

**Note:** The SIP-DECT OMM only uses the ConfigURL from RCS. Other information provided from RCS is not supported.

The OMM requests information from RCS only if no information has been retrieved from RCS prior to the request. The response is stored permanently in the OMM. To force a new RCS request, the OMM must be reset to default settings, through the **Discard OMM DB and configuration files** or **Reset OMM RFP(s) to factory defaults** on restart (see section 5.4.1.15).

### 7.8.9 CUSTOMER LOGO ON OMM WEB SERVICE

SIP-DECT 6.0 and later supports the integration of a customer-specific logo on the OMM Web service interface. If a customer\_image.png file is available on an external file server, customers can integrate their own logo into the OMM. This logo is displayed beside the Mitel logo on the top bar.

This image can be imported by:

- Configuration of a branding image URL to a file server using OMP (see section 6.5.2.7)
- Automatic search for a file named 'customer\_image.png' on the provisioning server

The branding image is stored permanently in the OMM database, ensuring that the image is available even if a configured file server or provisioning server is not reachable. The file is deleted automatically from the server on a "file not found" response or by disabling the branding image URL configuration.

The picture should not be larger than 50 pixels high and 216 pixels wide.

### 7.9 DECT BASE STATION CONFIGURATION FILES

IP-RFPs support two DECT base stations configuration files (downloaded from a server) to get configuration settings. There is one common file "ipdect.cfg" for all DECT base stations and one file specific file "<MAC>.cfg" for every IP-RFP. The DECT base station requests the "ipdect.cfg" file if a URL is provided. The RFP specific <MAC>.cfg is requested if this is indicated in the common "ipdect.cfg" file.

It is possible that all RFPs request "ipdect.cfg" and only selected RFPs request the <MAC>.cfg to obtain a specific configuration on some RFPs.

#### 7.9.1 STANDARD IP SETTINGS

Standard IP settings (which are necessary for access to the RFP configuration files) are configured via DHCP (see section 7.5) or OM Configurator (see section 7.6). These are:

- IP address
- Net mask
- Gateway (i.e. router)
- Boot file name
- TFTP server
- Public option 224: "OpenMobility" or "OpenMobilitySIP-DECT" (to identify the relevant DHCP offer)
- Domain Name Server (optional)
- Domain Name (optional)
- URL to the RFP configuration files

All other parameters can be set by using an RFP configuration file even if standard DHCP options or OM Configurator parameters exist.

#### 7.9.2 CONFIGURATION FILE SOURCE

A TFTP / FTP(S) / HTTP(S) URL specifies the protocol, server and path to access the RFP configuration files. The URL can include account data if appropriate.

Syntax:

```
{ftp|ftps|http|https}://[user:password@]server/[directory/]
or
http://server/[directory/]
```

The URL configuration is provided via DHCP option code 233 (prio1), or the OM Configurator.

- "ipdect.cfg" is mandatory if an URL is provided by DHCP or local static configuration via the OM Configurator.
- "<MAC>.cfg" is mandatory if it is indicated in the "ipdect.cfg" that a "<MAC>.cfg" exists for the DECT base station. (There is a key word to indicate that a "<MAC>.cfg" exists for every DECT base station.)

Mandatory means that if a file cannot be loaded, the DECT base station does not start. This is relevant for the following scenarios:

- RFP boot / startup (after power on, software update, etc)
- A change of the URL

#### 7.9.3 PARAMETER SETTINGS PRIORITY

Some parameters can be set via DHCP / OM Configurator or by using the files "ipdect.cfg" or "<MAC>.cfg". If a parameter is provided through more than one of the possible ways, the last setting has priority. There is the following order:



If the configuration file(s) cannot be retrieved ...

- The RFP continues operation with the last successfully retrieved configuration file(s).
- The RFP will try to retrieve the configuration files again, starting with an interval of one minute and doubling this interval with each retry, not exceeding the update check interval (either default or configured).
- If the RFP is using DHCP, a renewal of the lease is scheduled so that possible changes in DHCP configuration will be detected.
- Failure to retrieve the configuration files is reported via Syslog.

### 7.9.7 HANDLING OF PARAMETER CHANGES

A change of a parameter (DHCP / OM Configurator, RFP configuration files) does not necessarily mean a change to the RFP's configuration because the parameter could be covered up or previously set using an alternative way.

**Example 1:**  
IP address of a Syslog Daemon has been changed in "pdedct.cfg" but is covered up by "<MAC>.cfg" in which this parameter has not been changed.

**Example 2:**  
A parameter is new in "<MAC>.cfg" but has been set previously in "pdedct.cfg" with the same parameter value.

Only if a parameter change causes a change in RFP configuration (as a sum of e.g. DHCP / OM Configurator, "pdedct.cfg" and "<MAC>.cfg" files) will the RFP perform a configuration update procedure. Depending on the changed parameter, an RFP configuration update is done:

- On the fly without any service interruption e.g. IP address of a Syslog Daemon has been changed.
- With an application restart e.g. OMM IP address has been changed.

### 7.9.8 CONFIGURATION FILE SYNTAX

```
#####
# sample configuration file for the OpenMobility system
# retrieved via the net using file transfer protocols
# like ftp, ftp, http, https, ftps
#
#####
# comments start with the hash sign: "#"
#
#####
# BOOL variables support the following values
# YES Y 1 TRUE (case does not matter)
# NO N 0 FALSE (case does not matter)
# other values are interpreted as false
```

```
#
#####
# personal configuration files
#
# personal configuration files have the following name
# <OWN-MAC>.cfg, where <OWN-MAC>.cfg is of the form
# e.g. 003042ABCDEF.cfg
#
# all RFPs will also load the <OWN-MAC>.cfg file
OM_PersonalConfig1=1 # BOOL
#
# DO load the individual file for the RFP with mac 003042FEF0D0
# no matter what OM_PersonalConfigAll says
OM_PersonalConfig_003042FEF0D0=y
#
# DO NOT load the individual file for the RFP with mac 003042ABCDEF
# no matter what OM_PersonalConfigAll says
OM_PersonalConfig_003042ABCDEF=n # BOOL
#
# time interval for checking the remote cfg files in seconds
# minimum value is 300 (5 minutes)
# maximum value is 604800 (7 days)
OM_ConfigCheckInterval=500
#####
# OpenMobility system
#
# the OpenMobilityManager ip addresses
OM_ManagerIpAddress1=172.30.205.17
OM_ManagerIpAddress2=172.30.205.18
#
# path to the software image
OM_SwImageURL=ftp://172.30.207.21/openmobility/sw/!p=fp3g.dnld
#
# SYSLOG
OM_SysLogIpAddress=172.30.207.20
OM_SysLogPort=10115
#####
# transfer core files to the following directory
```

OMM\_ConfFiles=vpn1=ftp://10.103.35.20/confFiles

## 7.10 CONSOLIDATED CERTIFICATE MANAGEMENT

SIP-DECT has various secured interfaces to support secure connections for file imports from local servers or provisioning servers. By default, the OMM Web server uses the hardcoded self-signed OMM certificate as local certificate for encrypted AXI connections, for provisioning (mutual authentication), and for SIP-over-TLS connections.

Certificate and authentication validation settings for these secure connections can be inherited from the configuration file URL (see section 7.8.1).

### 7.10.1 SIP OVER TLS CERTIFICATES

SIP over TLS certificates are used for secure SIP connections. The hard coded self-signed OMM certificate is used by default, however you can import trusted certificates, a local certificate chain and a private key file (optionally password-protected) via:

- OMP (System -> SIP -> Security tab)
- OMM Web service (System -> SIP -> Security)
- A certificate server (usually running on a Mitel call server)

### 7.10.2 OMM CERTIFICATE (WEB SERVICE / AXI)

The OMM Web server uses the hard coded self-signed OMM certificate by default as the local certificate for encrypted AXI connections.

You can overwrite the hard coded OMM certificate by importing a local certificate chain and a private key file (optionally password-protected) via the OMP (System -> Advanced settings -> OMM Certificate tab). You can also configure an OMM certificate server (System -> Advanced settings -> OMM Certificate server tab) to enable provisioning of OMM certificate files.

The OMM certificate will be used for incoming AXI and HTTPS connections to the OMM services. If the OMM can be reached from the internet by a domain and an appropriate CA certificate has been imported, no security warnings are displayed in web browsers trusting the CA root certificate.

### 7.10.3 PROVISIONING CERTIFICATES

Provisioning certificates are used for secure connections to configuration or firmware files servers with support for mutual authentication (i.e., for FTP, FTPS, and HTTPS protocols).

The OMM uses a trusted certificate chain to validate the server. This is required if the server has no certificate derived from a trusted CA root certificate, where the OMM uses the Mozilla CA Certificate List. If no server certificate is available, you can disable the validation against trusted and CA certificates.

By default, the hard-coded self-signed OMM certificate is used for mutual authentication. You can overwrite the hard coded OMM certificate by importing trusted certificates, a local certificate chain and a private key file (optionally password-protected) via:

- OMM Web service System -> Provisioning -> Certificates page (see section 5.4.2.5)
- OMP System -> Provisioning -> Provisioning Certificates tab (see section 6.5.5.2)
- A provisioning certificate server through OMP System -> Provisioning -> Certificates server tab (see section 6.5.5.3)

The OMM provides the local certificate chain and the private key to servers requesting mutual authentication. The private key file may be password protected.

The system credentials can be inherited if specific sources for configuration and resource files are configured, where the 'Use common certificate configuration' option is enabled.

### 7.10.4 CERTIFICATE VALIDATION

If the HTTPS or FTPS protocol is used to retrieve files from the configured provisioning server, the OMM validates the server certificates according to the certificate validation settings.

You can configure the certificate validation settings via OMP (System -> Provisioning -> Provisioning - SSL settings) or the OMM Web service (System -> Provisioning -> Certificates). Certificate validation settings can also be part of the ConfigURL provided by the RCS or via DHCP.

If you want to use the same validation settings for a specific URL (i.e., other than the configuration file URL), enable the "Use common certificate configuration" parameter when configuring the URL (unless the "Import certificates with first connection" parameter is enabled).

## 7.11 RFP 35/36/37 IP / RFP 43 WLAN SOFTWARE UPDATE

The DECT base station checks several locations for a software update. If found, the software is copied to the flash memory, leaving the current software intact. After successful installation, the OMM is notified about the new software. Activation of the software is then managed by the active OMM. DECT base stations that do not have a connection to the OMM activate and start the software immediately.

Locations for software updates:

- Attached USB mass storage device with a software image **iprtf36.dnd** in its root directory. The USB mass storage device must be formatted using the vfat32 file system.
- If ipdect.cfg supplies the **OM\_SwImageURL** variable, the URL is used to get the boot image. Please see section 7.7.7.
- TFTP server, path and file configured using the OM Configurator or via DHCP.
- OMM (SIP-DECT 6.0 or later): If the RFP 35/36/37 IP / RFP 43 WLAN have no valid URL from which to load the software, they attempt to load the software from the connected OMM. If the OMM is running on a DECT base station, the RFP OMM delivers the software to the connected base stations. See section 7.8.7 for more information.

## 7.12 802.1Q SUPPORT

The IP RFPs support VLANs according to IEEE 802.1Q. VLAN can be administered

- on a per port basis of the LAN switch assuming that the IP RFPs are connected to a single port of a switched Ethernet environment, or
  - by assigning a VLAN ID to the IP RFP matching the VLAN they should operate in.
- VLAN tagging has only to be set to IP RFPs in the last case. The whole section refers to that case. With this, also 802.1p priority within Ethernet frames is enabled.

The scope of the following description is restricted to VLAN tagging and obtaining the VLAN ID. Quality of Service mechanisms like 802.1p priority and DiffServ are not described in this section.

#### VLAN implementation notes referring to IP RFPs:

- IP RFPs are not able to support VLAN ID 0 as described later in this section. Any other valid VLAN ID can be configured.
- If a VLAN ID is configured, all traffic from an IP RFP will be tagged with this VLAN ID.
- The VLAN ID configured for an IP RFP is also used for the OMM running on this IP RFP.
- Once a VLAN ID is set to the IP RFP, incoming frames are only accepted if they are tagged as well. Therefore the switch port must be configured as a tagged trunk for this VLAN.
- The VLAN configurations can be done using DHCP or the interface for the local static configuration, the OMI Configurator.
- The use of VLAN does influence the boot up process of the IP RFP because the VLAN configuration takes place during the boot up phase.
- The default setting is not to tag the traffic. 802.1Q tagging is enabled if the VLAN ID is set. If no VLAN ID is set 802.1Q is disabled.

#### Why not VLAN ID 0 ?

VLAN ID 0 means that the IP RFP's traffic belongs to the port/native VLAN. The Ethernet switch port to which the IP RFP is connected must be configured to accept 802.1Q tagging for this to work, and the switch must interpret VLAN ID 0 as the port/native VLAN ID per the IEEE 802.1Q standard.

The packets from the IP RFP are tagged with VLAN ID 0 and the packets sent to the IP RFP are tagged with the port/native VLAN ID. This scenario does not work, because the IP RFP supports only one VLAN ID in both directions. That means the VLAN ID in the receive direction must be the same as the send direction.

### 7.12.1 BOOT PHASE OF IP RFPs (DHCP)

Because the IP RFP does not know about VLAN at the beginning of the start up, two DHCP scopes are required. This applies regardless of the Ethernet switch being used. The following scenario with arbitrary VLAN IDs' details the steps an IP RFP would go through in a typical dual-VLAN implementation.

#### Step A. DHCP scope within the native VLAN:

- 1 IP RFP boots up and obtains an address on the native VLAN.
- 2 The data VLAN DHCP option 132 directs the IP RFP to go to voice VLAN.

#### Step B. DHCP scope within the voice VLAN:

- 1 IP RFP releases the data VLAN address and obtains an address on the voice VLAN and all other parameters.
- The voice VLAN does not have the DHCP option 132, because an IP RFP already on the voice VLAN does not need to be directed to go there.

- 2 IP RFP is operational on the voice VLAN.

If a reboot or power cycle occurs, the IP RFP returns to step A.

If an IP RFP cannot obtain an address on the voice VLAN, due to network or DHCP problems then the IP RFP falls back automatically to untagged frames (native VLAN).

To avoid the DHCP scope within the native VLAN the VLAN ID to be used can be set permanently via OMC without losing the ability to provide other parameter via DHCP, please see section 7.7.

### 7.12.2 BOOT PHASE OF IP RFPs (LOCAL CONFIGURATION)

The PC running the OMI Configurator must be a member of the native VLAN for the first configuration, later on within the voice VLAN set.

If a wrong or unknown VLAN ID is set, you can overwrite or read the configuration using no VLAN tag on the switch port in the first six seconds after the RFP is connected to a power supply / PoE. After six seconds the RFP applies the local configuration and starts using the parameters.

### 7.13 INSTALLING OMM IN HOST MODE

In this case, the OMM software must be installed on a PC running Red Hat Enterprise Linux 7 or CentOS 7. The network parameters with which the OMM works in this mode depend on this PC's network configuration.

Once started, OMM works permanently on the PC. In case of fatal error or PC restart, OMM will restart automatically.

**Please note:** Check that the versions of the OMM and RFP software on your SIP-DECT installation are the same.

### 7.13.1 SYSTEM REQUIREMENTS

The OMM application is a 32-bit/x86 application that can be installed on a 32-bit or 64-bit (recommended) operating system. The PC-based OMM requires the following configuration:

- Red Hat Enterprise Linux 7 or CentOS 7 operating system
- Server hardware minimum:
  - Processor : Dual Core Intel@ Xeon@ 3065, 2.33GHz, 4MB cache
  - Bus 1333 MHz
  - Memory : 4GB DDR2 SDRAM 667 MHz
  - Hard disk: 80 GB SATA 7200 rpm
  - 1 GB/s Ethernet interface

### 7.13.2 INSTALLING THE OMM SOFTWARE

The OMM software for the Linux Redhat server is provided as a self-extracting executable file (e.g., SIP-DECT\_6.1.bin). This binary file contains two Red Hat packages:

- SIP-DECT-OMM-<SIP-DECT-version>.i586.rpm  
OpenMobility Manager software.
- SIP-DECT-HANDESET-<DECT phone-version>.i586.rpm  
Software for Mitel 600 DECT phones

The Mitel 600 DECT phone software can be updated via the Air interface, see section 7.20. A separate software package can also be provided for specific updates of the DECT phone software.

**IMPORTANT :** Log in as "root" to install and/or update OMM. If you do not login as root to open the OMM console, the path to omniconsole is not set. You must enter the whole path "/usr/sbin/omniconsole" to start the OMM console.

#### Command syntax

For extraction and automatic standard installation  
`sh SIP-DECT_<version>.bin`

For extraction and automatic standard installation  
`sh SIP-DECT_<version>.bin -f`

For extraction of RFP packages only  
`sh SIP-DECT_<version>.bin -x`

RPM packages can also be installed manually.

For a first OMM type installation

`rpm -i SIP-DECT-OMM-<version>.i586.rpm`

For an OMM software update (see section 7.14)  
`rpm -U SIP-DECT-OMM-<version>.i586.rpm`

For Mitel 600 DECT phone software installation

`rpm -i SIP-DECT-HANDESET-<version>.i586.rpm`

To delete a software release

`rpm -e SIP-DECT-HANDESET and`

`rpm -e SIP-DECT-OMM`

To check an installed release

`rpm -qi SIP-DECT-OMM`

or

`rpm -qi SIP-DECT-HANDESET`

After the installation phase, start OMM by running the command  
`"/etc/init.d/sip-dect-omm start"`

### 7.13.3 CONFIGURING THE START PARAMETERS

The basic data for initializing OMM is stored in the file "/etc/sysconfig/SIP-DECT". It can be edited to modify the OMM interface.

```
#####
# OMM configuration file
#####
# If you use a different interface for omn activate/correct parameter below
#OMM_IF="eth0"
#
# OMM_CONFIG_FILE=/opt/SIP-DECT/tmp/omm_conf.txt
#
# If you use OMM resiliency for OMM activate parameter below with OMMs IP addresses
#OMM_RESILIENCY="192.168.0.1:192.168.0.2"
#
# Automatic OMM database import:
# rmp / rmp / HTTP(S) URL specifies the import server and file
```

| Parameters      | Description   |
|-----------------|---|
| OMM_IF          | Interface for communicating with the RFPs (by default: eth0)                              |
| OMM_CONFIG_FILE | File that contains the OMM configuration (by default: /opt/SIP-DECT/tmp/omm_conf.txt)     |
| OMM_RESILIENCY  | In case of OMM redundancy, enter the two IP addresses of the OMMs. See also section 7.15. |

### 7.13.4 SPECIFIC COMMANDS – TROUBLESHOOTING

The OMM software is installed but does not work automatically when the PC starts. The command below stops or starts OMM manually (User root):

`/etc/init.d/sip-dect {start|stop|restart}.`

The command line interface for OMM is accessible via telnet on port 8107.

#### Malfunction

To check whether OMM is working, see the list of procedures for the "SIP-DECT" process. If OMM does not start, delete the lock file "/var/lock/subsys/SIP-DECT".

To delete the OMM configuration remove the OMM configuration file "/opt/SIP-DECT/tmp/omm\_conf.txt" (by default).

### 7.14 UPDATING THE OMM

The procedures for updating an existing DECT installation with new software depend on

- whether a single OMM or standby OMM installation is used
- whether the OMM is running on an RFP or PC

The OMM "standby" feature is described in section 7.15.

The update mechanism allows an update of the RFPs with minimum impact to DECT services, especially for installations with a standby OMM.

All RFPs check the availability of a new boot image file automatically when:

- the DHCP lease is refreshed,
- the RFP lost the connection to the OMM,
- one of the service applications running on the RFP must be restarted, and
- an RFP configuration file update check is done (see section 7.7.7).

**Please note:** Make sure that all configured software sources point to the same software version, so that the OMM and all RFPs are running the same software version.  
**Please note:** RFPs without a configured software image URL (via DHCP, OMC or ipdectl.<mac>.cfg) retrieve their software directly from the OMM. In this case, the RFP activates the software immediately. This feature is only available with 3G RFPs.

As soon as an RFP detects a new boot image file on the TFTP server (or the software download server using FTPS or HTTPS), it notifies the OMM. The OMM keeps track when it is safe to restart an RFP in order to leave the DECT service synchronized.

RFPs scheduled for restart are marked with a yellow sign within the Web service (see section 5.6.1) or in a separate column within the OM Management Portal (OMP), see section 6.7.1.1.

**Please note:** Only software upgrades from the preceding two releases are tested for upgrade to the current release. Additional steps may be required to upgrade systems with software that is three or more releases behind the current release.

### 7.14.1 UPDATING A SINGLE OMM INSTALLATION

In the case of a single OMM installation, a DECT network outage during the update procedure is unavoidable.

**Please note:** Updating a single OMM installation results in a DECT network outage during the update procedure.

For the update, replace the boot image file on the TFTP server(s) with the new one.

#### OMM in RFP mode

If the OMM is running on an RFP, force the update of this RFP by pressing the **Update** button on the **System settings** web page (see section 5.4.1.6). The RFP checks the boot image file on the TFTP server and reboots if a new one is found.

#### OMM in host mode (on Linux server)

If the OMM is running on a dedicated Linux server, install the new software as described in section 7.13.2 on the PC with the command `SIP-DECT_<version>.bin`. This stops the running OMM automatically and installs the new software. After the installation phase, restart the OMM by executing the command `/etc/init.d/sip-dect-omm start`.

As soon as the RFPs lose the connection to the OMM (because of the update), the RFPs detect that a new image file is on the TFTP server and reboot with the new image file.

### 7.14.2 UPDATING A STANDBY OMM INSTALLATION

**Please note:** Updating a standby OMM installation causes a switch over between both OMMs. All active calls will be dropped.

For the update replace the boot image file on the TFTP server(s) with the new one.

#### OMM in RFP mode

Force the update by pressing the **Update** button on the **System settings** web page (see section 5.4.1.6). The OMM-RFP checks the boot image file on the TFTP server and initiates an update procedure, if a new image file has been found.

The automated update procedure performs the following steps:

- 1 Reboot the RFP residing the standby OMM.
- 2 Reboot the RFP residing the active OMM which causes a failover to the standby OMM.
- 3 Reboot all other RFPs that are able to find the new boot image file one by one. This is managed by the new active OMM.

This procedure reduces the downtime of the SIP-DECT system to a minimum due to the optimized failover.

**Please note:** Please be aware that a minimum downtime of the system can only be reached if the system was in a stable working state when initiating the update and the IP infrastructure guarantees a fast update of the OMM RFPs (e.g., no 64kbit/s line to download the SW into the RFP).

#### OMM in host mode (on Linux server)

For an update with a minimum impact to the DECT service do the following:

- 1 Replace the boot image file on the TFTP server(s).
- 2 Manually update the standby OMM.
  - a) Stop the OMM service.
  - b) Install the new software.
  - c) Start the OMM service.
  - d) Wait at least 30 seconds before you go on with updating the active OMM.
- 3 Manually update the active OMM.
  - a) Stop the OMM service.
  - b) Install the new software.
  - c) Wait at least 30 seconds.
  - d) Start the OMM service.

**Please note:** A one-by-one update of RFPs is not possible if the signaling interface between the OMM and the RFP has been changed. Please see the release notes delivered with the software.

To enforce an update of the whole DECT system at once, deactivate / update both OMMs simultaneously. The RFPs will lost the connection to both OMMs and will automatically restart with the new boot image file.

## 7.15 OMM STANDBY

To perform OMM standby, two OpenMobility Managers must be provided in an OMM network. One operates as the active OMM, and the other operates as the standby OMM.

In the event that the RFP designated as the OMM fails, the other RFP, designated as the secondary OMM automatically assumes the role of the OpenMobility Manager.

### How OMM Standby works

During system start-up, each RFP retrieves either one (if no standby OMM is configured) or two (if OMM Standby is configured) OMM IP addresses and both try to connect to each other. The active OMM serves all connections from RFPs or DECT phones.

During normal operations, both the active and the standby OMM are in contact and monitor each other's operational state. They continually exchange their current standby states and the standby OMM receives a copy of any configuration changes on the active OMM. As long as both OMMs are in contact, their databases are synchronized automatically.

If the primary OMM fails, the OMM responsibilities are taken over by the standby OMM to maintain operation. A "No Standby" warning is displayed on the OMM web interface, indicating that there are no longer two functioning OMMs in the network or cluster. Configuration changes are made unsafely in this situation.

If the active OMM fails, the inactive OMM recognizes this and begins to act as the active OMM, and starts the web service.

If the connection between the two OMMs fails, the network or cluster essentially breaks into two operational parts. The standby OMM becomes the active OMM. At this point, the two OMMs cannot detect one another and, therefore, cannot synchronize. When the connection between the two OMMs is re-established, the synchronization of the OMMs forces one OMM to become the standby OMM again. Once the recently failed OMM returns to service and becomes the inactive OMM, it does not resume the role of active OMM.

### 7.15.1 CONFIGURING OMM STANDBY

Each RFP of the DECT system must be configured with two OMM IP addresses. Both OMM addresses can be either configured via DHCP (see section 7.5.1) or with the OM Configurator (see section 7.6).

### 7.15.2 FAIL OVER SITUATIONS

Fail over occurs when:

- an OMM error occurs on the active OMM.
- the RFP, acting as the active OMM is shut down or rebooted at the SSH console.
- the OMM is rebooted in the web browser menu.

- the active OMM is unreachable.
- the standby OMM becomes the active OMM when:

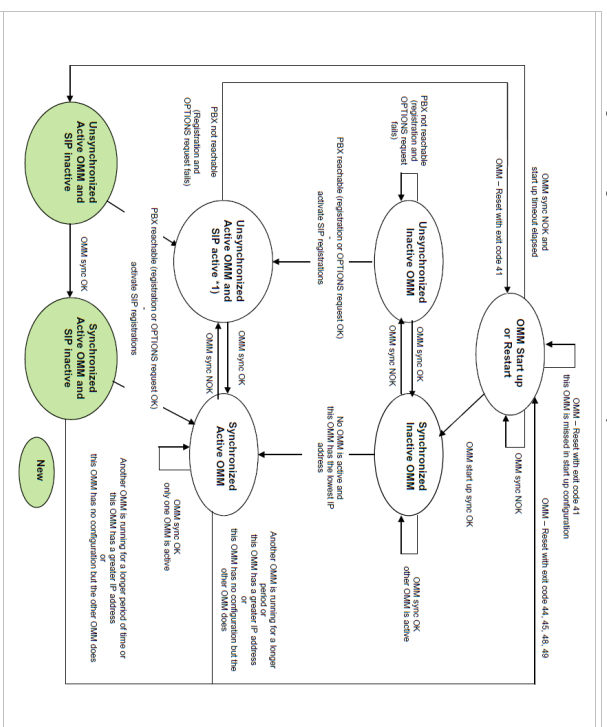
- the configured SIP Proxy/Register is reachable.
- the other OMM has a larger IP Address while no OMM is active and both OMMs are in contact with each other (normally at system startup).

When the OMMs get in contact again:

- both OMMs check which one ran for a longer period. That one will become the active OMM. The other one falls back to the standby one.

### 7.15.3 FAIL OVER FAILURE SITUATIONS

Failover failure occurs when the connection between OMMs fails and the configured SIP Proxy/Register is unreachable. In this case the active OMM waits until the SIP Proxy/Register is reachable. The following state diagram shows the OMM Standby states:



**OMM sync OK**: OMMs are synchronized and are able to exchange their operational states

**OMM sync NOK**: OMMs are not synchronized and are not able to exchange their operational states

**\*)** In this state the DECT air interface might not be in a definite state as both OMMs are active but cannot connect with each other! This is caused by IP network failures and cannot be handled by the SIP-DECT system in



a proper automatic way. In such a scenario it is not predetermined which RFP connects with which of the 2 OMMs. The DECT network can split-up into two unsynchronized DECT sub-networks. This can cause voice quality and handover problems.

With these states ("... SIP inactive") the OMM standby mechanism takes care in the start up phase that all SIP users does not become active if the PBX is not reachable. This avoids a possible double SIP registration when the PBX and the other OMM is reachable again before both OMMs negotiate which OMM becomes the active one.

The double SIP registrations might cause a user not to be reachable when his latest SIP registration came from that OMM that was negotiated to be the inactive one and the SIP registrar cannot handle two or more simultaneous registrations (non-forking proxy).

Similarly, it could happen in rare cases that both OMMs become temporarily active. In such a situation all SIP-DECT users would be SIP registered from both OMMs to the configured PBX. This can cause problems, if the PBX accepts only one registration per user (non-forking proxy).

To prevent such problems a mechanism is implemented to detect situations with two active OMMs. If such a situation is detected the remaining active OMM SIP re-registers all users to the PBX if the OMM **SIP Registrar after 2 active OMM failover** parameter is set (see section 5.4.3.6).

#### 7.15.4 SPECIFIC STANDBY SITUATIONS

Some aspects must be described in case of OMM state changes when they are unsynchronized.

##### 7.15.4.1 How a standby OMM becomes active

In an unsynchronized OMM state, the standby OMM must decide whether to become active or not. The OMM tries to contact the configured SIP proxy and registrar. If a specific user account has not been designated to use for visibility checks (see section 7.20.7), the OMM starts a SIP registration for the DECT phone with the lowest phone number and sends an OPTIONS request to the configured proxy. If there is an answer the SIP proxy/registrar is considered reachable and the OMM becomes active.

##### 7.15.4.2 When OMMs are not synchronized

In an unsynchronized OMM Standby state, the connection between the OMMs is broken. In case of a network problem, both OMMs might be in this state. During this time an inconsistent OpenMobility system is operational with some constraints.

The OMM Web service issues a warning with the message "No Standby" for both OMMs and it is possible that configuration changes made are not saved.

When both OMMs are in contact again, the longer running OMM becomes the active OMM and overwrites the database file in the standby OMM. Configuration changes made in this OMM instance are lost.

#### 7.15.4.3 Two DECT air interfaces

When both OMMs are in an unsynchronized and active state, they are fully operational. DECT base stations that lose their connection to the OMM because of a network outage might connect to the other OMM. Two DECT air interfaces are present and work in parallel.

**Note:** Since both air interfaces use the same PARK, it is impossible to determine on which OMM a location registration succeeds.

For DECT phones different situations are possible:

- They do not notice this situation:
  - active calls stay established, depending on network conditions;
  - DECT phones can make and receive new calls, depending on an available PBX connection;
  - DECT phones can do handover to RFPs connected to the same OMM;
  - DECT phones can call DECT phones that are registered to the other OMM
- They lose their RFP base station and perform a new location registration:
  - active calls are broken;
  - DECT phones can make and receive new calls, depending on an available PBX connection;
  - DECT phones can do handover to RFPs connected to the same OMM;
  - DECT phones can call DECT phones that are registered to the other OMM;
- They lose their RFP base station and search the DECT network without finding another one:
  - active calls are broken;
  - DECT phones stay in searching for network until an air interface is available again.

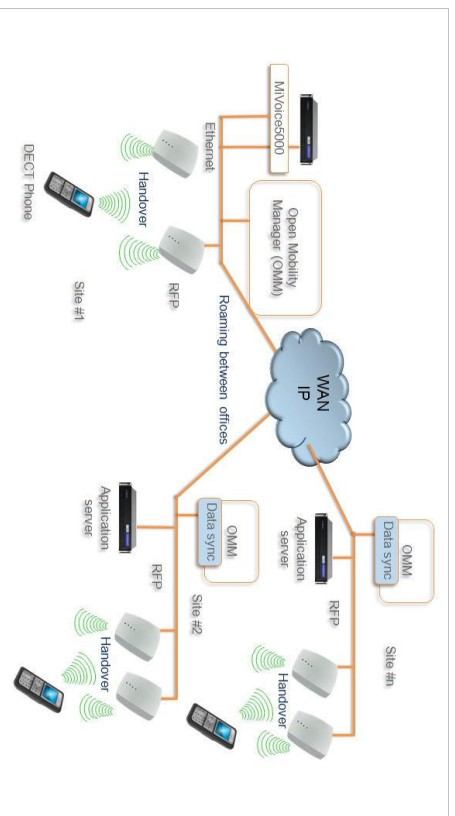
**Note:** Handover between DECT phones located to RFPs that are controlled by different OMMs is not possible.

When the OMMs are in contact again, the inconsistencies are resolved.

## 7.16 USER DATA SYNCHRONIZATION (MINVOICE 5000 DUAL HOMING SUPPORT)

SIP-DECT 6.1 introduces support for user data synchronization to ensure that SIP-DECT telephony services survive if the network connection to the OMM goes down. The feature ensures user and device database redundancy among all OMM instances in the system.

When user data synchronization is enabled on an OMM instance, the OMM propagates changes in user, device, Configuration over Air (CoA) profiles or SAR1 configuration to a central OMM. AXI is used to distribute configuration changes between the central and peripheral OMMs.



Instead of subscribing to the standard Primary Access Rights Key (PARK) of a single OMM when registering with the system, the DECT phones subscribe using the Secondary Access Rights Identifier (SARI) that applies to multiple OMMs in the system. All DECT phones that are subscribed to the system using the SARI can roam between sites (and OMMs). The PARK of the central OMM is defined to be the SARI.

**Please note:** Subscription to the SARI and successful roaming is only supported for Mitel 600 DECT phones. Behavior of third party GAP phones is not guaranteed. It is recommended that you add 3rd party GAP phones as fixed devices and configure them to subscribe to the "PARI only". See section 6.10.4.5 for more information.

All DECT phone users are registered to a central SIP proxy, used by all OMM sites (as long as the network environment is stable). OMM sites may implement local secondary SIP proxies, where local DECT phones register in case of a failed network connection.

## 7.16.1 ROAMING

The following sections describe the roaming concepts supported with the user data synchronization feature.

### 7.16.1.1 Device roaming

All DECT phones that subscribe successfully to the system SARI can roam between sites. Subscription to the system SARI is enabled by default when a DECT phone is created. SIP registration is renewed automatically with the OMM at the new site so that users can make and receive calls from all sites. Unbound devices can also roam, but they are not SIP registered.

### 7.16.1.2 User roaming

Users with existing DECT phones can go to another site and log into an unbound DECT phone. The login to the old DECT phone is removed, and when the SIP registration is renewed, the DECT phone is registered with the OMM at the new site, so that the user can make and receive calls from there.

### 7.16.1.3 Move of SIP registration

The SIP registration follows the user's location, according to the following rules:

- When the change in site location is detected, the new OMM initiates a SIP registration.
- All other OMM sites are notified of the change, such that the OMM for the previous site does not renew the DECT phone SIP registration and broadcasts the change to all other OMMs.
- When the new OMM receives the update from the previous OMM, the SIP registration is repeated.

If there is any interruption in the user data synchronization, other OMMs are not notified of the change. In this case, the OMM at the new site initiates a SIP registration as soon as the change in site is detected. If the OMM does not receive an update within 30 seconds, the new OMM renews the SIP registration anyway.

When user data synchronization is restored, the appropriate notifications resume:

- The previous OMM does not renew SIP registration for the DECT phone and broadcasts the information to all other OMMs.
- The OMM at the new site repeats the SIP registration when the update is received.

**Please note:** If the OMM hosting an active Mitel DECT phone does not receive an updated location registration for the device for more than two hours, the OMM does not renew the SIP registration until the location registration is refreshed.

## 7.16.2 SETTING UP USER DATA SYNCHRONIZATION

Data synchronization is only implemented for user, DECT phone, and Configuration over Air (CoA) data. The SARI is copied from the central OMM to the peripheral OMMs. All other data must be configured on each OMM individually. If there are any configuration conflicts due to network connection failure, the user and device changes (that have the same key id) with the most recent time stamp are used.

To set up user data synchronization for your SIP-DECT system, you must:

- define the central OMM and generate a SARI for all OMMs to use when registering to the system
- configure links to the central OMM from every peripheral OMM in the system
- create a dedicated user account to verify standby OMM availability

### 7.16.2.1 Defining the central OMM

You must select an OMM to act as the central OMM for user data synchronization. When you have selected the OMM, generate the SARI from the OMM's PARK value (via the OMP System -> Basic settings -> DECT tab). See section 6.5.1.2 for configuration details.

All Mitel 600 DECT phones registered with the OMM can then roam to all other OMM sites (which may be added later).

### 7.16.2.2 Configuring links to the central OMM

Each peripheral OMM in the system must connect to the AXI interface of the central OMM for user data synchronization. If a standby configuration is used for the central system, both OMMs must be configured in the peripheral OMMs. You configure the connection to the central OMM via the OMM **System** -> **Data management** -> **DECT phones synchronization** tab (see section 6.5.7.3 for configuration details).

Before you link a peripheral OMM to the central OMM, you must delete all user and device data, and CoA profiles from the local OMM. After the connection is established, verify that the user and device data from the central OMM have been received, then reconfigure the deleted users and devices.

**Please note:** Concurrent configuration of user and device data may cause conflicts. This can happen if one or more OMMs are not visible due to network issues. If conflicts are detected for user or devices with the same key Id, those with the most recent timestamp are kept.

SIP-DECT provisioning mechanisms ensure that there are no conflicts with user data synchronization. However, the system cannot regulate operations such as "auto-create on subscription". Under rare circumstances, conflicts can arise with the result that a user action may be ignored: Repeat the action to ensure it is registered by the system.

You must also ensure that the calling party numbers do not conflict with any conference room, FAC prefix or alarm trigger number across all OMMs in the system.

**Please note:** The user data synchronization mechanism does not validate conference room, FAC prefix or alarm trigger numbers. If such numbers conflict with a user's calling number, synchronization terminates immediately.

### 7.16.2.3 Creating a user account for standby visibility checks

If the active or standby OMM loses connectivity, each OMM checks connectivity to the SIP proxy. By default, a real SIP user account is used to check the availability of the OMM (via a SIP registration to the SIP proxy). In a dual homing environment, this may impact the user's telephony services due to the data synchronization.

To avoid this issue, you must create a virtual SIP user to be used exclusively for checking OMM availability (one account for the entire system). See 7.20.7 for more information on this feature.

## 7.16.3 USER DATA SYNCHRONIZATION MODES

The user/device synchronization runs on every peripheral OMM with a configured link to the central OMM. The synchronization function requires an internal AXI connection and an external AXI connection to the central OMM.

There are two synchronization modes: System startup or reconnection to resolve conflicts and copy new or changed datasets, and dynamic synchronization mode.

### 7.16.3.1 Start-up / reconnection mode

In start-up/reconnection mode, the user data synchronization service reconciles the data in the peripheral OMMs and central OMM. The steps in the user data synchronization mechanism are:

- 1 Read user/device data and profiles from internal AXI.
- 2 Read SARI from external AXI.
- 3 Set SARI on internal AXI.
- 4 Read user/device data and profiles from external AXI.
- 5 Resolve conflicts.

- **Inconsistent associations** (one device bound to two different users): Association is deleted on the system with the older user/device timestamps. An unbound user remains.
- **Inconsistent number** (two different user datasets using the same number): The user with the older timestamp is deleted (including any existing device associations)
- **Inconsistent additional ID** (two different user datasets with the same additional ID): The user with the older timestamp is deleted (including any existing device associations)
- **Inconsistent association** (one user bound to two different devices): Association is deleted on the system with older user/device timestamps. An unbound device may remain if an IPEI was configured, otherwise the device is deleted.
- **Inconsistent IPEI** (two different device datasets with the same IPEI): The device with the older timestamp is deleted (including any existing user associations)

### 6 Copy data.

Data with the most recent timestamp is copied to either the peripheral OMM (if data in the central OMM is more recent) or the central OMM (if data in the peripheral OMM is more recent), including:

- profile datasets with newer timestamps
- changed users with newer timestamps (with the device dataset, if bound)
- new users (with the device dataset, if bound)
- changed unbound devices with newer timestamps
- new unbound devices

### 7.16.3.2 Dynamic mode

In dynamic synchronization mode, events related to new, changed, or deleted users/devices received from one OMM are applied on the other OMM.

In rare cases, when configuration changes are made on multiple OMMs simultaneously (e.g. by configuration via OMP/Web, login/logout on devices, auto-create on subscription, etc), thereby creating new conflicts, the user data synchronization service closes the AXI connections and restarts after a minute to initiate a new synchronization.

## 7.17 MANAGING ACCOUNT DATA FOR SYSTEM ACCESS

Each RFP provides different independent access types:

- The OMM Web service/HTTPS interface (see section 5);
- The OMP (see section 6);

The OMM Web service and the OMP are mainly used for configuration and administration.

- The OM Configurator (see section 7.6);
- The SSH user shell (see section 8.3.5).

The OM Configurator is mainly used for static local configuration of an RFP.

The SSH user shell is mainly used from experts for diagnosis.

Each of these access types uses the same account data.

The account data can be altered at the **User account** page of the OMM Web.

The OMM delivers all the necessary account data to all connected RFPs. The RFPs save the account data inside their permanent memory. This has some implications:

- An RFP out of the box uses the default account data as long as this RFP is not connected to the OMM.
- An RFP which was connected for at least one time with the OMM uses the account data from the OMM.
- When the account data are changed on the OMM, any not connected RFPs will continue to use the older passwords.

### 7.17.1 ACCOUNT TYPES

There are three different account types:

- **Full access:** This access type is the "normal" access for the configuration. Using this access it is allowed to configure the OMM and each RFP. On the SSH interface of an RFP this access type allows login for debug information e. g. "pinging" another RFP to check visibility.

The factory setting for this account is

Name: 'omm'  
Password: 'omm'  
Active: 'n/a'

- **Read-only access:** As the name suggests this access type is not allowed to configure any item of the OMM installation. This access type can only be used on the OM Web service. The account can be deactivated.

The factory setting for this account is

Name: 'user'  
Password: 'user'  
Active: 'yes'

- **Root (SSH only) access:** This access type is only applicable on the SSH interface of an RFP. Its purpose is to get detailed information e. g. parameters from the kernel. The access using this account type is not reachable from other hosts hence a login using the full access type is necessary.

263

The factory setting for this account is

Name: 'root'  
Password: '22222'  
Active: 'n/a'

**Please note:** It is highly recommended not to use the "Root (SSH only) access" account type. It is meant for technical support only.

### 7.17.2 POTENTIAL PITFALLS

When an RFP is configured via the OM Configurator and is taken out of an installation, the RFP may become unusable:

- When this RFP comes up, it finds a valid configuration in its permanent memory. It will hence skip DHCP for booting.
- But when this configuration is not valid anymore (e.g. the TFTP server has a new IP address meanwhile), the RFP isn't able to complete the boot and is hence not able to connect to the OMM.
- The RFP will not get newer passwords from the OMM.

It is therefore recommended to switch of the OM Configurator before taking an RFP out of an installation. But nevertheless the OM Configurator allows to reset the permanent memory of an RFP (the Mitel support must be connected).

## 7.18 WLAN CONFIGURATION

### 7.18.1 WLAN CONFIGURATION STEPS (RFP 42 WLAN / RFP 43 WLAN ONLY)

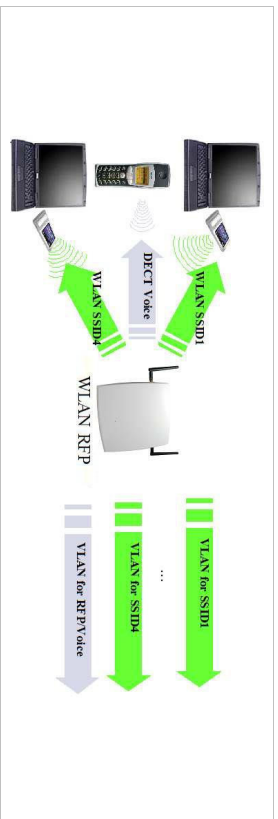
The correct configuration of an RFP with a WLAN interface requires the correct configuration of the DECT part. The second step is to specify the **Regulatory domain** of the WLAN network at the **System settings** page of the OMM web service (see section 5.4.1.3).

**WARNING:** Please note that selecting the incorrect regulatory domain may result in a violation of applicable law in your country!

Select one of the two-letter country codes. This setting depends on the country and is prescribed by the laws of that country. Only the setting prescribed for that country must be used.

The third step is to specify the WLAN parameters in a profile (see section 5.8.1). The WLAN profile determines the name (SSID) of the WLAN network and other parameters. The encryption and authentication procedures are especially important and must be planned carefully beforehand.

264



The access point can be assigned to a VLAN that conforms to 802.1q. All the data that is received from and that is to be forwarded to the WLAN clients is then carried by the configured VLAN. All other data, such as VoIP packets, configuration data or authentication data (Radius), is given the VLAN tag configured for the RFP. The switch port of the network component to which the access point is connected must be configured as a trunk port.

**Note:** The RFP 42 WLAN and RFP 43 WLAN must be connected at least via a 100BaseT Ethernet link in order to activate the RFP's WLAN function.

As a fourth step, you must assign a WLAN profile to a configured RFP. This can be done on the **DECT base stations** page of the OMM web service or on the **OMP DECT base stations -> Device list** page. Note that specific radio settings for the RFP, such as the channel, 802.11abgn mode, or antenna settings, are also done in this step.

**7.18.2 WLAN CONFIGURATION STEPS (RFP 48 WLAN)**

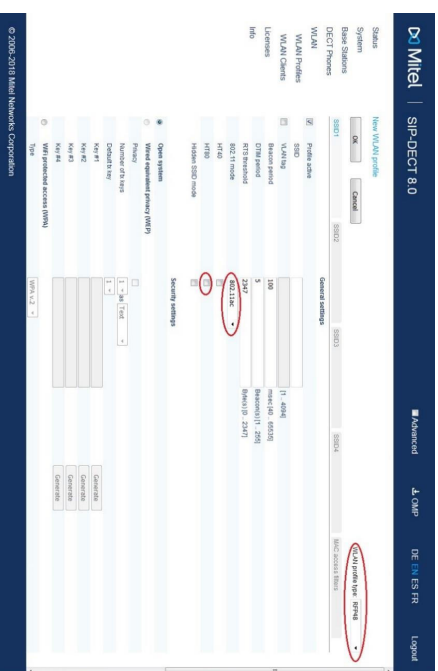
**7.18.2.1 Support of 802.11ac WLAN**

802.11ac is backwards compatible with 802.11a and 'n'. Like the RFP 43, the RFP 48 can only work in one WLAN spectrum at the same time (2.4 GHz or 5 GHz). Within the 2.4 GHz spectrum the WLAN module supports the 802.11b/g/n modes in the same way as the RFP 43:

- to enable the DFS channels: **System/System Settings (Advanced)**

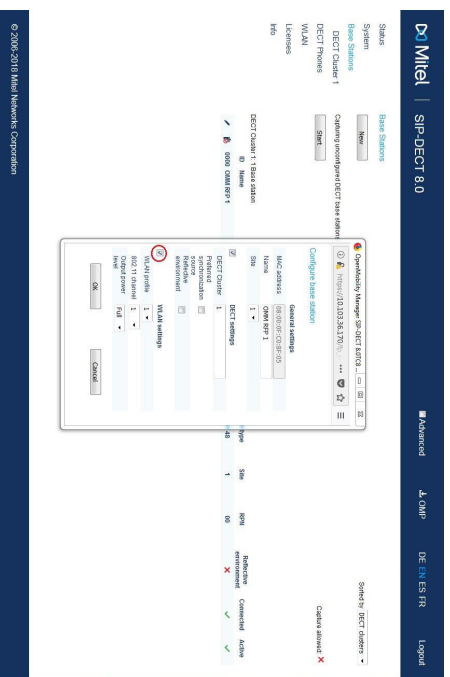


- to enable the ac mode and HT80: **WLAN/WLAN Profiles (new/edit)**



HT80 includes the HT40/HT20 bandwidth setting. A channel with a bandwidth of 80 MHz occupies 4 WLAN channels with a bandwidth of 20 MHz.

- to activate WLAN and to set the WLAN profile / channel / power level for a base station (edit):



The selected WLAN channels have a default bandwidth of 20 MHz. If the WLAN profile options HT80/HT40 MHz is activated, the necessary center channel is automatically selected. In the 2.4 GHz band, a channel with 40 MHz bandwidth is only established if no other 20 MHz channel is disturbed. Otherwise, a fallback to 20 MHz bandwidth will be made.

### 7.18.3 OPTIMIZING THE WLAN

#### Beacon Interval

Transmitting beacons requires transmission channel capacity. A shorted beacon interval increases the WLAN network's ability to detect signals, thus improving its availability. At the same time, it increases the network's ability to adjust the mutually negotiated signal strength. A longer beacon interval saves WLAN air time and also reduces the power consumption of mobile WLAN clients.

#### RTS Threshold

If the network throughput is low or if many retransmissions occur, the RTS/CTS handshake can be activated by reducing the RTS threshold value below 1500 byte. This can improve throughput, especially in environments where reflection and attenuation cause problems for HF.

#### Fragmentation Threshold

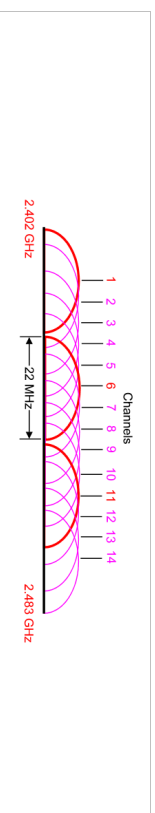
In environments where there is a lot of interference and poor radio quality, reducing the fragment size below 1500 bytes can improve the effective throughput. However, transmitted data frames must be fragmented, which means a higher load on the RFP's processor.

#### DTIM Period

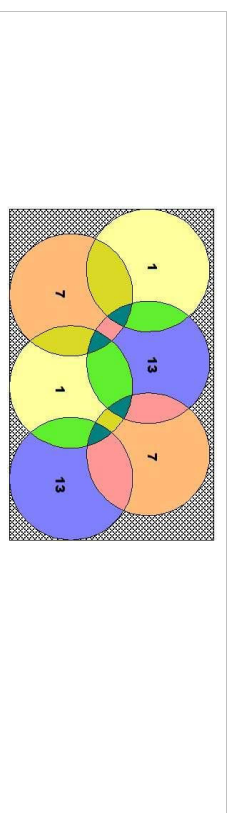
The DTIM period specifies the interval between transmissions of the broadcast and multicast packets. All WLAN clients must be active during this interval. Increasing the DTIM period lowers the client's power consumption slightly. Not all programs can manage the increase in response times, however.

#### Channel Allocation

Every WLAN RFP must be configured to a channel. You should ensure that the channel settings do not overlap. WLAN RFPs within range of each other should be configured at least five channels apart. When the radio field is planned, the WLAN RFPs of foreign WLANs that may be operating in the vicinity must be taken into account.



When planning the radio coverage for a two-dimensional area, please bear in mind that the distance between any two base stations operating on the same frequency must be at least twice their range. The range can be adjusted by lowering the output power level.



#### 802.11i: WPA2-Enterprise Pre-Authentication for fast Roaming

WLAN stations (e.g. laptop) which decide to roam to another WLAN access point (AP) must perform the full authentication process with the new AP. In 802.11x (RADIUS) networks this can take a long time resulting in network dropouts during the roam.

The AP share authentication information with other APs, so the station can authenticate faster (pre-auth) when roaming to a new AP. This method reduces network dropouts significantly.

The RFP 43 automatically enables pre-authentication for WPA-Enterprise enabled WLANs. The RFP 42 does not support this feature.

#### Channel Configuration Feedback for HT40 and Transmit Power

The HT40 channel configuration in 802.11n enabled networks may not always become active because of other access points that use channels that would overlap. In this case, the RFP 43 will fall back to HT20. The effective channel configuration and the transmit power are reported to the OpenMobility Manager.

Users can inspect these parameters using the WEB interface and the OMP and may change the channel to a frequency without overlapping APs.

#### Support of 802.11ac-WLAN for RFP 48 WLAN

The RFP 48 WLAN is a new WLAN module, which supports the WLAN ac mode wave 1. Within the 5 GHz spectrum, the ac mode is 2.5x faster as the 'n' mode of WLAN. The RFP 48 is 4x faster with comparison to the RFP 43 having two antennas. This is achieved by more efficient coding (256-QAM)

with more bandwidth (HT80) per channel and one more antenna (3x3 MIMO compared to the RFP 43; 2x2 MIMO).

For more information about data rates, see: <http://mcsindex.com/>

## 7.18.4 SECURING THE WLAN

In order to ensure that communication in the WLAN network is secure, several measures must be taken. Firstly, data packets transmitted via the openly visible radio interface must be encrypted, and secondly, all WLAN components that provide services must authenticate themselves.

There are different encryption methods available that you configure within the WLAN profile (see section 5.8.1). However, only the recent WiFi protected access (WPA) encryption offers sufficient security against possible intruders. You should not use the (older) WEP encryption for your company LAN.

Especially with larger WLAN installations, the single shared secret offered by WPA-personal may not be sufficient for your security requirements, because any person that connects to the WLAN needs to know the same shared secret. For this reason, you should also setup RADIUS authentication that is supported by all RFP 42 WLAN and RFP 43 WLAN devices.

A Radius Server (Remote Authentication Dial In User Service) handles 802.1x Authentication, thus authorizing different WLAN clients with an individual username / password combination to log in. We recommend a Radius Server with EAP-TLS (e.g. FreeRadius or MS Windows 2003 IAS Server) and a Certificate Authority (CA).

The RADIUS authentication takes place between the RADIUS server and the RADIUS client, with the WLAN RFP to pass-through this communication. You should refer to the documentation that comes with your RADIUS product for details on how to setup, maintain and operate the RADIUS system.

The WLAN module of RFP 48 supports Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC). These features are required for the radar detection (flight and weather) and are necessary to use the WLAN channels 52 – 140 in Europe and USA. If radar pattern detected, the RFP 48 changes its WLAN channel by itself to another channel without radar for a half hour. The 5GHz high band with its channels 149 – 165 is supported too.

## 7.19 SNMP CONFIGURATION

To manage a larger RFP network, an SNMP agent is provided for each RFP. This will give alarm information and allow an SNMP management system (such as "HP Open View") to manage this network. The SNMP agents can be configured in the **SNMP** menu of the OM Web service (see section 5.4.6).

All SNMP agents are configured by the OMM. Additional parameters that are valid for the individual RFP (e.g. "syslocation" and "sysName") are generated. The "syslocation" parameter corresponds to the location configured via the OMM web interface. The "sysName" parameter is generated using the MAC address and the RFP device type (e.g. RFP 43 WLAN). The RFP uptime can be requested by reading the "sysUpTime" parameter. This value indicates how long the RFP application software is running. It does not indicate the uptime of the operating system which does not correspond to the operational RFP state.

The SNMP agent responds to SNMPv1-read and SNMPv2c-read requests for the standard MIB-II objects. The Management Information Base (MIB-II) contains 11 object groups. The agent receives both SNMPv1 and SNMPv2c traps. It sends a "coldStart" trap when it first starts up. It also sends an enterprise-specific trap "nsNotifyShutdown" when it stops. When the SNMP agent receives an SNMP request using an unknown community name, it sends an "authenticationFailure" trap. The SNMP agent also generates an enterprise-specific trap "nsNotifyRestart" (rather than the standard "coldStart" or "warmStart" traps) after being reconfigured.

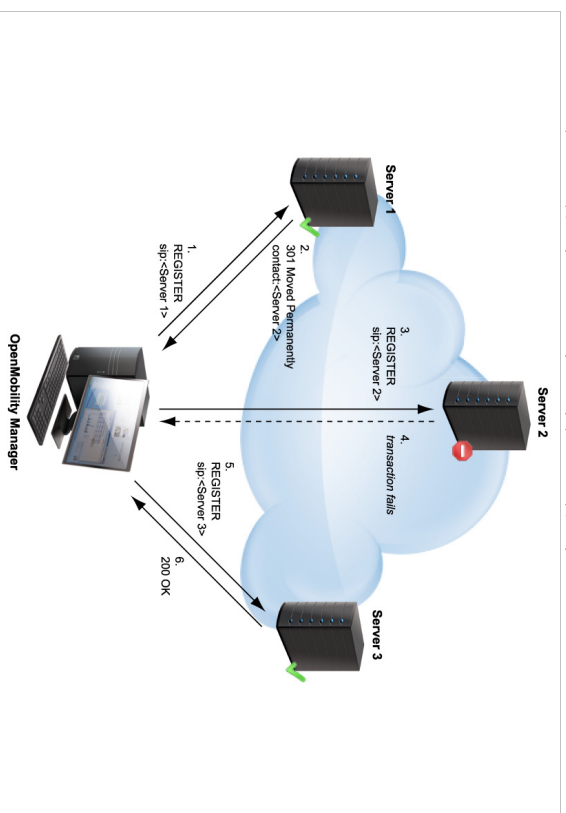
## 7.20 BACKUP SIP PROXY/REGISTRAR

This section provides an overview about the supported redundancy concepts with SIP-DECT to realize a high availability solution together with IPBX redundancy mechanism.

The focus of this section is IPBX redundancy. For information regarding OMM redundancy, see section 7.15.

### 7.20.1 REGISTRAR REDIRECT

To allow IPBX systems to spread the registration and call traffic over different servers the OMM supports 301 (Moved Permanently) or 302 (Moved Temporarily) responses for registrations. When a 301 or 302 response is received, the OMM follows the redirect and registers the concerning user to the given address. If more than one contact address are given in the 301/302 response, the OMM tries to contact the registrars successively until the registration succeeds. If the redirected registrar succeeds and if the configured proxy and registrar are identical, all subsequent INVITE requests are sent to the redirected server. In the other case all subsequent INVITE requests will be sent to the (outbound) proxy or secondary/tertiary (outbound) proxy.

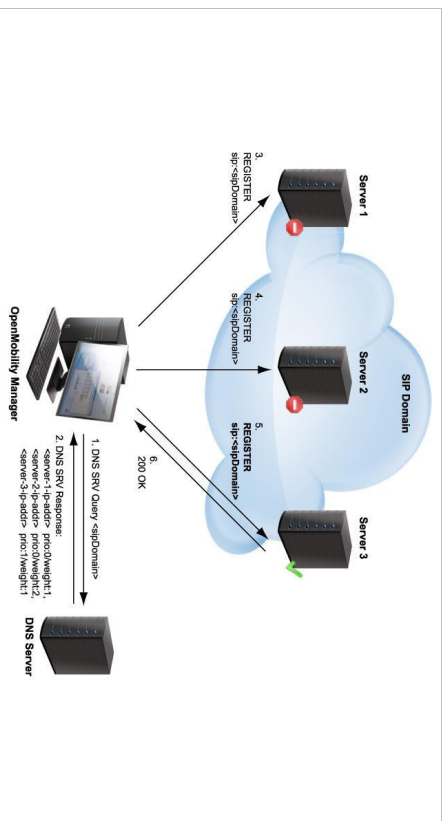


## 7.20.2 DNS SRV

If a full qualified domain name is configured as proxy, outbound proxy or registrar server and the respective port setting is set to zero ("0"), the OMM performs a DNS SRV query before an appropriate SIP transaction is started. Herewith the OMM locates a list of servers responsible for the given SIP domain. With this configuration, the default port ("5060") is used for every server address acquired with this mechanism.

The DNS SRV results are sorted by priority and weight in ascending order by the OMM. As soon as the DNS SRV query succeeds, the OMM starts the appropriate SIP transaction by sending the request to the server with the uppermost priority and weight of the DNS SRV result.

If there is no answer from the first SIP server in a configurable time frame ("Transaction Timer" parameter), or a 5xx response is received, it will be assumed as unreachable and the OMM tries to contact the next server of the DNS SRV result. Therefore the request will be sent to the second server of the DNS SRV query result. If there is also no answer in the given time frame or a 5xx response is received from the second server, the request will be sent to the third server and so on. When there is an answer other than 5xx from one of the contacted servers, this server will be used for this transaction.



To prevent situations where the OMM tries to contact with each new transaction servers which are unreachable (out of service), the OMM offers a blacklist feature. If there is no answer from a SIP server, this specific server can be put into a blacklist and will not be contacted anymore for a configurable time of "Blacklist time out" minutes by all adjacent SIP transactions.

In differentiation to the concepts described in the following sections note that independent of which SIP server is used, all requests sent by the OMM carry the same sender Address-of-Record (AOR)<sup>1</sup>. This

<sup>1</sup> RFC 3261: An address-of-record (AOR) is a SIP or SIPS URI that points to a domain with a location service that can map the URI to another URI where the user might be available. Typically, the location service is populated through registrations. An AOR is frequently thought of as the "public address" of the user.

means that the sender URI consisting of user-ID and domain is not changed during a failover to another server.

## 7.20.3 BACKUP SIP SERVERS

The SIP-DECT solution allows configuration of two additional levels of backup servers, in addition to the primary proxy, outbound proxy and registrar server. These two additional levels of backup servers are referred to as secondary and tertiary servers in the following sections.

| Configuration       | Intercomunicable                | Supplementary service | Conference                 | Security       | Outbound server |
|---------------------|---------------------------------|-----------------------|----------------------------|----------------|-----------------|
| Status              | Basic settings                  | Advanced settings     | Registration/white ringing | Basic settings | RTP settings    |
| System              | Secondary proxy server          | 10.35.124.89          |                            |                |                 |
| Basic settings      | Secondary proxy port            | 5060                  |                            |                |                 |
| Advanced settings   | Secondary registrar server      | 10.35.124.89          |                            |                |                 |
| SIP                 | Secondary registrar port        | 5060                  |                            |                |                 |
| Provisioning        | Secondary outbound proxy server |                       |                            |                |                 |
| User administration | Secondary outbound proxy port   | 5060                  |                            |                |                 |
| Data management     | Tertiary proxy server           |                       |                            |                |                 |
| Stakes              | DECT base stations              | 5060                  |                            |                |                 |
| WLAN                | Tertiary proxy port             |                       |                            |                |                 |
| Video devices       | Tertiary registrar server       |                       |                            |                |                 |
| DECT phones         | Tertiary registrar port         | 5060                  |                            |                |                 |
| Conference rooms    | Tertiary outbound proxy server  |                       |                            |                |                 |
| System features     | Tertiary outbound proxy port    | 5060                  |                            |                |                 |
| Licenses            | Failover keep alive             | 5 min                 |                            |                |                 |
|                     | Failover keep alive time        |                       |                            |                |                 |

SIP backup servers can be configured in the **System -> SIP** menu of the OM Management Portal (OMP), see also section 6.5.4.

You can configure IP addresses, names or full qualified domain names as server addresses. It is also possible to configure a mixture of IP addresses, names or full qualified domain names for the different servers.

If fully qualified domain names are configured and the respective port setting is configured to zero ("0"), DNS SRV queries are performed to locate a list of servers in the domain. It is assumed that all server addresses are specified by name or IP address. With fully qualified domain names, the behavior described in section 7.20.2 is performed in addition to contact the SIP servers in the given domain.

This redundancy mechanism is based on a failover concept where the OMM first tries to contact the primary server. If the primary server fails, the OMM tries to contact the secondary server and if the secondary server fails also, the OMM tries to contact the tertiary server.

The OMM failover behavior in detail depends on the backup server settings.

### 7.20.3.1 No Secondary/Tertiary Proxy, Outbound Proxy and Registrar Configured

In this case is no failover to a secondary/tertiary (outbound) proxy / registrar is possible.



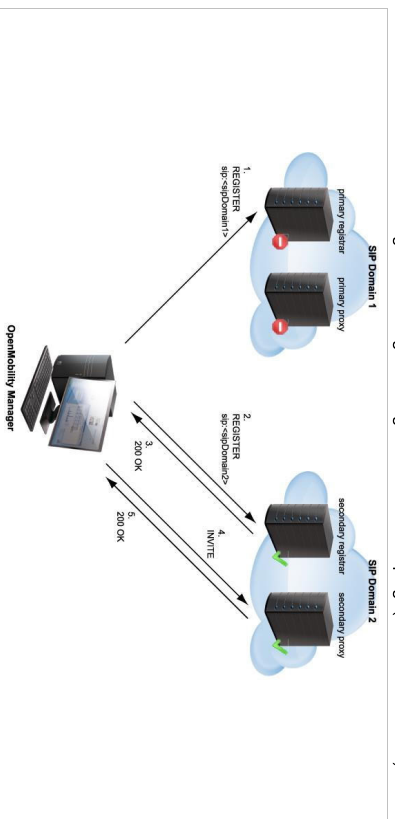
### 7.20.3.2 Secondary/Tertiary Proxy and Registrar Configured

All REGISTER and re-REGISTER requests attempt to use the primary registrar first.

If the primary registrar fails (e.g. no answer in "transaction timer" time frame), the user is tried to register with the secondary/tertiary registrar using as AOR the secondary/tertiary proxy address.

When the registration with the secondary/tertiary registrar succeeds:

- the MM/I subscription is moved to the secondary/tertiary proxy,
- all subsequent INVITE requests attempt to use the secondary/tertiary proxy,
- the registration of all other users currently registered with the failed server will be automatically refreshed if the "Failover keep alive" setting is enabled (see page 137). For this purpose, the re-registrar requests will be queued and proceed according to the settings for "Registration traffic shaping" (see section 5.4.3.5).



If a user was registered successfully with the secondary/tertiary registrar and can be registered again with the primary registrar e.g. during a re-registration:

- the MM/I subscription is moved back to the primary (outbound) proxy,
- all subsequent INVITE requests attempt to use the primary (outbound) proxy again,
- the registration of all other users currently registered with the secondary/tertiary registrar will be automatically refreshed.

As long as no successful registration exists, all INVITE requests attempt to use the primary (outbound) proxy as first.

If the INVITE request to the primary proxy fails, the INVITE request attempts to use the secondary/tertiary proxy. If an INVITE request fails (no answer in "transaction timer" time frame) send to a proxy identical with own registrar, the registration will be refreshed.

### 7.20.3.3 Secondary/Tertiary Proxy, Registrar and Outbound Proxy Configured

In this case, the OMM behavior is as described in section 7.20.3.2 but all requests for the secondary/tertiary proxy/registrar are sent through the outbound proxy.

### 7.20.3.4 Secondary/Tertiary Proxy Configured Only

All REGISTER, INVITE and SUBSCRIBE requests attempt to use the primary proxy or registrar first. If an INVITE/SUBSCRIBE request fails, the INVITE/SUBSCRIBE request attempts to use the secondary/tertiary proxy.

### 7.20.3.5 Secondary/Tertiary Outbound Proxy Configured Only

The OMM behavior is as described in section 7.20.3.2 but

- all requests for the secondary/tertiary proxy/registrar are sent through the outbound proxy,
- if the registration with the primary registrar fails, the registration is re-tried using the primary proxy address as AOR sent through the outbound proxy.

### 7.20.3.6 Secondary/Tertiary Registrar Configured Only

All REGISTER, INVITE and SUBSCRIBE requests attempt to use the primary proxy or registrar first. If a REGISTER request fails, the request attempts to use the secondary/tertiary registrar.

### 7.20.4 KEEP ALIVE MECHANISM

A keep-alive mechanism implemented in the OMM allows the automatic failover to secondary/tertiary servers or automatic coming back to primary servers. The keep-alive mechanism is based on the registration process and utilizes the special behavior that all REGISTER and re-REGISTER requests are sent to the primary registrar first.

The following configuration parameters are introduced: **Failover keep alive** and **Failover keep alive time**. These parameters are set in the OM Management Portal (OMP) on the **Backup settings** tab of the **System: SIP** menu (see page 137).

For each registration target, a user could be registered successful with, a keep alive procedure is started. For this purpose the first user registered successful on a registration target will be selected to re-register all "Failover keep alive time" before the registration period expires.

If the re-registration of this selected user detects that the current primary server fails, the registration of all users registered on the same server will be refreshed automatically. For this purpose the re-registrar requests are queued and proceed according to the registration traffic settings (see section 5.4.3.5 for OMM Web or section 6.5.4.3 for OMP).

If the re-registration of a selected user detects that the primary server is available again, the registration of all users registered on a secondary/tertiary registrar will be refreshed.

## 7.20.5 PRIORITIZED REGISTRATION

Depending on the settings for "Registration traffic shapping", the registration of a high number of users could need minutes. In effect single users could not be reachable for minutes during startup.

To guarantee a minimum blackout for very important people (e.g. emergency user) the registration of such people can be prioritized. Therefore a special user attribute VIP (very important person) is introduced. The corresponding option is set in the **SIP** tab of the DECT phone **Detail Panel** (see page 174).

## 7.20.6 MONITORING THE SIP REGISTRATION STATUS

The SIP registration status of a DECT phone user can be monitored by using the OpenMobility Management Portal (OMP). In OMP monitor mode you can view on which registrar a specific DECT phone user is registered and whether the server is a primary, secondary or tertiary server. To monitor the SIP registration status proceed as follows:

- 1 Launch the OMP (see section 6.1) and navigate to the **DECT Phones -> Overview** menu.
- 2 Switch to **Monitor Mode**.
- 3 Activate the **Registered**, **Registrar server type**, **Registrar server** and **Registrar port** columns (see section 6.10.9).

## 7.20.7 CONFIGURABLE USER ACCOUNT FOR STANDBY CHECK

The "Standby OMM" feature of SIP-DECT allows configuration of the user account to be used to check IPBX availability. Such an availability check starts automatically in fail over situations.

Therefore, the OMM starts a SIP registration for a specific DECT phone user and sends an OPTIONS request to the configured SIP proxy. If there is an answer, the SIP proxy/registrar is considered reachable and the standby OMM becomes active.

With older SIP-DECT releases, the OMM used the user account with the lowest phone number for the check procedure.

To select a specific user account for this purpose, enable the **Used for visibility checks** flag on the **SIP** tab when creating or editing a DECT phone.

**Please note:** The "Used for visibility checks" flag can only be set for one user. The number for visibility checks is shown in the OMP under **Status -> Users -> Number**.  
If the flag is not set for a specific user, the OMM uses the user account with the lowest phone number.

## 7.20.8 OMM STANDBY ENHANCEMENT

With SIP-DECT systems using the OMM standby feature it could happen in rare cases that both OMMs become temporarily active. In such a situation all SIP-DECT users were SIP registered from both OMMs to the configured PBX. This can cause problems, when the PBX accepts only one registration per user (non-forking proxy).

To prevent such problems a mechanism is realized to detect situations with two active OMMs. When such a situation is detected the remaining active OMM will SIP re-register all users to the PBX. This mechanism can be enabled/disabled via the **OMP SIP -> Supplementary Services** tab (see section 6.5.4.8).

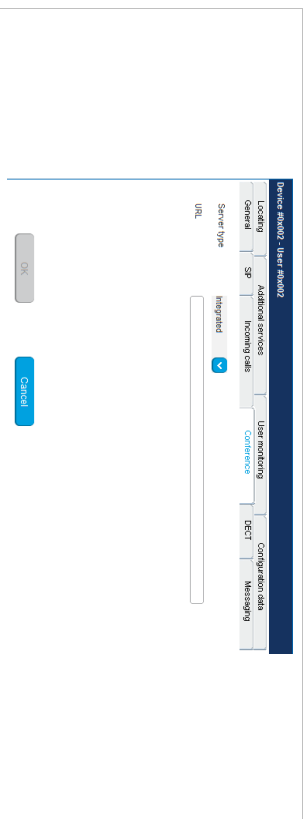
| Basic settings  | Advanced settings                   | Registration traffic shapping   | Backup settings                     | FTP settings | DNF settings       |
|---|-------------------------------------|---|-------------------------------------|--------------|--------------------|
| <b>Preconfig/Post-Check</b>   |                                     |   |                                     |              |                    |
| Call forwarding diversion   | <input checked="" type="checkbox"/> | Registration traffic shapping   | <input checked="" type="checkbox"/> | FTP settings | DNF settings       |
| Local fax handling  | <input checked="" type="checkbox"/> | When switched off, all 3 way events (hold, hold) in a call active state will be sent via SIP INFO as DTMF | Conference                          | Security     | Certificate server |
| Call transfer by hook (A-CDR)   | <input type="checkbox"/>            |   |                                     |              |                    |
| Call transfer by hook (local)   | <input checked="" type="checkbox"/> |   |                                     |              |                    |
| Truncate Caller identification after ""                                 | <input type="checkbox"/>            |   |                                     |              |                    |
| SIP registrar after 2 active OMMs failover                              | <input type="checkbox"/>            |   |                                     |              |                    |
| Repeat on fail  | <input checked="" type="checkbox"/> |   |                                     |              |                    |
| Call release timeout  | <input type="text" value="5"/> sec  |   |                                     |              |                    |
| Hold call release timeout   | <input type="text" value="5"/> sec  |   |                                     |              |                    |
| Failed call release timeout   | <input type="text" value="5"/> sec  |   |                                     |              |                    |
| <input type="button" value="OK"/> <input type="button" value="Cancel"/> |                                     |   |                                     |              |                    |

## 7.21 CONFERENCING

Depending on the type of conference server used, SIP-DECT offers the following operational modes:

- **None:** Neither external nor internal conference server is used.
- **Integrated:** The conference server integrated in SIP-DECT is used.
- **External:** An external conference server is used, e.g. Broadsoft or Syntro.
- **External – Blind Transfer:** A MinVoice Business conference server is used, whose proprietary SIP signaling requires that the initiation of the conference be signaled to the destination (as specified in the URL parameter) as a blind transfer.

The conference mode can be configured globally for all SIP-DECT users on the **OMP System -> SIP -> Conference** tab (see section 6.5.4.9). Alternatively, the conference mode for individual users can be configured on the **OMP DECT Phones -> Users -> Conference** tab (see section 6.10.4.4). When the **Global** setting is selected for a user, the global system conference mode will be used for this user.



The default for the global system conference mode is **None**. For the user-specific mode, the default is **Global**.

The global and/or user specific conference mode can also be configured via OMM configuration files or the OMM application XML interface (AXI).

### 7.21.1 CENTRALIZED CONFERRING

To enable SIP centralized conferencing on DECT phones select **External as Server type** for all users on the OMP's **System SIP** page or for specific users on the OMP's **DECT Phones -> Users** page. If there is specified a proxy / registrar server, then to reach the conference media server via the proxy server, set the **URI** field to one of the following prefixes:

- **Conf** (Sylantro server)
- **Conference** (Broadsoft server)

#### Examples

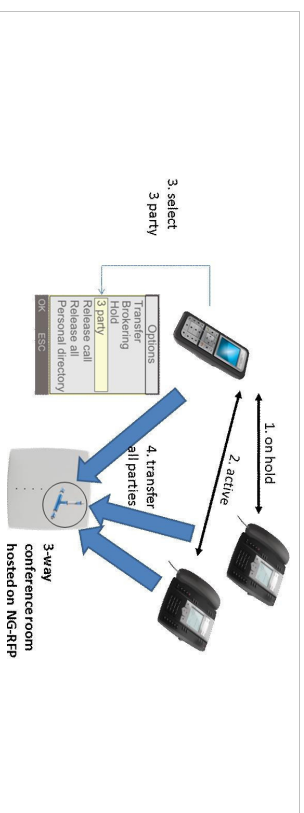
To set the **URI** field to "conf" or "Conference", specify "conf@<proxy-server-address><proxy-port>" or "Conference@<proxy-server-address><proxy-port>".

To reach the conference media server using a different address/port then that is specified by the proxy, set the **URI** field to "conf@<media-server-address><media-port>"

### 7.21.2 INTEGRATED CONFERENCE SERVER (ICS)

The conference server integrated in SIP-DECT is based on the SIP standard RFC 4579 and allows SIP-DECT users the ad-hoc initiation of 3-way conferences.

If this feature is enabled, it allows SIP-DECT users having an active call and holding another call to select **3 party** in the **Options** menu of a Mitel 600 DECT phone to initiate an ad-hoc 3-way conference. If a 3-way conference is initiated, the conference initiator and both connected parties are transferred to the next free conference room hosted on one of the RFP 35 / 36 / 37 / 43 devices. ICS provides the full range of voice codecs (G722, G711 µ-law, G711 a-law and G729) and supports trans-coding for all parties in a three-way conference session.



Enabling the SIP-DECT integrated 3-way conferencing requires the following configuration steps:

- Enable internal conference mode
- Select RFP devices for conferencing
- Configure conference rooms

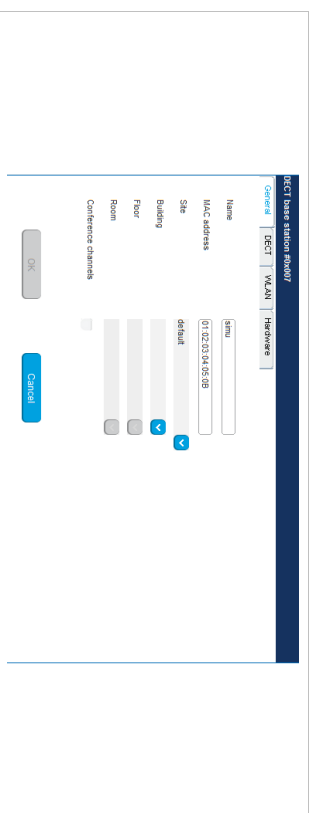
#### 7.21.2.1 Enable internal conference mode

To enable SIP-DECT internal 3-way conferencing for DECT phones select **Integrated as the Server type** setting for all users on the OMP's **System-> SIP** page or for specific users on the OMP's **DECT Phones -> Users** page.

#### 7.21.2.2 Select RFP devices for conferencing

Select some of the RFP devices from your SIP-DECT infrastructure to provide conferences. For this enable the **Conference cannels** flag for each selected RFP on the OMP's **DECT base stations -> Devices -> General** tab.

**Please note:** Only RFP 35 / 36 / 37 / 43 devices support 3-way conferences.



Depending on the DECT and G.729 configuration, an RFP device enabled for conferencing provides between 3 and 24 conference channels. To compute one 3-way conference 3 conference channels are necessary.

In particular, the G.729 codec, with its high consumption of computing time, reduces the number of available conference channels according to the following table.

| DECT enabled | Conferencing enabled | G.729 enabled | Conference channels | DECT voice channels |
|--------------|----------------------|---------------|---------------------|---------------------|
| Yes          | No                   | Yes/No        | 0                   | 8                   |
| Yes          | Yes                  | No            | 15                  | 8                   |
| Yes          | Yes                  | Yes           | 3                   | 5                   |
| No           | Yes                  | No            | 24                  | 0                   |
| No           | Yes                  | Yes           | 9                   | 0                   |

**Please note:** Activating the **Conference channels** option on an RFP with enabled DECT and in a system with enabled G.729 reduces the available DECT channels on that RFP from 8 to 5.

If the G.729 codec is not necessary on your /PBX platform, disable the G.729 codecs on the OMP's the **System: SIP** page / **RTP settings** tab to obtain the maximum number of conference channels.

The total number of conference channels in the SIP-DECT system is presented the OMP's **Status** -> **Conference** tab. The **Total** parameter provides the total number of conference channels in the system and the **Available** parameter provides the current number of available conference channels.

### 7.21.3 CONFIGURE CONFERENCE ROOMS

When a three-way conference is initiated by a SIP-DECT user, the initiator and the connected parties will be transferred to the next free conference room using SIP signalling. These conference rooms must be configured on the OMP's **Conference rooms** page with their SIP user id and SIP password (see section 6.11).

Configure as many conference rooms as necessary and as conference channels are available (3 channels per conference).

These conference rooms will be SIP registered on the configured SIP registrar and must be reachable via the configured SIP proxy for SIP signalling.

The following parameters can be configured for each conference room

- **Name:** SIP display name
- **Conference ID:** SIP user id
- **User Name:** SIP authentication name
- **Password:** SIP password
- **Fixed SIP port:** Port used explicitly for SIP signalling. If set to 0 (default), an automatically calculated port is used for this conference room. See section 3.17 for more information.
- **Calculated port:** Auto-calculated port used for SIP signalling (read-only). Only used if no value is specified for **Fixed SIP port**.

All configured conference rooms will be registered on the registrar / /PBX configured in OMM. If the **X-Aastra-id** info option is enabled on the OMP's **System: SIP** -> **Advanced settings** tab, a private X-Aastra-id header is sent out which identifies that these are conference rooms.



The X-Aastra-Id header has the following format for all conference rooms:

X-Aastra-Id: {type="29" model="01" version="1.0.0" }

The header's attributes have the following properties:

**type**

- the type parameter contains the phone type
- the value for all SIP-DECT conference rooms is "29"
- type = DQUOTE (\*2HEXDIG) DQUOTE

**model**

- it's the model of the terminal
- the value for all SIP-DECT conference rooms is "01"
- model = DQUOTE (\*2HEXDIG) DQUOTE

**version**

- the version is intended for later releases
- the value for all SIP-DECT conference rooms is "1.0.0"
- version = DQUOTE (\*16token) DQUOTE

**7.22 DOWNLOAD OVER AIR**

The "Download Over Air" feature allows updating the DECT phone firmware without any user interaction or interruption of the telephony services over the existing DECT air interface. This feature is currently available for the Mitel 600 DECT Phones.

With SIP-DECT 6.0 and later, the SIP-DECT RFP software image (iprf3G.dnd) contains the Mitel 600 DECT phone software. If the RFP houses the OMM, the OMM uses this software to update the DECT phones. The RFP OMM no longer automatically attempts to load a DECT phone software image from a RFP software URL when provided via DHCP or local configuration.

For specific maintenance purposes only, SIP-DECT allows configuration of a URL via the OMM Web service or OMP to use an alternative DECT phone software image (see section 5.4.1.6). The Mitel 600 DECT phone firmware packages are delivered in the "600.dnd" file for the OMM running on an RFP.

**7.22.1 HOW "DOWNLOAD OVER AIR" WORKS**

If the "Download over Air" feature is activated (see section 5.4.1.6), the OMM acts as a download server that provides the firmware for downloads.

The DECT phone sends its firmware version within the DECT attachment procedure. If the firmware version does not match the version provided by the OMM, the DECT phone will be queued into the update-queue. Later on the queued DECT phones will be paged to establish a download connection. After the connection is established, the OMM sends its actual DECT phone firmware version and the DECT phone will request a DECT phone description file. After receiving the DECT phone description file, the DECT phone decides which files are missing or must be updated. If files are missing or must be updated the DECT phone initiates the download procedure.

The OMM takes care of the following download scenarios automatically:

- If a DECT phones becomes unreachable e.g. when the DECT phone is switched off, the OMM will update the DECT phone when the DECT phone becomes available again.
- The OMM will take care of the software download while the user is moving between base stations (roaming) and location areas.
- The OMM has the capability of resuming a download from the point where it was last interrupted (e.g., the user leaves the coverage area during download or the DECT phone runs out of battery power).
- The OMM updates new DECT phones subscribed to the system.
- While the DECT phone is barred (e.g. low battery or "Download over Air" is disabled at the local menu), the download will be postponed.

The download happens without any user intervention. During the download, the telephony services, the roaming- and handover procedures are still available. The download stops automatically when e.g. the DECT phone leaves the coverage area or the RFP gets busy. The download resumes automatically when the stop cause is solved.

The Mitel 600 DECT phones have two partitions in the internal flash memory to hold 2 different software versions. During the download the new firmware is written to one partition and the DECT phone is running from the other partition.

After the download is successfully completed, the new firmware will be activated when the DECT phone is in the idle state.

The download of a single DECT phone with a firmware of 1 MB takes approximately 90 minutes. The number of DECT phones which can be downloaded depends on the available system resources.

The number of simultaneous downloads is limited per OMM (RFP: 30, PC: unlimited) and per RFP (6, decreased with each call).

The "Download over Air" service is delayed after a system startup for a while to allow the whole DECT system to become active. This may last several minutes.

### 7.22.2 HOW TO CONFIGURE "DOWNLOAD OVER AIR"

This section describes configuration of the "Download Over Air" feature via the OM Web service. The feature can also be configured using the OM Management Portal (OMP).

The "Download over Air" feature can be activated or deactivated on the **System Settings** web page (see section 5.4.1.6).

In the OMP, you can enable the "Download over Air" feature in the **System** -> **Advanced settings** -> **PP firmware** tab (see section 6.5.2.3).

If the "Download over Air" feature" is activated, the status of the **Activate firmware update** parameter is shown as enabled, service together with some statistics is displayed in the **DECT phones** section of the **Status** web page.

| DECT Phones                              |                                      |
|--|--------------------------------------|
| Total number                             | 64                                   |
| Subscribed                               | 4                                    |
| Subscription allowed                     |                                      |
| Activate firmware update                 |                                      |
| Loading firmware from                    | http://10.37.18.35/600_and           |
| Firmware version                         | !800_5.00_SPS_RCT1_!850_602_6.0_RCT8 |
| Number of known downloadable DECT phones | 4                                    |
| Number of already updated DECT phones    | 4                                    |

The DECT phone firmware container for DECT phone firmware update over the air includes packages for the Mitel 600 DECT phones. The available versions are also displayed on the **Status** web page.


**Please note:** The "Loading firmware from" on the OpenMobility Manager **Status** web page is only updated on restart of the OpenMobility Manager. Changing the location while the OpenMobility Manager is running has no effect.

The individual download status of each DECT phone is shown on the **DECT Phones** web page.

| Status          |              | Subscribed with configured IPES |               | Auto-create on subscription |          |
|-----------------|--------------|---------------------------------|---------------|-----------------------------|----------|
| System          | System       | Start                           | Start         |                             |          |
| Slices          |              |                                 |               |                             |          |
| Base Stations   |              |                                 |               |                             |          |
| DECT Phones     |              | Wi-Fi over subscription         | Start         |                             |          |
|                 |              | 2 min                           |               |                             |          |
| WLAN            |              |                                 |               |                             |          |
| System Features |              |                                 |               |                             |          |
| Info            |              |                                 |               |                             |          |
| Licenses        |              |                                 |               |                             |          |
|                 | Display name | Number/SIP user name            | IPES          | Subscribed                  | Download |
|                 | c2502-612d   | 2502                            | 1024-001839 * |                             |          |
|                 | c2503-620d   | 2503                            | 0368-062116 0 |                             |          |
|                 | c2504-620d   | 2504                            | 0368-062046 7 |                             |          |
|                 | 4202-620d    | 4202                            | 0368-062129 3 |                             |          |
|                 | senu pr 0    | 25001                           | 0010-000000 3 |                             | -        |
|                 | senu pr 1    | 25002                           | 0010-000001 4 |                             | -        |
|                 | senu pr 2    | 25003                           | 0010-000002 5 |                             | -        |
|                 | senu pr 3    | 25004                           | 0010-000003 6 |                             | -        |
|                 | senu pr 4    | 25005                           | 0010-000004 7 |                             | -        |
|                 | senu pr 5    | 25006                           | 0010-000005 8 |                             | -        |

The details in the **Download** column have the following meaning:

| Icon           | Meaning   |
|----------------|---|
| -              | Impossible to download the firmware to that DECT phone (e.g. not a Mitel 600 DECT phone)  |
|                | The DECT phone is paged to establish a download connection. In case of a successful connection establishment the DECT phone calculates the number of bytes to download. This may take several seconds.  |
| xx kbytes left | The download is ongoing and xx kbytes are left.   |
|                | The firmware of this DECT phone is up to date.  |
|                | The DECT phone is queued in the update-queue for updating (pending).  |
|                | Warning <ul style="list-style-type: none"> <li>- The download is barred because of one of the following reasons:                             <ul style="list-style-type: none"> <li>- The DECT phone is busy (temporary status).</li> <li>- The battery power is lower than 50% and the DECT phone is not connected to the docking station or the USB interface.</li> </ul> </li> <li>- This is not the master download system. A DECT phone can be enrolled on several OpenMobility systems. The first system to which the DECT phone will be enrolled is the "master system". The DECT phone downloads only from the "master system". A different "master system" can be chosen inside the local menu of the DECT phone.</li> <li>- The download is disabled in the local menu of the DECT phone.</li> </ul> The specific reason is shown as a tooltip. |
|                | Error <ul style="list-style-type: none"> <li>- The download failed because of one of the following reasons:                             <ul style="list-style-type: none"> <li>- checksum error,</li> <li>- file system error,</li> <li>- error while writing firmware to flash,</li> <li>- version mismatch,</li> <li>- error while expanding firmware container.</li> </ul> </li> </ul> The specific reason is shown as a tooltip.  |

| Icon   | Meaning  |
|--|--|
|  | Info   |
|  | The download is not possible because: <ul style="list-style-type: none"> <li>– the DECT phone is not reachable</li> <li>– the DECT phone is detached</li> </ul> The specific reason is shown as a tooltip. |

In the OMP, the “Download over Air” service status is displayed in the **Status** menu (see section 6.4).

## 7.23 CENTRAL DECT PHONE CONFIGURATION OVER AIR (COA)

Centralized DECT phone configuration over the air is supported for Mitel 602 DECT phones.

Configurable parameters include:

- settings (loudness, contrast, etc)
- menu items (switch on or off, enable password protection)
- key assignments (including an override of manual key programming)
- variable lists

DECT phone configuration over air (COA) is useful for deployment of special configuration to a single DECT phone or a large number of DECT phones. No local access to the DECT phone is required. DECT phone COA is implemented by providing additional configuration information to the well-known configuration files or providing profiles via OMP. Configuration can be changed at the device level (DECT subscription) or the user level (based on login).

Configuration of all DECT phones with a predefined default profile is also supported. Up to 20 DECT phone profiles make it easy to adapt to different usage scenarios for heterogeneous user groups (e.g. nurses and doctors in hospital environments).

**IMPORTANT :** This feature requires 6.00 DECT phone software or later.  
**IMPORTANT :** Centralized DECT phone configuration over the air is only available on the Download over Air (DoA) master system.

### 7.23.1 CONFIGURATION FILES

You can use three kinds of configuration files:

- Default DECT phone configuration profile
- Default configuration file used for all suitable DECT phones. The configuration is loaded into the DECT phone when subscription is complete, even if a user has not logged in to the device.
- DECT phone configuration profiles
- User-focused DECT phone configuration file used for a group of users. The configuration is loaded into the DECT phone when a user belonging to this group logs in to the device.
- DECT phone user individual configuration settings
- Individual DECT phone configuration settings used for a single user. The configuration is loaded into the DECT phone when the user logs in to the device.

The system consolidates the DECT phone settings before loading the configuration settings for a logged-in user into the DECT phone. Settings from DECT phone profiles overwrite default configuration settings, and individual user configuration settings overwrite DECT phone profiles and default configuration settings. For a complete list of supported settings, see section 10.4.

Configuration can be completed by using OMP (file import and download configuration settings) and user configuration files (user\_common.cfg and <user.cfg files), wherein a list of user-friendly settings can be used for the DECT phone configuration.

**Please note:** Deleting or overwriting configuration files on a DECT phone does not restore configuration to default or previous settings. Configuration elements that are not part of the new downloaded configuration file persist. To restore all settings, the administrator must initiate a power off/on at the DECT phone or use a default configuration file that contains all relevant settings.

To avoid interfering with the telephony or message service (especially with respect to alarm messages within the SIP-DECT system), only one configuration data download to the DECT phone is performed at a time. Therefore, changing the default profile settings or other profile settings may take some time in a large system, until all the related DECT phones are updated.

### 7.23.2 CONFIGURATION FILE DOWNLOAD TO DECT PHONES

Profiles are downloaded to the DECT phone via the messaging mechanism, in conjunction with the internal message type “CONF OVER AIR”. This occurs in parallel with general message transfer to the DECT phone, and the lowest priority is used to ensure that the download does not interfere with the delivery of urgent messages. The message mechanism is also used to confirm a successful profile download, through AXI events.

Profile downloads to DECT phones are limited system-wide to a maximum of one download at a time to ensure no interference with OMM system operation. You can view the download on the OMM console (console command `hcm`). The download state is also part of the system dump.

#### 7.23.2.1 Download Triggers

The OMM maintains a profile download list for all DECT phones that have configuration data to be set. These DECT phones are stored with the checksum of configuration data to be set. A DECT phone is included in this list when:

- the OMM system starts up and the associated DECT phone has configuration data to be set
  - the associated DECT phone’s configuration data changes (this is communicated via AXI), such as:
    - change in the default configuration profile
    - change in the configuration profile for the user of the associated DECT phone
    - change in the individual user configuration profile for the user using the associated DECT phone
    - change in the configuration profile assigned to the user using the associated DECT phone
- Profile downloads to the DECT phones (as maintained in the profile download list) are scheduled at regular intervals. A new download to DECT phones in the profile download list is scheduled when:
- a configuration change occurs on the DECT phone (via AXI notification)

- a location registration is received, and the checksum of the configuration data stored in the profile download list is different from the checksum sent in the location registration
- a download to a DECT phone completes

### 7.23.3 COA CONFIGURATION USING OMP

OMP configuration of DECT phones is restricted. You can do the following through OMP:

- List the current user and device state via the **DECT Phones -> Overview** menu and **DECT Phones -> Devices -> Configuration data** tab (in Monitoring mode)
- Import the default profile and one to 20 individual profiles via the **System features -> COA profiles** menu (see section 6.12.8)
- Assign one of 20 profiles to an internal user via the **DECT Phones -> Users -> Configuration data** tab (see section 6.10.4.10)

The syntax of the profiles that can be imported by the OMP is the same as that specified for the user\_common.cfg and <user>.cfg files.

**Please note:** COA configuration via OMM Web service is not supported. You can only list the current user and DECT phone state in the "User and DECT phone configuration and status data summary".

### 7.23.4 CONFIGURATION USING USER\_COMMON\_CFG/USER\_CFG FILES

The user\_common.cfg and <user>.cfg configuration files are used for DECT phone configuration. The following configuration attributes in the user\_common.cfg file control central DECT phone configuration:

- **Default profile settings**

```

OM_Profile.0.Default.<key>=<values>
...
OM_Profile.0.Default.<key>=<values>

```
- Where "Default" is the reserved name for the default profile, and <key> is one of the configuration settings with its <values> to be set.

**Example:**

```

OM_Profile.0.Default.UD_DisplayLang="en"
OM_Profile.0.Default.UD_DisplayFont="large"
OM_Profile.0.Default.UD_DisplayColor="black"
...
    • one of up to 20 profile settings
OM_Profile.<no>.<name>.<key>=<values>

```

Where <no> is the number of the profile, <name> is the name of the profile to be configured, and <key> is one of the configuration settings with its <values> to be set.

**Example:**

```

OM_Profile.5.Doctor.UD_DisplayLang="en"
OM_Profile.5.Doctor.UD_DisplayFont="large"
OM_Profile.5.Doctor.UD_DisplayColor="black"

```

**Please note:** To assign a profile to a user, you can use the UD\_PpProfileId= <profileNo> setting in <user>.cfg files. When <profileNo> is 0, no profile or (depending on configuration) the default profile is used. The default profile is defined in user\_common.cfg.

**Please note:** A complete removal of a profile from user\_common.cfg does not remove the profile in the OMM database. It must be explicitly deleted in the OMM database.

For individual user DECT phone configuration settings, the following configuration attributes are available in the <user>.cfg file:

- User configuration settings

```
<key>=<values>
```

```
<key>=<values>
```

Where <key> is one of the configuration settings with its <values> to be set.

**Example:**

```

UD_DisplayLang="en"
UD_DisplayFont="large"
UD_DisplayColor="black"

```

#### 7.23.4.1 CoA Example

```

UD.ConfigurationName = "omm-test"
UD.DisplayLang="en"
UD.DisplayFont="small"
UD_DisplayColor="black"
UD_RingerMelodyIntern="ringing_1"
UD_RingerMelodyExtern="ringing_2"
UD_RingerVolumeIntern="increasing"
UD_RingerVolumeExtern="increasing"

```

Configuration file is named "omm-test"  
 Language is set to English  
 Display font is set to small  
 Display color scheme is set to black  
 Internal call melody is set to melody "ringing\_1"  
 Internal call melody is set to melody "ringing\_2"  
 Internal call finger volume is set to increasing  
 External call finger volume is set to increasing

See section 10.4 for a full list of supported CoA configuration parameters.

### 7.23.5 VARIABLE LISTS

The Mitel 602 DECT phone 6.1 firmware introduces variable lists. A variable list includes a number of items, each of which corresponds to an action to be performed on the DECT phone.

A list item consists of an index identifier (1..10) and either a number (to be dialed) or a function/feature that is supported by the DECT phone. Other attributes are optional. If there is a FunctionID, the entry does not have a sub key line in the variable list. If there is a number and a FunctionID the DECT phone executes the associated action (if available); otherwise, the DECT phone dials the number.



| Item Attribute   | Type                         | Description   | Example        |
|------------------|------------------------------|---|----------------|
| Index            | Decimal number               | Index of list item (1..10)                            | 7              |
| Number           | quoted UTF8-string           | Number to dial  | "\x2312777"    |
| Name             | quoted UTF8-string           | Text displayed for item                               | "My Voice Box" |
| FunctionID       | Function-ID-string           | Function or feature to execute                        | pxx_directory  |
| ShortName/icon   | quoted UTF8-string           | Short name and/or icon displayed                      | "\xEE808B VB"  |
| Handstree        | Boolean ("0" or "1")         | Dial in hands-free mode                               | 1              |
| VisibleSpecifier | 4 digit string of "0" or "1" | Item visible in idle, dial, alerting and active state | 1000           |

The COA profile supports two variable lists for each DECT phone. Each list can contain up to 10 items.

Use the UD\_VListEntry configuration command to configure an item for one of the lists. The first value specifies the index (1 or 2) of the list, followed by the attributes listed above.

The values-attribute pairs must be separated by a space and their position in the configuration command are fixed. Unused attributes (empty strings) can be omitted at the end of the configuration command. Unused attributes (empty strings) can be omitted at the end of the configuration command.

A variable list can hold a name and/or short name (used to represent it in another list or near a programmed soft key or side key). The 'short name' attribute also allows you to specify an icon. A third attribute, 'sub item', determines whether or not subitems (sub key lines) of a list are displayed. By default, the subitem (sub key line) is only displayed if the item is selected.

| List Attribute | Type               | Description                        | Example       |
|----------------|--------------------|------------------------------------|---------------|
| Name           | quoted UTF8-string | Text displayed for list            | "My Own Menu" |
| ShortName/icon | quoted UTF8-string | Short name and/or icon displayed   | "\xEE808B M1" |
| Subitems       | Boolean (0 or 1)   | Show sub-key line of selected item | 1             |

**Examples:**

```
#PBX Menu using COA variable list
UD_ConfigurationName=PBX Menu

#Key assignment (function: vlist1 and vlist2)
UD_KeyAssignmentId=esc vlist1

#Menu Design
UD_VListName = 1 "Call services" #Title
UD_VListShortName = 1 "More" #Softkey
UD_VListSubItems = 1 0 #Display Details per Item

## PLACEHOLDERS to add into Number field:
#<no> will be replaced with a number from handset editor e.g. "*"12"<no>#"
```

```
#<dial> will be replaced with a number from handset editor or directory, caller-list...
#<t=> following dial-digits will be delayed for ... ms e.g. <t=3000ms>
#<inf=> get info-box with ... string for (3000ms) continue dialing after info box e.g.
#<inf=please wait>
#<r=> call will be released after ... ms e.g. <r=10000>
#<close> will close this Menu.

## Entry: UD_VListEntry = List Index "Number" "Name" FunctionID "ShortName" Handstree
# Visible
# ITEM TYPE DESCRIPTION
# List decimal number item belong to variable list (1..2)
# Index decimal number index of list item (1..10)
# Number quoted UTF8-string number to dial "\x1234" (use \x23 for #)
# Name quoted UTF8-string displayed text of item "My Voice Box"
# FunctionID function-ID-string function/feature to execute e.g. pxx_directory
# (if available, preference over number)
# ShortName quoted UTF8-string displayed short name and/or icon
# Handstree Boolean (0 or 1) dial in hands-free-mode
# Visible 4-digit-string of 0 or 1 item visible in idle, dial-, alerting- and active-state e.g.1000
# notice: to skip a parameter in the row use "" (even if the type is unquoted)

## idle menu functions
#Call Forward **8 (predial) + number
#Call Forward Cancel #8 (dial)
#Do Not Disturb #5 (dial)
#Do Not Dist. Cancel #5 (dial)
#Call Pickup *6 (dial)
#Call Park Retrieve *8# (predial) + number
#Direct/Group Page *37 (predial) + number
#Loudspeaker Page **9 (dial)

UD_VListEntry = 1 1 ""*8<dial>\x23<inf=call FWD enabled><r=2000>"Call Forward" "" ""
UD_VListEntry = 1 2 "\x23\x238<inf=call FWD off><r=1000><close>" "Call Forward Cancel" ""
"" ""
UD_VListEntry = 1 3 ""*5<inf=DND enabled><r=1000><close>"Do Not Disturb" "" ""
UD_VListEntry = 1 4 "\x235<inf=DND off><r=1000><close>" "Do Not Dist. Cancel" "" ""
UD_VListEntry = 1 5 ""*6<close>" "Call Pickup" "" "" ""
UD_VListEntry = 1 6 ""*8\x23<dial>"Call Park Retrieve" "" "" ""
UD_VListEntry = 1 7 ""*37<dial>"Direct/Group Page" "" "" ""
UD_VListEntry = 1 8 ""*9<close>"Loudspeaker Page" "" "" ""
```

**7.23.5.1 Icon coding**

The following table lists the UTF8-codes for Mitel 602 DECT phone icons.

| ICON | UTF8-Code | Description                 |
|------|-----------|-----------------------------|
|      | \XEE8083  | Arrow Up                    |
|      | \XEE8084  | Arrow Down                  |
|      | \XEE8085  | Arrow Left                  |
|      | \XEE8086  | Arrow Right                 |
|      | \XEE8088  | Fox Key                     |
|      | \XEE80B0  | Locked                      |
|      | \XEE80BC  | Search                      |
|      | \XEE80BE  | Info                        |
|      | \XEE81A5  | Attention                   |
|      | \XEE80BA  | Tip                         |
|      | \XEE808A  | Telbook Private number      |
|      | \XEE808B  | Telbook Mobile number       |
|      | \XEE808C  | Telbook Business number     |
|      | \XEE818C  | VIP number                  |
|      | \XEE808D  | Telbook Fax number          |
|      | \XEE808E  | Telbook Email address       |
|      | \XEE808F  | Telbook Name                |
|      | \XEE809B  | Hook off / Predial          |
|      | \XEE809C  | Hook on / Release           |
|      | \XEE81B0  | Register-recall             |
|      | \XEE8092  | DTMF                        |
|      | \XEE8182  | 3-party                     |
|      | \XEE80A0  | List Incoming call list     |
|      | \XEE80A1  | List Outgoing call list     |
|      | \XEE8196  | List Private directory /    |
|      | \XEE8199  | List Central directory      |
|      | \XEE818C  | List VIP                    |
|      | \XEE8181  | List Filter / Call Filtered |
|      | \XEE80A1  | Call outgoing               |
|      | \XEE8099  | Call Waiting                |
|      | \XEE80A7  | Call Rejected               |
|      | \XEE81AD  | Call SOS                    |

| ICON | UTF8-Code | Description                 |
|------|-----------|-----------------------------|
|      | \XEE809D  | Call Headset autoanswer     |
|      | \XEE8098  | Call Loudspeaker autoanswer |
|      | \XEE809B  | Call Hook autoanswer        |
|      | \XEE80B8  | Call deflected              |
|      | \XEE80A3  | Call missed                 |
|      | \XEE80A4  | Call answered               |
|      | \XEE8195  | Call on Voicebox            |
|      | \XEE81AE  | Call VIP                    |
|      | \XEE81B1  | Pickup                      |
|      | \XEE8296  | Pickup select               |
|      | \XEE80BF  | Call Park                   |
|      | \XEE8298  | Call protection             |
|      | \XEE8292  | Call routing                |
|      | \XEE8292  | Callback                    |

### 7.23.5.2 Number string coding

Note that the number specified in the list item may include one or more placeholders, so that, for example, the user can enter a number before the number is dialed. The placeholder keywords are specified in angle brackets ("`<>`").

If the dialed number includes angle brackets, you must use "`<<>>`".

| Number Placeholder | Description   |
|--------------------|---|
| <no>               | If the number strings consists of <no>, it is replaced with a number from the DECT phone editor   |
| <dial>             | If the number string consists of <dial> it is replaced with a number from the DECT phone editor or directory, caller-list. For example: <code>**12&lt;no&gt;#&gt;</code> -> ok <edit-number> send cc=info"12"<edit-number># (numbers may include letters like abcd... if the system supports alpha dialing) |
| <close>            | All parents (e.g. a list from which this item is started) are closed  |
| <f...>             | Following dial-digits are delayed for ... ms e.g. <f=3000ms>  |
| <inf...>           | Set info-box with ... string for (3000ms) continue dialing after info box ( e.g. <inf=Please wait>)   |
| <r...>             | Call is released after ... ms e.g. <r=10000>  |

## 7.24 EXTENDED DECT PHONE INTERFACE

With SIP-DECT 6.0 and later, the Mitel 600 DECT phones include an **Administration** menu that offers administrative functions to the user such as login, logout, and configuration and status summary display. The menu is available as an option under the **System menu** which can be accessed via the main menu of the DECT phone, or directly by a long press of the right soft key “>>>”.

**Please note:** The **Administration** menu is only available on Mitel 600 DECT phones, version 4.0 or higher.

The following table summarizes the options under the **Administration** menu. The menus allow basic OMM configuration and require a login (the same account and password as used for administrative access via OMP or Web service).

| Menu option           | Description   | OMM login   |
|-----------------------|---|-------------|
| 1. Login              | User can log in to the DECT phone (free DECT phone only)                                  |             |
| 2. Logout             | User can log out of the DECT phone (free DECT phone only)                                 |             |
| 3. PP state           | Display user/device configuration and status data summary (see section 5.7.6 for details) |             |
| 4. Sync user data     | Refresh SIP registration and synchronize user data, if they are stored externally         |             |
| 5. Sync system data   | Reload configuration and resource files   | Yes         |
| 6. System credentials | Set authentication for provisioning servers (see section 7.8.6.1)                         | Conditional |
| 7. Status             | Display basic OMM network settings (e.g., DHCP, IP addresses)                             |             |
| 8. System             | Set basic OMM system data   | Yes         |
| 9. SIP users/devices  | Perform basic configuration of users and DECT phones                                      | Yes         |
| 10. Version           | Display current OMM software version  |             |

The options available depend on the DECT phone state and the OMM platform (i.e., RFP OMM or Linux Server). The following table summarizes the options under the **Administration** menu according to device state and OMM platform.

| Menu option         | Fixed device | Logged out | Logged in | RFP OMM | Linux Server OMM |
|---------------------|--------------|------------|-----------|---------|------------------|
| 1. Login            |              | √          |           | √       | √                |
| 2. Logout           |              |            | √         | √       | √                |
| 3. PP state         | √            |            | √         | √       | √                |
| 4. Sync user data   | √            |            | √         | √       | √                |
| 5. Sync system data | √            | √          | √         | √       | √                |

293

|                       |   |   |   |   |
|-----------------------|---|---|---|---|
| 6. System credentials | √ | √ | √ | √ |
| 7. Status             | √ | √ | √ | √ |
| 8. System             | √ | √ | √ | √ |
| 9. SIP users/devices  | √ | √ | √ | √ |
| 10. Version           | √ | √ | √ | √ |

The following table summarizes the submenus available according to the OMM platform.

| Submenu                | SIP-DECT | RFP OMM | Linux Server OMM |
|------------------------|----------|---------|------------------|
| 1. System name         | √        | √       | √                |
| 2. Date and Time       | √        | √       |                  |
| 3. SIP                 | √        | √       | √                |
| 4. User administration | √        | √       | √                |
| 5. Restart             | √        | √       | √                |

## 7.25 OMM/DECT PHONE LOCK WITH BRANDING ID

With SIP-DECT 6.0 and later, customers can use a specific branding key to lock the OMM. The key must be branded to all DECT phones before they can be subscribed.

**Note:** This feature is only available by special request. Please contact your Mitel representative for more information.

You generate the branding key using the `DECTSuiteBrandingInstallation.exe` tool (provided by Mitel on special request). When you have the generated keys, you set the branding key in the OMP, via the **System** -> **Advanced Settings** -> **Special branding** tab (see section 6.5.2.7).

The branding key can be only removed from the OMM system by using a special key, also generated with the DECT-Suite PC Tool and entered in the OMP Special branding tab. You must remove the branding key before changing to a different brand.

### 7.25.1 SUBSCRIBING THE DECT PHONE

The user who subscribes the DECT phone must explicitly invoke the transfer of the branding key (done in the AC-Editor).

Add “R\*” (or “R<additional\_id>” in one case) as a suffix to the typed AC code (or just R\*, if there is no AC code).

- Type R\* for normal subscription for fixed devices.
- Type R\* for auto-create by subscription.
- Type R\* for wildcard subscription without DECT phone data record selection.

294

- Type R<additional\_id> for wildcard subscription with record selection by the additional id.

## 7.26 DEVICE PLACEMENT

The OM Locating application uses small graphic maps for visualization of DECT base station placement. From SIP-DECT release 3.1 on, these graphics can be created with the OMP in **Planning Mode**.

### 7.26.1 "PLACEMENT" VIEW

By using the mouse with drag and drop, you can move RFP icons to their correct mounting position on the loaded background image. Note that you must provide background images first (see also (27)).

A DECT base station is drawn as green circle with its ID number inside.

Background images can be loaded into the application on the **Image Management** panel (see section 7.26.3).

The assignment of devices to the currently active image must be done on the **DECT base stations** page.

#### 7.26.1.1 Functionality of the "Placement" View

- Left mouse click selects/deselects the DECT base station the mouse is pointing to. A selected device is shown with thicker border.
  - Drag and drop functionality: a device can be moved while the left mouse button is pressed and hold.
  - If left mouse button is hold and no device is selected, the complete view content gets moved.
  - By turning the mouse wheel the view gets scaled up or down depending from the direction of turning.
  - By pressing the right mouse button a pop-up menu is displayed:
    - **Move selected RFPs**: All selected devices (drawn with a thick border) will be moved to the current position of the mouse pointer. Distances between the devices are not changed as long as all devices can be drawn inside the background image. Moving devices to the area outside the upper or left border of the image is not possible.
    - **Reset selection**: The selection is canceled for all currently selected devices.
    - **Remove selected device(s)**: Selected devices are removed from the current image after confirmation in a dialog box. Those devices can be assigned to an image again via the **DECT base stations** menu (see also section 7.26.2). If no devices are selected but the mouse is pointing to a device, that device is removed from the image without further inquiry.
    - **Reset View**: The view is redrawn in its original appearance. Any translation and scaling applied to the view is cancelled.
- 7.26.1.2 Activation of the "Placement View"**
- The **Placement view** can be activated by:
- Selecting the **Placement View** menu entry. The currently loaded image with its assigned devices is displayed. If no image is currently loaded, the view is empty.

- Double-clicking on a table row in the **DECT base stations** view. This activates the placement view with the image the clicked device is assigned to.
- Selecting the **Assign to active image** task in the **DECT base stations** view. The selected devices are assigned from the table to the current image.
- If a selected device was already assigned to another image, the assignment is changed upon confirmation in a dialog window.
- Selecting an entry in the **Image management** view (double-click or click on **Show image** task).

### 7.26.2 "DECT BASE STATIONS" VIEW

The view shows a table based list of RFP.

When you select table rows and click **Assign to active image**, the selected devices are assigned to the currently active image. Devices already assigned are tagged with a green sign in the table column **Positioned**.

If a selected device was already assigned to another image, the assignment will be changed when confirmed through a confirmation dialog.

### 7.26.3 "IMAGE MANAGEMENT" VIEW

With the **Image management** view all background images assigned to the SIP-DECT system can be managed. Also, the generation of the graphic maps used by the OM Locating application can be started by this view.

If the user activates this view and a background image was loaded, the OMP automatically creates a project file the current SIP-DECT system on the PC. This file contains references to the background image files and the device assignment and placement coordinates. It automatically gets reloaded to the application if the OMP user enters the **Device Placement** menu again during a connection to the same SIP-DECT system.

The images and placement coordinates are stored only on the local PC and not together with the SIP-DECT system configuration (due to storage size limitations). Therefore it is recommended to export the project and save the project data at a secure place after finishing the placement of devices for a SIP-DECT system.

#### 7.26.3.1 "Show image" Task

After selecting an image entry from the table with a left mouse click and then selecting the **Show image** task, the image will be displayed with its assigned devices in the **Placement view**.

A left mouse double click on a table entry also opens the **Placement view**.

#### 7.26.3.2 "Add image" Task

With the **Add image** task, the user calls up a File Open dialog which allows the addition of one or more background images stored on the PC to the system.

The OMP supports \*.jpg and \*.png image files. A maximum of 800 images can be managed by the OMP. The maximum size per image is limited to 3000 pixel in both height and width.

### 7.26.3.3 “Remove Image” Task

The selected image table entries will be removed from the current project after an inquiry dialog. All devices which were already assigned to one of the removed images will be reset to unassigned state.

### 7.26.3.4 “Generate” Task

By choosing this task the user can start the generation of the graphics data needed by the OM Locating application. The OMP will only create graphics data for selected image table.

In a file save dialog the user can select a storage directory for the generated graphics data. A progress dialog informs about the actual status of the generation process. If the process is canceled by the user, the OMP will finish generation of graphics data for the actual background image before stopping the process.

### 7.26.3.5 “Import project” Task

With the **Import project** task the user can load a previously exported project. Images and device placements done before importing a project will be substituted by the data contained in the project.

The system name and the PARK are not checked during this operation. It is possible to import a project created for another system or after the system name or PARK was changed.

Devices are managed by their IDs. If a device ID from imported data cannot be matched with a device ID from the system the OMP is currently connected to, the placement data for such a device will not be imported.

The image files will not be copied. The actual project will save references to the storage place of the images.

### 7.26.3.6 “Export project” Task

With the **Export project** task, the user opens a File Save dialog where the user can select a directory for the exported data, or create a new one.

The OMP exports the project file and copies all background image files to the chosen destination.

A project exported with this task can be imported again via the **Import project** task.

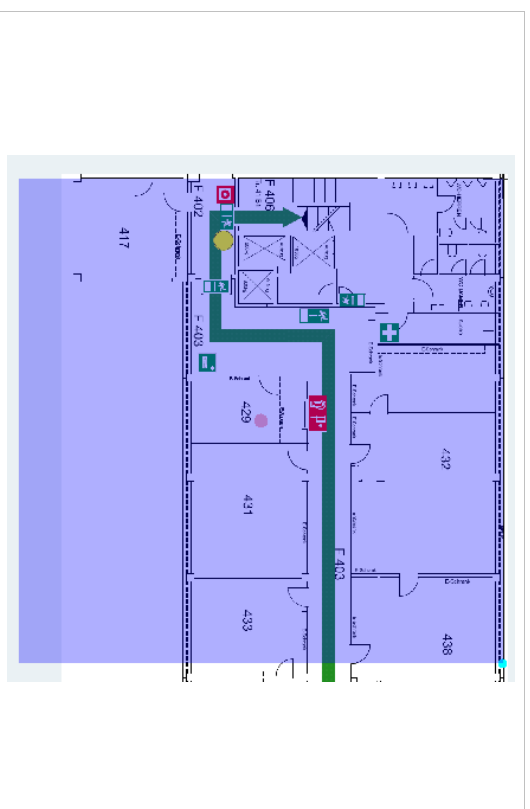
### 7.26.3.7 “Adjust overview size” Task

The OM Locating application needs two graphic maps for each device:

- One detail map image showing the position of an RFP in same scale as the background image on which the device was placed.
- An overview map showing a bigger area of the background image down scaled and the position of the RFP.

There is no special requirement to the scale of the used background images. The selection of the overview scale may differ depending from building or area proportions.

With the **Adjust overview zoom** task the user can adjust the down scale zoom factor for the overview map images (2) individually for the currently selected background image.



The content of an area generated as overview map is shown by the transparent overlay square.

Changing the size of this area can be done by grabbing the light blue point at the right upper edge and moving the edge to (or away from) the center of the area.

By grabbing the red point in the middle of the overlay square it is possible to move the overlay square around.

For generation of the overview map images the position of overlay square does not matter. Only the size is important to calculate the scale ratio for down scaling.

### 7.26.3.8 “Set overview size” Task

Instead of adjusting the scale factor for down scaling on generation of overview maps with the method described in section 7.26.3.7 it is possible to set a scale factor for the selected images.

The value of the scale factor must be chosen with the slider **Overview size** in the task panel prior to assign it to one, several or all images with the **Set overview size** task.

## 7.27 MONITORING WITH USB VIDEO DEVICES

To use an USB video device in interaction with the OM Locating application, a video user account must be configured. In addition the configuration and activation of a video device (“USB Web Cam”) itself is needed.

### 7.27.1 CONFIGURATION OF A VIDEO USER ACCOUNT

An active user account with at least read and video permissions must be configured, to use it inside the OM Locating application.

**Please note:** If you have already configured the OMM's "Full access" account within the OM Locating application to access OMM service, you must change this account to the video-enabled account created in this step.

### 7.27.2 CONFIGURATION OF USB VIDEO DEVICES

You configure video devices on the OMP's **Video devices** page (see section 6.9). The **Video devices** page contains a list of known video devices and you can access the configuration window for the video devices by double-clicking on an entry. Use the left side of the panel to enter a description of the camera and its position. On the right side of the window, you can set the parameters for **Resolution** and **Frame rate**.

The selected values for resolution and frame rate must fit the parameter specifications of the camera device. Changes to these settings are not possible on cameras in a "started" state (i.e., viewed in the OM Location application).

By setting the **Active** option, the video device is permitted to send images.

### 7.27.3 MONITORING WITH USB VIDEO DEVICES

Using the OMP monitoring mode for a video device opens a window with two tabs, the **General** tab and the **Status** tab. On the **General** tab the actual configuration of the video device will be shown. On the **Status** tab the actual status of the camera device will be shown. The tag is an internal identifier of a video device, the **RFP ID** is the identifier of the RFP the video device is plugged in, **USB path** is an identification of the plug-in position and **State** is the actual state of the video device.

### 7.28 TERMINAL VIDEO

As of SIP-DECT 5.0, Mitel 602 DECT phones support video streams from cameras connected to SIP-DECT RFP 35/43 base stations. When a user has video stream permission, he can choose in the system menu from a list of cameras to connect.



Video Streaming is only available when the DECT phone is connected to a RFP 35 and the permission is set for the site and the DECT phone.

Video streams are treated like a call by the DECT phone, which require two (of eight) air channels on the RFP for each stream. The DECT phone can also perform handover between DECT base stations with an active video connection.

A video connection is automatically terminated by the system in case that any related capability (e.g. video stream permission) is changed.

#### 7.28.1 TECHNICAL DETAILS

Terminal video resolution and framerate are independent from the configured camera resolution and framerate.

The resolution of the terminal video stream is automatically downscaled to 176 \* 144 pixels (QCIF) with a frame rate of approximately 2 frames per second.

The resulting overall delay is below 2 seconds.

The maximum number of simultaneous terminal video streams per camera is restricted to 10.

#### 7.28.2 OMP CONFIGURATION STEPS

Connection and configuration of cameras is similar to the steps required to configure the locating application. Special steps necessary for terminal video are:

- Enable all steps, which have the technical capability (only RFP 35/36/37/43 are referred to it), via OMP for terminal video.
- Enable via OMP (**DECT Phones** -> **Users** -> **Additional services**) by setting the "Video stream permission" for those users who are allowed to use this feature.