP-PBX

Figure 9. Distribution of software components in remote site A.

3.3.3   MULTIPLE MOBILITY MASTER SYSTEMS

- Up to 1000 users per Master (Note: Up to 500 users per Master if SIP over TLS is used.)
- Max. 10 Mobility Masters per System
- When the system ID used in the installation is between 1 to 36:
  Max. 1023 IPBS per Pari Master
- When the system ID used in the installation is between 37 to 292:
  Max. 127 IPBS per Pari Master
- When the system ID used in the installation is between 293 to 296:
  Max. 2047 IPBS per Pari Master
- Max. 100 Masters per Mobility Master

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.
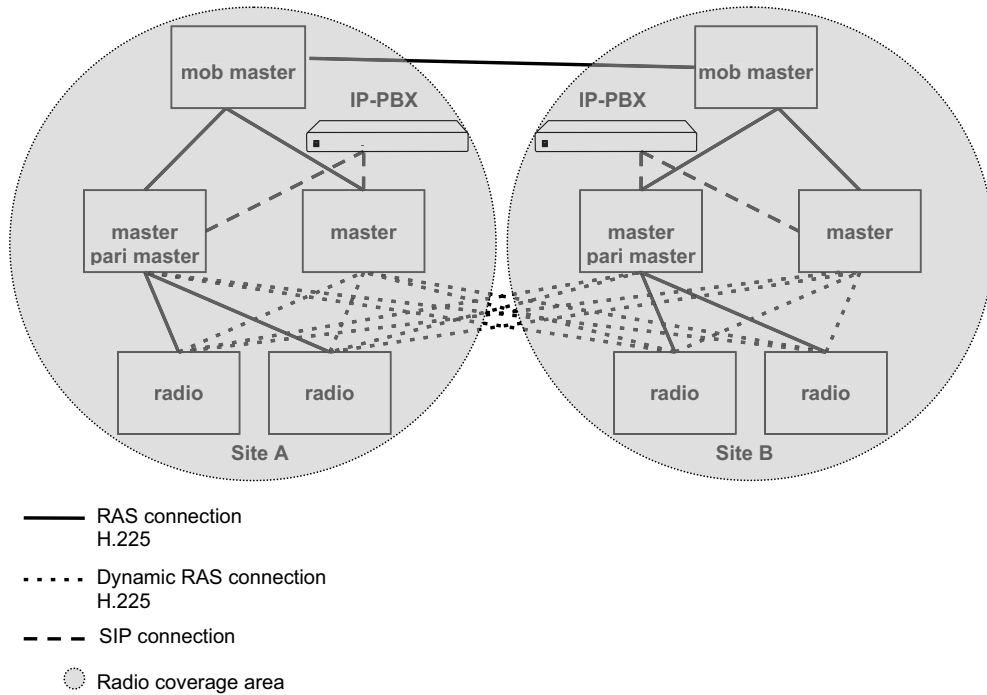
Figure 10. Multiple site installation

The figure 12 below shows the software components. An IPBS includes all software components as described in 3.1 *Software Components* on page 9.

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

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.

The following figure shows an example with four mobility masters.

Figure 11. Four Mobility Master Site Installation
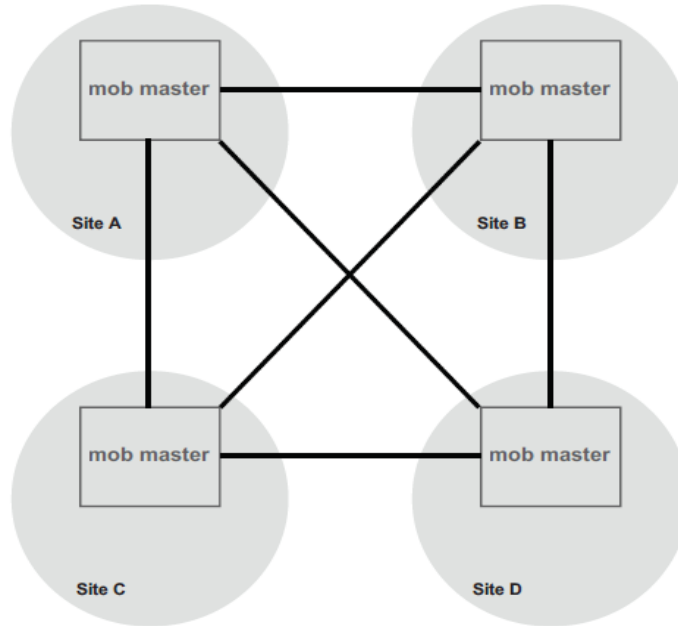
The table below shows how four mobility masters, as shown in the figure 11, should be configured.

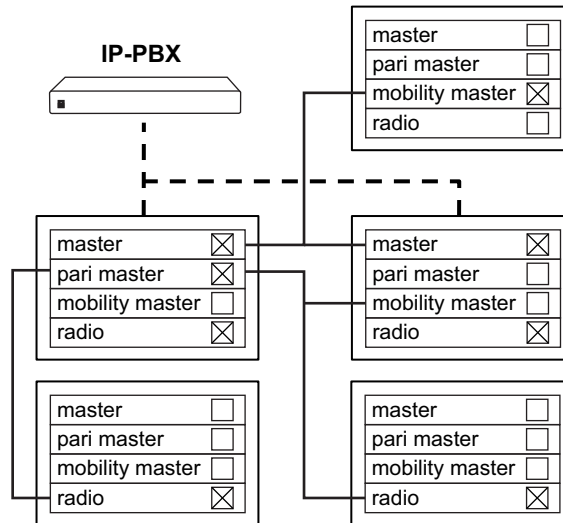| MOBILITY MASTER	CONFIGURE TO OTHER MOBILITY MASTERS
Site A	Site B,C,D
Site B	Site C
Site C	Site D
Site D	-

Figure 12. Distribution of software components in site A and B.

3.3.4 ONE MASTER SYSTEMS WITH ENHANCED DECT SECURITY

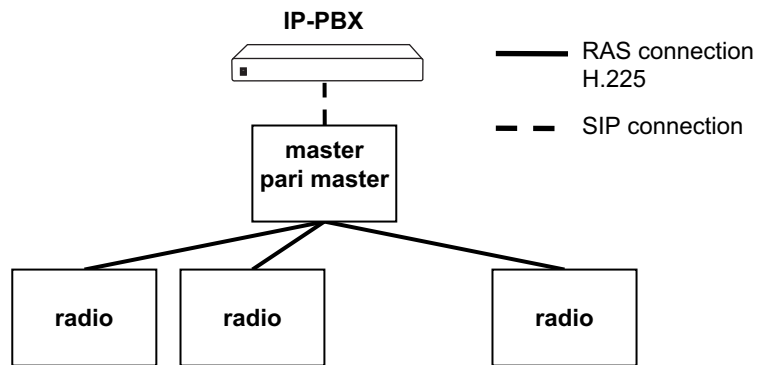The Crypto Master function needed for encryption, will be automatically activated in the Master.

Figure 13. Enhanced DECT Security in a one Master System

3.3.5 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 14. Enhanced DECT Security in a Multiple Master System

3.3.6 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.
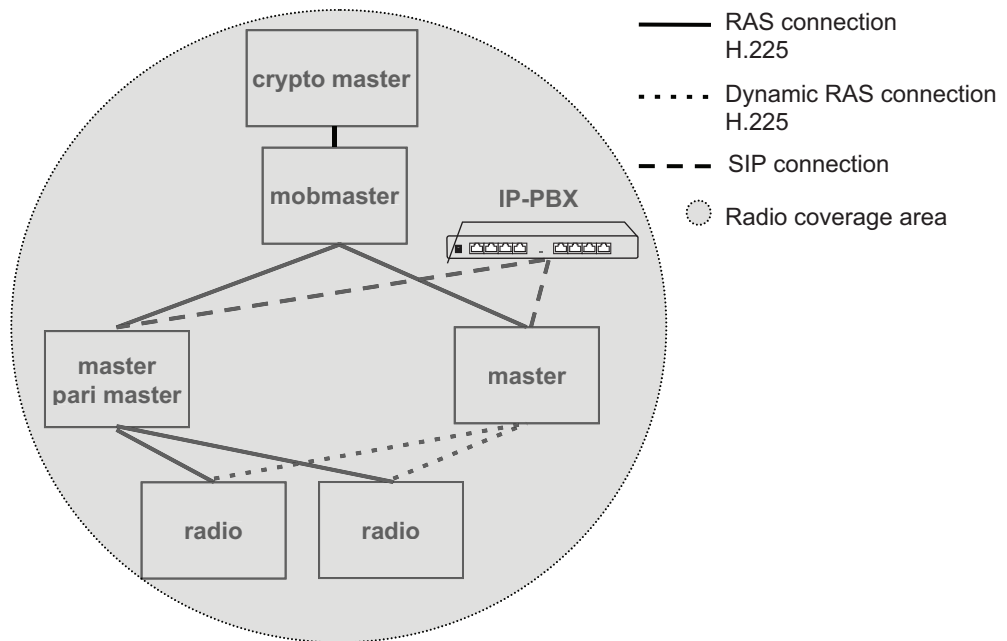
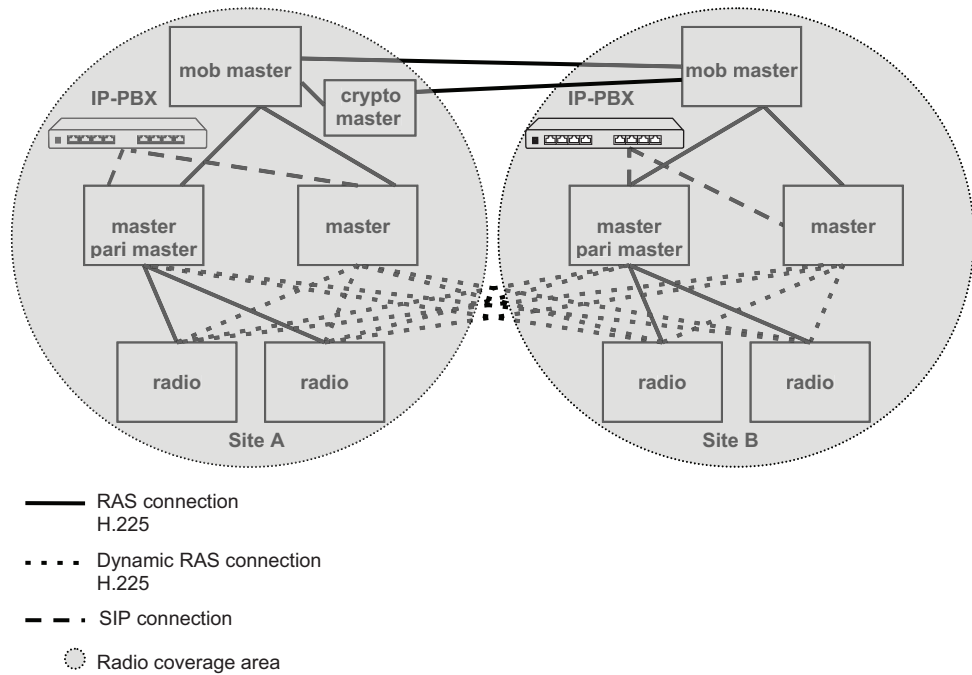**Note:** There can be only one Crypto Master.

Figure 15. Enhanced DECT Security in a Multiple Mobility Master System
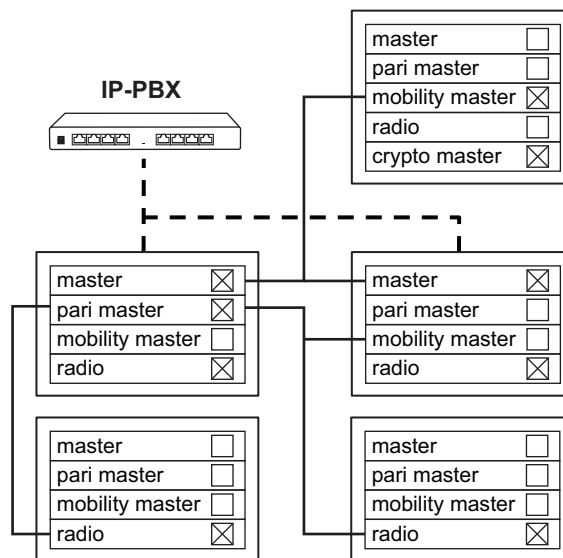
Figure 16. Distribution of software components in site A. Site B is the same but without Crypto Master.

3.4 STANDBY IPBS

It is recommended to have Standby IPBS's in an IP-DECT system. Depending on how the IP-DECT system is configured, standby IPBS's can be Standby Master, Standby Pari Master, Standby Mobility Master. When a Master goes down the corresponding Standby Master takes over.
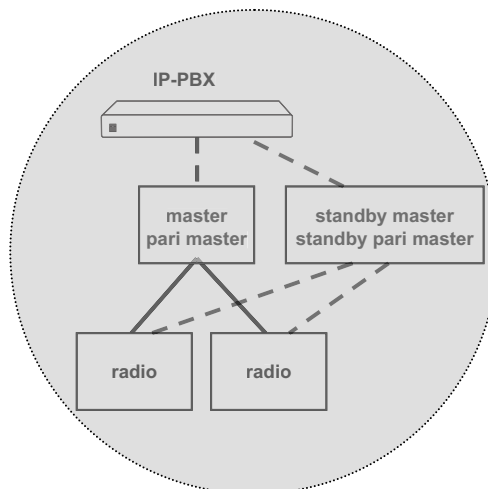
Read also about Mirror IPBS's, see *3.5 Mirror IPBS's*.

Figure 17. An IP-DECT system with a Standby Pari Master.

3.5 MIRROR IPBS'S

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.

3.5.1 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 IPBS. 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.

3.5.2 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.
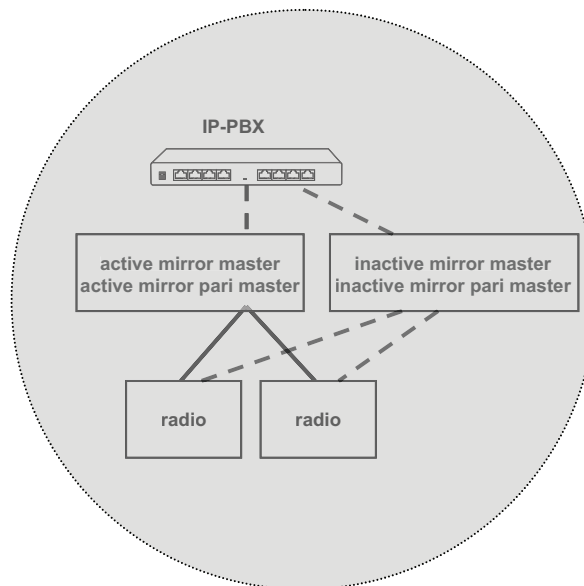

Figure 18. An IP-DECT system with Mirror Masters.

3.6 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).
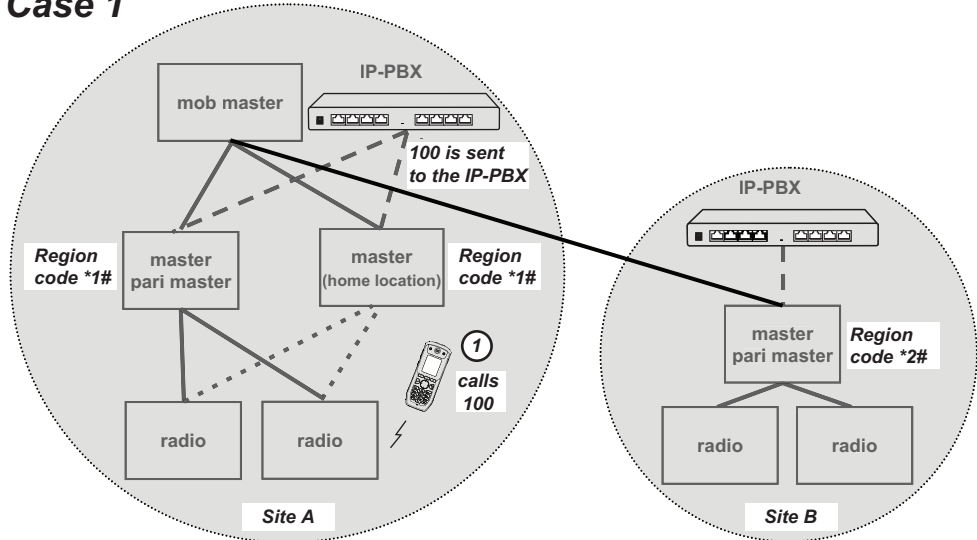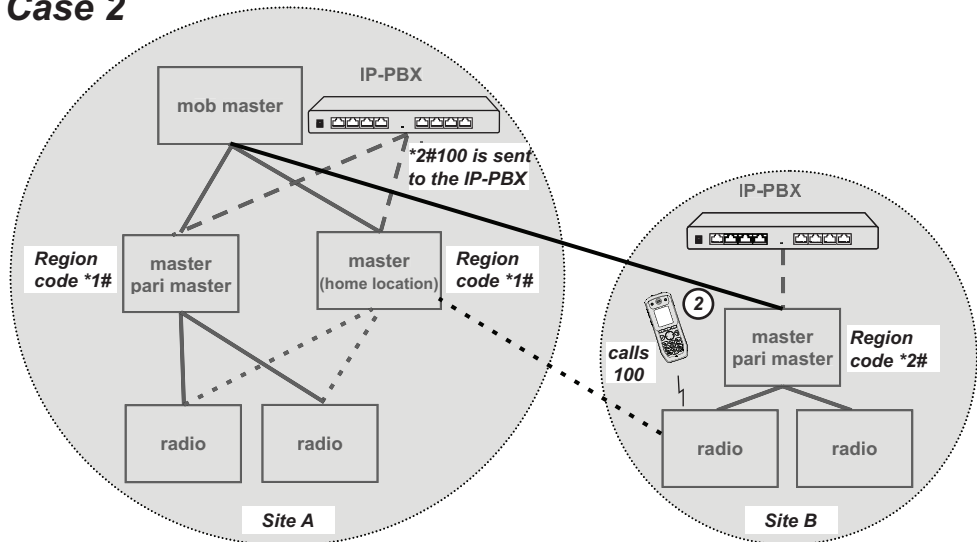
Call Localization using region codes.

3.7 MESSAGING IN MULTIPLE MASTER SYSTEMS

For messaging purposes the IP-DECT system can be connected to one or several CPDM3/WSM3 units. To have messaging functionality for all handsets in a multiple

Master system, each Master with handsets assigned must have a connection to a CPDM3/WSM3.
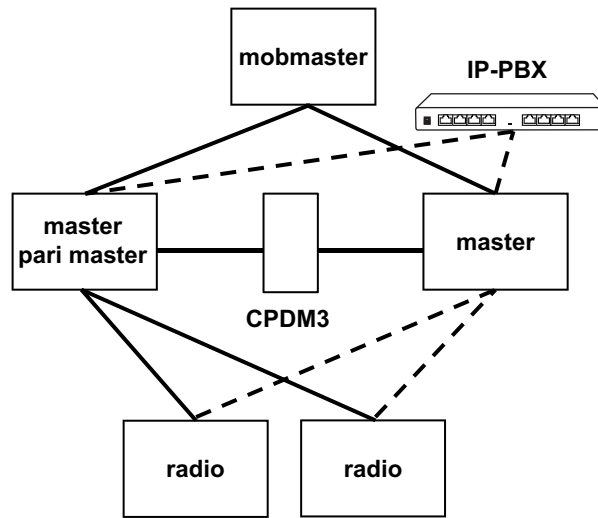

Figure 19. Messaging in multiple Master systems.

3.8 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.

3.9 DEVICE MANAGEMENT

A Device Manager (included in the CPDM3/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 for example upon handset model, number of simultaneous downloads, and call traffic load. The download time varies approximately from 17 minutes to 70 minutes.

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	
1	4
2	3
3	2
4 or more	1
	0

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.

3.10 FAULT REPORTING

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

3.11 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*.

3.12 SYNCHRONIZATION

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

- Air synchronization (IPBS)

3.12.1 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 20.

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 20.

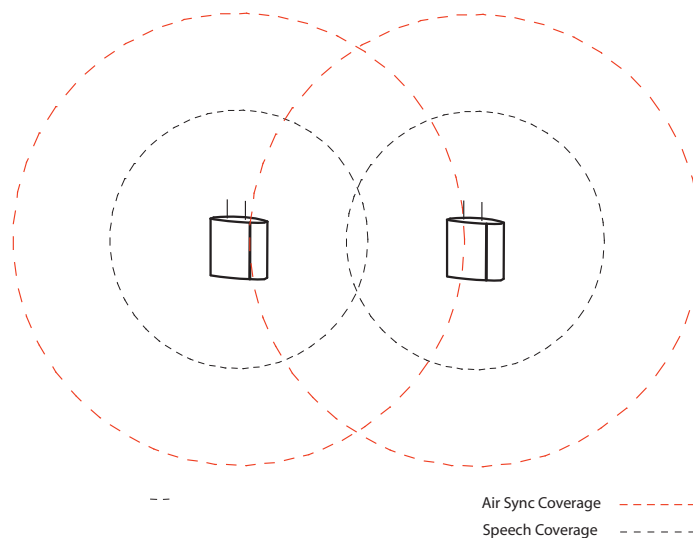Air Sync Coverage – – – – – –
Speech Coverage – – – – – –

005

Figure 20. Air- and speech sync radius.

3.13 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.

3.13.1 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 21.
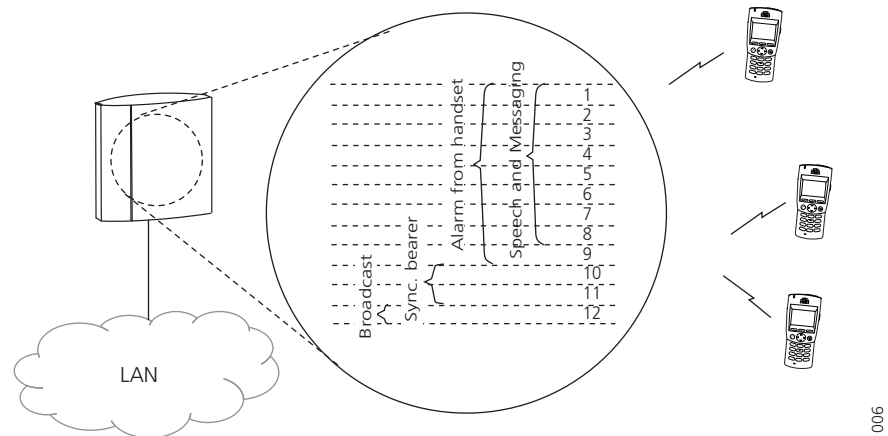
Figure 21. Channel distribution in the IPBS.

This means that even if a IPBS 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.

3.14 IP-DECT SYSTEM MANAGEMENT

3.14.1 ON SITE MANAGEMENT

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

3.14.2 REMOTE MANAGEMENT

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

3.14.3 IP ADMINISTRATION SECURITY

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

3.14.4 SOFTWARE UPGRADE

The IPBS 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 which 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.

4.3 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 if in a Multiple Master system.

1718-1719 is used for connection with the PARI Master. 1724-1727 are used for DECT broadcast and multicast messaging. 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 the 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 1718-1719,1724-1733.

5   RELATED DOCUMENTS

System Planning, IP-DECT	51/1551-ANF 901 14
Installation and Operation Manual for IP-DECT Base Station	13/1531-ANF 901 14
Installation and Operation Manual, Central Portable Device Manager (CPDM3)	19/1531-ANF 901 43
Wireless Messaging Gateway (WSM3) Installation and Operation Guide	-
WinPDM Installations and Operations Manual	12/1531-ANF901 43

Appendix A: Messaging Capacity

A.1 Alarm Messages from DECT handset

Time until received in CPDM3/WSM3:	~ 2 sec

A.2 Data to DECT handset

A.2.1 Incoming Messages to DECT handset

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 IPBS: TIME IN SECONDS UNTIL ONE HANDSET IS PAGED:
20 characters	1	~ 3
120 characters	1	~ 3
240 characters	1	~ 3
500 characters	1	~ 3

NUMBER OF MESSAGE CHARACTERS:	NO OF DECT HANDSETS:	FOR IPBS: TIME IN SECONDS UNTIL ALL HANDSETS ARE PAGED:
20 characters	1 10 30 100	~ 3 ~ 3 ~ 6 ~ 23
120 characters	1 10 30 100	~ 3 ~ 3 ~ 9 ~ 27

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

| NUMBER OF MESSAGE CHARACTERS	NO OF DECT HANDSETS:	FOR IPBS: TIME IN SECONDS UNTIL THE GROUP IS PAGED:
20 characters	Unlimited	~ 4
120 characters	Unlimited	~ 5
240 characters	Unlimited	~ 13
500 characters	Unlimited	~ 31

Appendix B: Messaging in Mitel Multiple Master System

B.1   Messaging limitations

B.1.1   System with two sites and one Master on each site

If a message call is initiated at the WSM3/CPDM3 connected to the handset's "Home Master". The handset will always receive the message even when the handset is at the "other" site.

Figure 22. Two Site System - One Master on Each Site
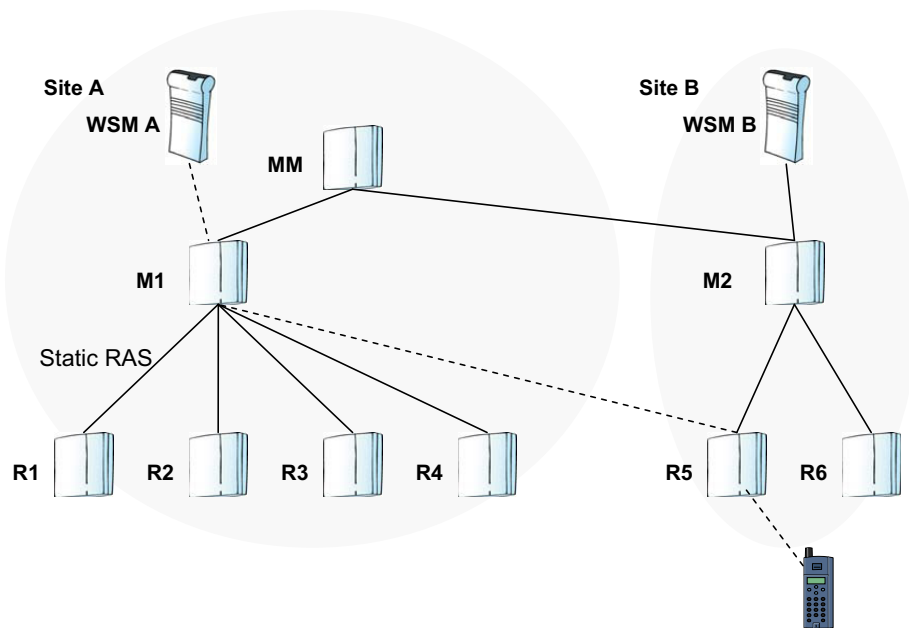
B.1.2   System with one site but two or more Masters

If you have more than 1000 users on a site, you must have two or more Masters. If all handsets shall have messaging, each Master must have its own WSM3/CPDM3. There

is no message routing between the WSM3/CPDM3s or the Masters. A message call to a handset must be entered at the handset's home WSM3/CPDM3 and Master.

Figure 23. One Site System - Two or More Masters