Installing and Managing Terminals: Mitel 6700 and 6800 SIP Phones MiVoice 6900 IP Phones

09/2022

AMT/PTD/PBX/0043/1/1/EN

Warning

Although the information contained in this document is considered as pertinent, Mitel Networks Corporation (MITEL ®) cannot guarantee the accuracy thereof.

The information may be changed without notice and should never be interpreted as a commitment on the part of Mitel, its affiliates or subsidiaries.

Mitel, its affiliates and subsidiaries shall not be held liable for any errors or omissions made in this document. This document -may be reviewed or re-edited at any time in order to add new information.

No part of this document may be reproduced or transmitted in any form whatsoever or by any means - electronic or mechanical - regardless of the objective, without the written consent of Mitel Networks Corporation.

CONTENTS

1 INTRODUCTION

This document describes the MiVoice 5000 solution used to manage 6xxxi connections via IPv6 and for downloading thanks to HTTP / HTTPS compatibility.

Downloading via the protocol improves security compared to the FTP used in previous releases (> R7.0).

This document specifically describes how to connect and manage 6xxxi terminals.

Concerning terminals 53xxip and 53xx R7.0, they are still managed in FTP only and will not be subject to any software upgrade. Refer to document AMT/PTD/TR/0014.

1.1 TERMINOLOGY

1.1.1 TERMS AND EXPRESSIONS

Mitel 5000 Gateways This term refers to all XS, XL, XD and 500 systems.

MiVoice 5000 or MiVoice 5000 Server Telephone switching system hosted by a PC running with Linux Redhat or Centos

XS, XL, XD Mitel physical gateways.

XS This term includes XS, XS12 and XS6 systems

MiVoice 5000 Manager: Systems management centre

1.1.2 ABBREVIATIONS

DHCP	Dynamic Host Configuration Protocol.
IP	Internet Protocol. This is a protocol used to route packets on networks. IP is an OSI-model level 3 protocol which offers a single addressing service for all connected terminals.
GDB	**G**NU **D**e**B**ugger
PPP	Point-to-Point Protocol.
MMC	Man Machine Interface (here **MiVoice 5000 Web Admin**
SSO	Single Sign On: function which enables a user to open one TWP and MiCollab Client session with the login/password defined for Windows.
TDM	Time Division Multiplexing. Multiplexing through time division. Time is divided into intervals each of which is assigned to a communication channel. This is the principle of signal transport in digital telephony.

1.2 REFERENCE DOCUMENTS

The information in this manual refers to the following documents:

- Mitel XD - XL - XS - XS12 - XS6 - Functional description and Hardware installation - AMT/PTD/PBX/0150/EN
- Mitel 5000 Gateways and MiVoice 5000 Server Activation - AMT/PTD/PBX/0151/EN
- Mitel 5000 – Multi-site management - Operating manual - AMT/PTD/PBX/0081/EN
- CAC Programming guide - AMT/PTD/PBX/0019/EN
- Mitel Terminals - Terminal installation manual - Full Version -AMT/PTD/TR/0014/EN
- IP DECT service - Installation and implementation guide - AMT/PTD/PBX/0062/EN
- Managing DID numbers in R5.2 and later - AMT/PTD/PBX/0099/EN
- Upgrading NeXspan 500 and M6550 iPBXs to Mitel 500 - AMT/PTD/PBX/0113/EN
- Picture management: Operating manual - AMT/PTD/PBX/0114/EN

Also refer to the documentation available on the Mitel.com site.

1.3 REMINDER CONCERNING THE LAW ON INFORMATION TECHNOLOGY

It is the responsibility of a PBX user to check that it is used in accordance with the applicable law, standards and directives.

Therefore, the user is reminded that the use of PBXs in the workplace must comply with the specifications, standards and recommendations of the IT law in force.

The user's attention is also drawn to any clauses applicable in laws relating to the confidentiality of calls transmitted by means of electronic communications, which he must comply with.

2 MIVOICE 5000 ARCHITECTURES WITH MITEL 6000 SIP PHONE.

Mitel 6000 SIP Phones are declared in the systems (MiVoice 5000 Server or Mitel 5000 Gateways), and are connected via the SIP service integrated in the UCV card of Mitel 5000 Gateways, or via the SIP service integrated in MiVoice 5000 Server.

These terminals support the login site optimisation function. This enables the terminal to register with the SIP service of a site which may differ from the site on which the terminal subscription is declared.

Mitel 6000 SIP Phones are connected either to a ToIP VLAN dedicated to terminals, or used together on a Data VLAN and ToIP VLAN in 802.1Q if a PC is connected to the terminal.

The server used to download Mitel 6000 SIP Phones (firmware and configuration files) may be hosted:

- **On an external third-party system that can be managed via FTP**,
- **On an external iPBX such as MiVoice 5000**,
- **On the iPBX itself, MiVoice 5000**. In this case, the server is fitted on the iPBX, and the corresponding service will be fully managed by this same iPBX.

For each terminal, the download server address used must be declared:

- Either through configuration directly on the terminal,
- Or via the **Terminal Service** application (TMA). This application may be the one integrated and installed on an iPBX, or in a multi-site configuration, the one available in MiVoice 5000 Manager in Menu**Telephony>Terminal Management**.
- Or by configuring the DHCP server.

A DHCP server for providing IP addresses must be accessible from the ToIP VLAN.

The level 3 Ethernet switch (router in general) is used for inter-VLAN routing, as well as the DHCP relay for devices outside the Data VLAN.

2.1 CONFIGURING MITEL 6000 SIP PHONES

The different configuration modes for Mitel 6000 SIP Phones are:

- For a single-site configuration, from the integrated TMA (**Terminals service** menu) on Mitel 5000 Gateways and MiVoice 5000 Server
- For a multi-site or cluster configuration, from the TMA hosted by MiVoice 5000 Manager (**Terminals service** menu in the **Terminal management** column)
- Manual mode through direct access in the terminal menus
- Manual mode through the terminal management web interface

Modes recommended according to configuration:

- For a **single-site configuration** of a MiVoice 5000:

Mitel recommends configuring the terminals from the TMA integrated into MiVoice 5000 systems also using the integrated services.

- During a **first installation**:

Deployment may be automatic during start-up in STANDARD or TOTAL mode using the keys CTRL + i. Refer to the section **Managing terminals with the TMA integrated into MiVoice 5000**.

- During an **iPBX update**:

The terminals are automatically updated.

The new software release of the iPBX also contains the new software releases associated with the terminals. Refer to the chapter **Managing terminals with the TMA integrated into MiVoice 5000**.

- For a **multi-site configuration**

For a configuration with several sites or multi-site configurations or cluster, one or more external DHCP servers, one or more external download servers, the use of the TMA hosted by MiVoice 5000 Manager is highly recommended.

This application is used to update software solutions and the global and specific data of terminals Mitel 6000 SIP Phones, without any manual intervention on the terminal. Refer to the section **Managing terminals with the TMA hosted by MiVoice 5000 Manager**.

- In case of **manual configuration**

To quickly deploy some terminals, you may envisage direct configuration on the terminal or via the WEB interface. Refer to the section **Manual configuration of Mitel 6000 SIP phones**.

- If **TMA is not available**:

Whether for a simple or complex configuration, Mitel recommends configuring the terminals via an integrated or external DHCP server so as to automatically recover the standard network parameters and manage those associated with the vendor class of Mitel 6000 SIP Phones if necessary.

The configuration is completed by downloading the software and configuration files associated with Mitel 6000 SIP Phones via an integrated or external download server, by placing these files manually in the appropriate storage directory.

3 GENERAL INFORMATION ABOUT TMA (MIVOICE 5000 MANAGER AND EMBEDDED)

3.1 GENERAL INFORMATION

TMA (**T**erminal **M**anagement **A**pplication) is used to deploy and update the following terminals:

- Mitel 6000 SIP Phones,
- MiVoice 5300 Digital Phone (TDM) and MiVoice 5300 IP Phones (not described in this document, refer to AMT/PTD/TR/0014).

For all the other terminal types, only inventory is possible and only from the TMA on MiVoice 5000 Manager.

The TMA may either be embedded into a MiVoice 5000 (**Terminal service** menu accessible from Web Admin) or centralised on a MiVoice 5000 Manager (Menu **Telephony>Terminal management**).

ATTENTION : The TMA service must be deactivated on the iPBXs of the different sites when the TMA of MiVoice 5000 Manager is used.

No specific additional licence is required to use TMA. However, the **Subscriber management** licence must be unlocked in MiVoice 5000 Manager to access the TMA start menu.

The application is generally in charge of providing configuration software and files on one or more download servers.

TMA can be used for the following operations:

Mitel 6000 SIP Phones,

- Configuring Mitel 6000 SIP Phones:
  - Deploying Mitel 6000 SIP Phones automatically via **manual login**
  - Deploying the terminals via an Excel form
- Taking an inventory of Mitel 6000 SIP Phones (logged and unlogged)
- Updating the (logged and unlogged) terminal software releases:
  - Managing the production release
  - Managing a test version: this function allows a new software release to be loaded only on one part of the terminals so it can be tested before being deployed if necessary on all the terminals in the installation.
- Updating the (logged and unlogged) terminal data:
  - Updating global terminal data
  - Updating specific terminal data
- Exporting (logged and unlogged) terminal configuration files in .csv format:
  - Exporting global terminal data
  - Exporting specific terminal data
- Encrypting the configuration files (specific and global file)
- Downloading files directly into download server(s):
  - A file "**modele.cfg**" may be downloaded to configure the system keys in addition to those managed from Web Admin.
  - Certificates.
- Activating the **Remote worker** function: see the document Remote Worker via MBG - AMT/PTD/PBX/0161 for more information about the deployment of this function.

3.2 MAIN DIFFERENCES BETWEEN TMA ON MIVOICE 5000MANAGER AND TMA INTEGRATED INTO MIVOICE 5000

3.2.1 DIFFERENCES IN TERMS OF DESIGN

The TMA in MiVoice 5000 Manager is used to manage terminals in a multi-site configuration. It is therefore necessary to first select the following from the MiVoice 5000 Manager client terminal:

- Region
- Multi-site configuration.

TMA will then be launched with this initialised data.

3.2.2 FUNCTIONAL DIFFERENCES

The functional differences are:

- MiVoice 5000 Manager **Server Configuration** menu: for creating or adding a new external repository download server and define its configuration parameters. The accounts defined by default for an integrated server, if appropriate, may be restored automatically by clicking **Initialize embedded**.
- i**PBX configuration** menu: this menu is available on MiVoice 5000 Manager only.
    - It is used to send a request to an iPBX in order to delete the TDW tables containing the data version and index information expected for the terminals. This menu must be used after a TMA /TMA-EP passage.
    - This menu is also used to manage the integrated download server, i.e. to delete the content of the download areas on an iPBX. This function can be useful if you wish to use an integrated download server in TMA in MiVoice 5000 Manager.
- **Application configuration** menu:

In MiVoice 5000 Manager, this menu allows you to:

- Configure the application management mode (TMA or TMA-EP)
- Temporarily exclude one or more sites under maintenance
- Test the configuration (accessibility to sites and download servers).

- **Terminal configuration export**: the **specific site data** button is used to export in **.csv** format only the specific data of terminals in site-based production software release. This function is used to export the specific data meant to be used by TMA-EP.

3.2.3 COMPARISON OF THE TMA SERVICES AVAILABLE IN MIVOICE 5000 MANAGER AND INTEGRATED INTO MIVOICE 5000

TMA services in MiVoice 5000 Manager Server **Multi-site or Cluster Configuration**	**Integrated TMA services in MiVoice 5000** **Single-site configuration**
Terminal management	
Mitel 6000 SIP Phone, MiVoice 5300 IP Phone, MiVoice 5300 Digital phone	Mitel 6000 SIP Phone, MiVoice 5300 IP Phone, MiVoice 5300 Digital phone
Terminals logged on and not logged on to the multi-site network	Terminals logged on and not logged on to the site
Inventory	
All types of terminals	All types of terminals
Download server	
External	External or integrated
Software management	
For MiVoice 5300 IP Phones, MiVoice 5300 Digital phones, Mitel 6000 SIP Phones	For MiVoice 5300 IP Phones, MiVoice 5300 Digital phones, Mitel 6000 SIP Phones
Manual operation in TMA to trigger terminal software update for: - A list of terminals (test mode) - All the terminals (production mode)	Manual operation in TMA to trigger terminal software update for: - A list of terminals (test mode) - All the terminals (production mode)
	Automatic terminal software update when the integrated download server is used.
Configuration of Mitel 6000 SIP Phones	
Manual operation in TMA to trigger terminal configuration update for: - A list of terminals (test mode) - All the terminals (production mode)	Manual operation in TMA to trigger terminal configuration update for: - A list of terminals (test mode) - All the terminals (production mode)
Configuration file export	Configuration file export
	Automatic update of the terminal's global configuration file when the integrated download server is used.
A file **modele.cfg** can be directly downloaded into the download servers.	A file **modele.cfg** can be directly downloaded into the download servers.

ATTENTION : For the functions available in TMA-EP mode, see the TMA-EP operating manual (AMT/PTD/TR/0027*).

4 MANAGING TERMINALS WITH THE TMA INTEGRATED INTO MIVOICE 5000

TMA: (**T**erminal **M**anagement **A**pplication)

TMA can be either embedded into a Mitel 5000 Gateways or MiVoice 5000 Server system (accessible from Web Admin), or centralised on a MiVoice 5000 Manager.

The integrated TMA is accessible via the **Terminal service** menu, on the Web Admin welcome screen.

4.1 PRESENTATION AND PRINCIPLES

The TMA application embedded into Mitel 5000 Gateways and MiVoice 5000 Server systems allows the deployment and management of Mitel 6000 SIP Phone SIPs.

The TMA integrated into Mitel 5000 Gateways and MiVoice 5000 Server has a single-site range only.

No specific additional software licence is required to use the integrated TMA. However, the licences for SIP subscribers must be unlocked.

The integrated TMA is compatible with the FTP server integrated into Mitel 5000 Gateways and MiVoice 5000 Server, as well as with external download servers; the principles are respectively:

- **For an integrated download server**, the integrated TMA creates some symbolic links between the directories on the download server and the tree directories of TMA.

Note : If the configuration file encryption function is enabled, the encrypted configuration files are physically copied into the integrated download server storage directories.

- **For an external download server**, the integrated TMA copies the files (configuration software and files) from the TMA directories to the external download server storage directories.

Note : During each terminal update operation (software, configuration), TMA checks the accessibility of the sites and external download servers concerned by the action. In case of error during this check, the action is not performed.

As of R7.0, access to the directories containing the software releases may be via HTTP/HTTPS protocols and no longer via FTP, thus improving security. This is the default configuration for a new installation.

On Mitel5000 Gateways, downloading via HTTP is only available, but TMA uses HTTPS for file management.

However, downloading via FTP is still available but not recommended, especially for read access (by terminals) in the event of an upgrade or if 53xxip terminals are present in the installation.

Case of third-party download servers

On third-party servers, the connection is managed in HTTPS.

Administration is still via FTP to ensure the encryption of all outgoing traffic from the iPBX.

The following table describes the protocols used to download terminals or to manage download spaces (Admin).

The 53xxip terminals are indicated for information purposes but are not subject to any software upgrade as of R7.0.

TMA Embedded

			MiVoice 5000 download server						Third party server		
			Embedded			Not Embedded					
			FTP	*FTP+WEB*	*WEB*	*FTP*	*FTP+WEB*	*WEB*	*FTP*	*FTP+WEB*	*WEB*
	Admin		internal	internal	internal	FTP	HTTPS	HTTPS	FTP	FTP or FTPS	FTP or FTPS
Download		53xxip	FTP	FTP	X	FTP	FTP	X	FTP	FTP	X
		6xxxi	FTP	WEB	WEB	FTP	WEB	WEB	FTP	HTTPS	HTTPS
										Optional	

Local: direct access to disk space.

FTP: simply an FTP access.

WEB: HTTPS or HTTP, because HTTPS is not possible on Mitel 5000 Gateway. E mode cannot be selected as long as there are 53xxip terminals in the installation.

FTP + WEB: the two protocols for accessing the download areas are available, FTP for 53xxip terminals and WEB for 6xxxi.

X: not supported

4.2 LAUNCHING THE TMA

From Web Admin, start TMA by selecting **Terminal service**:

Terminal service is activated during first installation and during an upgrade.

If **Terminal service** is not activated, at the Web Admin level, select Menu **Telephony Service Menu>System>Configuration>Services** and start **Terminal service**.

- The TMA welcome window opens.

The following menus are accessible in the left column:

- **Call Dist**: This menu is used to return to the Web Admin home page.
- **Application configuration**:

This menu is used to:

  - Deactivate the management of global and specific data files and to retain only software update actions on the terminals, in the actions managed by TMA
  - Activate **configuration file encryption mode**
  - Activate the **Remote worker** function: See the document Remote Worker via MBG - AMT/PTD/PBX/0161 for more information about the deployment of this function.
  - Enable certificate verification between the iPBX and the download server.

- **Model management**: This menu allows you to activate or deactivate the management of the model in question.
- **Servers configuration**: This menu is used to define the parameters of the external storage server(s).
- **Inventory**: This menu is used to view the inventory of installation terminals and manage the list of terminals.
- **Software management**: This menu is used to install and manage the terminal software releases and start terminal update actions.
- **Terminals configuration**: This menu is used to distribute the global and specific parameters and to start data update on the terminal.
- **Deployment**: this menu is used to deploy the terminals manually. This menu is also used to make available to the download server(s) the template files (**modele.cfg**) and the certificates (**ca.crt**) used by Mitel 6000 SIP Phones.
- **Terminals configuration export**: This menu is used to export in **.csv** format the global and specific data about Mitel 6000 SIP Phones.
- **Actions display**: This menu is used to track the actions started on the terminals (deployment, terminal software, global and specific data).
- **Events log**: This menu displays the events log.

4.3 CONFIGURING TMA

4.3.1 CONFIGURING THE TERMINALS

For Mitel 6000 SIP Phones, TMA is dedicated to the management of two data types:

- The software release compared to that of the iPBX
- The global and specific data about each terminal model of the range in question.

In some cases, only the management of software release may be necessary on this terminal range.

The **application's configuration** menu can be used to disable the management of configuration files and, thus, to also disable the deployment actions and to only preserve the terminal software update operations.

The following operations will not be carried out:

- Automatic terminal software and global data updates if the iPBX is upgraded (if the download server integrated into Mitel 5000 Gateways or MiVoice 5000 Server is started)
- Automatic global data configuration file update
- Encryption of configuration files.

Select the **Application configuration** menu from the TMA main menu.

- Untick the **Terminals configuration** box.
- Click **Validate**.

Only the menus relating to terminal software update are then proposed.

4.3.2 ENCRYPTING CONFIGURATION FILES

The **Application configuration** menu is also used to activate the **configuration file encryption** function:

- For Mitel 6000 SIP Phones, the specific and global configuration files, as well as the template files **modele.cfg** made available via the **deployment** menu, are encrypted.

The configuration files of Mitel 6000 SIP Phones are encrypted automatically by TMA during the following operations:

- Specific data update
- Global data update
- Deployment via the Excel form
- Terminal software package update in production mode and test mode
- Automatic terminal software and global data updates if the iPBX is upgraded (if the download server integrated into Mitel 5000 Gateways or MiVoice 5000 Server is started)
- Automatic update of the global data configuration file after certain parameters are modified via Web Admin (terminal VLAN, PC VLAN, LLDP, etc.).

To activate configuration file encryption, select the **Application configuration** menu from the TMA main menu.

- Tick the **Configuration file encryption** checkbox.
- Click **Validate**.
- Validate the confirmation message by clicking **Yes**.

ATTENTION : Configuration file encryption can only be deactivated manually. Contact Mitel technical support.

4.3.3 CHECKING CERTIFICATES

The **Check Certificates** checkbox strengthens the security of the HTTPSconnection between TMA and iPBX by checking the certificate on both sides.

TMA uses the certification authority stored in the certification authorities' base to check the certificates.

Certificates issued to terminals have the same certification authority as the iPBX to which they are attached.

By default, certificates are checked on a system after a first installation and not after an upgrade.

4.4 MODEL MANAGEMENT

Model management is performed from this menu and is taken into account in the embedded TMA.

When downloading a terminal package, TMA Embedded only keeps the software of managed models.

Therefore, during a software update, only files related to managed models are sent to the download servers.

4.5 CONFIGURATION PARAMETERS OF THE DOWNLOAD SERVER(S)

4.5.1 INTRODUCTION

TMA is generally in charge of providing some configuration software and files on one or more download servers during day-to-day terminal deployment or management.

4.5.2 SINGLE-SITE CONFIGURATION

For Mitel 5000 Gateways and MiVoice 5000 Server systems as well as a single-site configuration, an integrated download server called "**internal**" is available and is automatically configured during the automatic start procedure in STANDARD or TOTAL mode using **CTRL + i**, or when it is started manually via Web Admin.

Note : The integrated download server of the TMA integrated into Mitel 5000 Gateways is automatically configured and accessible from the server configuration menu.

ATTENTION : For MiVoice 5000 Server, the downloading service must first be installed during the start procedure in STANDARD or TOTAL mode using CTRL + i (only if there are 53xxip terminals in the installation.

The downloading service can then be started automatically or manually via Web Admin.

Providing configuration software and files:

- **For an integrated download server**, the integrated TMA creates some symbolic links between the storage directories of this server and the work directories of TMA.

Note : If the configuration file encryption function is enabled, the encrypted configuration files are physically copied into the integrated download server storage directories.

- **For an external download server**, the integrated TMA copies the files (configuration software and files) from the TMA work directories to the external download server storage directories.

Note : During each terminal update operation (terminal software, configuration files), TMA checks the accessibility of the sites and external download servers concerned by the action.
In case of error during this check, the action is not performed.

4.5.3 MULTI-SITE CONFIGURATION

In this case, TMA is started from MiVoice 5000 Manager and the download servers must be manually defined in the **Server configuration** menu.

The download servers integrated into the multi-site Mitel 5000 Gateways and MiVoice 5000 Server may be used by identifying and configuring them from MiVoice 5000 Manager in the same **Servers configuration** menu.

4.5.4 CONFIGURATION WITH SEPARATING TELEPHONY AND ADMINISTRATION FLOWS

If the server to be configured is a local server with Web access (Https, FTP), the address to be entered in the **Server configuration** menu must be the one defined for the **Telephony network>IP address field for the terminals.**

4.5.5 MANAGING THE DOWNLOADING AREA (IN WEB ADMIN)

4.5.5.1 *Introduction*

As of R7.0, the **Terminal areas** tab of Menu **System>Software maintenance>File downloading** allows you to define a terminal management and update area used by TMA for 6xxxi terminals.

This management area includes:

- A production version downloading area,
- A test version downloading area,
- A deployment area.

The following actions are possible in these areas:

- Add or update files (final version or any other configuration file),
- Delete files.

Note: The TFTP tab of the same menu is still available and is used to download the files for the following devices to a specific directory dedicated to the TFTP server:

- **DECT SIP RFP 32-34-42**
- **IMA CONGIGURATION**
- **TERMINAL A6XX (“aafon6xxd.dnld”)**
- **WIFI TERMINAL 312I ("312w.dnld")**

Refer to the latest version of Manual AMT/PTD/PBX/0080 - Mitel XD-XL-XS-XS-XS12-XS6-500 and MiVoice 5000 Server OPERATING MANUAL

The administrator can also add and delete specific files directly in this area, for example when TMA is not used.

Files can be retrieved from the downloading URLs specified in the last **Get file** column.

4.6 CONFIGURING AND STARTING THE DHCP SERVER

4.6.1 INTRODUCTION

The DHCP server is used to automatically assign an IP address to Mitel 6000 SIP Phones, with a lease, and to negotiate some standard and specific network parameters with them. These parameters will enable them to download the terminal software and configuration files placed in the right storage areas on the download server(s) in question.

The parameters which can be negotiated with Mitel 6000 SIP Phones are described in Chapters 6 and 7.

The type of DHCP server used depends on the type of configuration.

Single-site configuration

For Mitel 5000 Gateways and MiVoice 5000 Server, as well as a single-site configuration, an integrated DHCP server is available and configurable:

- Either automatically during the start procedure in STANDARD or TOTAL mode using **CTRL + i**. This method is highly recommended in this type of configuration.
- Either manually from the Web Admin **DHCP SERVICE** menu. See Chapter 6.

Multi-site configuration

In this case, the DHCP server is external and must be configured manually. See Chapter 7 for more information about external DHCP server configuration.

4.6.2 STARTING THE DHCP SERVICE INCORPORATED INTO THE MITEL 5000 GATEWAYS SYSTEM

The integrated DHCP server on the Mitel 5000 Gateways system is not started by default when the Mitel 5000 Gateways system is installed.

To see its status, proceed as follows:

- From the web browser, connect to the system’s MiVoice 5000 Web Admin.
- Go to the service management menu:

This menu (231) is accessible via **Telephony service>System>Configuration>Services**.

Check the status of the **DHCP service** that must be **STOPPED**. It must be started manually through this menu or started and configured automatically through the procedure described in Chapter 6.

4.6.3 STARTING THE DHCP SERVICE INCORPORATED INTO A MIVOICE 5000 SERVER SYSTEM

By default, the integrated DHCP server on MiVoice 5000 Server is not installed and started when MiVoice 5000 Server is installed.

Therefore, the **DHCP** service is not accessible in Menu **Telephony service**>**System>Configuration>Services** (231).

For the installation and configuration of the start of the integrated DHCP server on MiVoice 5000 Server while starting in STANDARD or TOTAL mode using **CTRL + i**, refer to Section 4.9.4.

4.7 PREPARING THE DEPLOYMENT OF TERMINALS FOR A NEW MITEL 5000 GATEWAYS INSTALLATION

4.7.1 PRINCIPLE

The advantage of using integrated TMA in the deployment phase lies in the possibility to automate the deployment of IP terminals using the integrated TMA, FTP and DHCP services.

This automatic configuration is made during the start procedure in STANDARD or TOTAL mode using **CTRL + i**.

Note : See also Implementing Mitel 5000 Gateways and MiVoice 5000 Server - AMT/PTD/PBX/0151* for more information about implementing an installation.

4.7.2 CONFIGURING THE SYSTEM VIA CTRL I

Access is provided locally on the COM port of the CPU card, using a NULL MODEM cable (ref.: BHG0024A) connected between the COM port of the CPU card and the PC COM port.

On the PC connected to the COM port:

- Open a Hyperterminal window and configure the connection as follows:
  - Bits per second: 115200 bits/s
  - Data bits: 8
  - Parity: none
  - Stop bits: 1
  - Flow control: None.
- Power on the system and follow the start-up progress on the PC.
- Upon display of "**Identification starting**":
- Press **Ctrl** + **I**: the screen displays the different configuration modes.
- Select **S** mode then press "**Enter**" to enter the network parameters configuration menu.

4.7.3 CONFIGURING NETWORK PARAMETERS IN A MITEL 5000 GATEWAYS SYSTEM

- The system's default network configuration is displayed on screen.
- Press "**Y**" then "**Enter**" to access the different fields.
- Enter successively the system parameters, using the **Enter** key to change line.
- After the last line is validated, a summary of the network parameters is displayed for confirmation.
- Press "**Y**" to confirm the input or "**N**", in case or error, to enter the network parameters again.

4.7.4 CONFIGURING FLOW SEPARATION IN A MITEL 5000 GATEWAYS SYSTEM

The screen then displays the flow separation configuration for signals and data.

ATTENTION : Answer "N" and go to the next screen. If necessary, refer to the flow separation operating manual (AMT/PTD/PBX/0101*).

4.7.5 CONFIGURING THE INTEGRATED SERVICES OF THE MITEL 5000 GATEWAYS SYSTEM WHILE STARTING THE SYSTEM

The screen below is used to define the status of the integrated services when starting the system, so as to automate terminal deployment.

By default, the TMA and FTP services are started automatically (TMA = 1, FTP = 1). The integrated DHCP server must also be started and configured automatically.

Note : These services can also be activated later from Web Admin if automatic deployment is not envisaged.

- Press "**Y**" to modify the configuration and set automatic start of the integrated DHCP server.
- Press "**Y**" to confirm the input.

4.7.6 CONFIGURING THE PARAMETERS FOR AUTOMATIC DEPLOYMENT OF MITEL 6000 SIP PHONES IN A MITEL 5000 GATEWAYS SYSTEM

The screen below is used to define the parameters for automatically deploying Mitel 6000 SIP Phones.

- Press "**N**". Press "**Y**" to modify the default configuration, if necessary.
- The default parameters are as follows:
  - LLDP ENABLED=0
  - This field is used to activate the LLDP in the terminal (1 = yes) or not (0= no).

Note : This value can also be viewed and modified via the Web Admin menu Telephony service>Subscribers>Terminals and applications>6xxxi parameters.

4.7.6.1 *LLDP operation of the 6700 SIP, 6800 SIP and 6900 IP terminals (optional):*

Mitel 6700 SIP, 6800 SIP and 6900 IP phones are LLDP-MED compatible, which allows the acquisition of the VLAN ID with which they must be deployed. This operating mode is active by default on the terminals and, to be operational, the terminals must be connected to a network SWITCH compatible with this function. This latter must then provide the required VLAN ID.

However, when a terminal is started, a first **DHCP DISCOVER** request may be sent without VLAN tag (default VLAN of the SWITCH), or in the data VLAN if already configured in the terminal.

The acquisition of an IP address in this default VLAN is not mandatory, and the DHCP request sent may remain without any reply.

If an IP address is assigned to the terminal by a DHCP server, it is immediately released through a DHCP RELEASE before a new DHCP DISCOVER request is made in the new VLAN acquired during the LLDP discover procedure.

Thereafter, the terminal continues to work in the VLAN sent by the SWITCH with an IP address assigned by a DHCP server in the corresponding IP subnet.

4.7.7 CONFIGURING THE NETWORK PARAMETERS OF THE DHCP SERVER INTEGRATED INTO A MITEL 5000 GATEWAYS SYSTEM

The following screen is used to define the configuration parameters of the integrated DHCP server in Mitel 5000 Gateways systems. This menu is used to define the parameters that allow the integrated DHCP server to be configured automatically for the terminals.

Note : Manual configuration of the DHCP server is available from Web Admin and allows the modification of the automatic configuration defined via this menu. See Chapter 9 for more information on how to manually configure the integrated DHCP server.

- Enter successively the configuration parameters of the integrated DHCP server, using the **Enter** key to change line.
- **SUBNET MASK**: Subnet mask for MiVoice 5300 IP phone, Mitel 6000 SIP Phone and i7xx.
- **BEGIN RANGE and END RANGE**: Address range for MiVoice 5300 IP phone, Mitel 6000 SIP Phone and i7xx.
- **GATEWAY**: Network gateway IP address for MiVoice 5300 IP phone, Mitel 6000 SIP Phone and i7xx.
- **TERMINAL VLAN and PC VLAN**: These parameters are used to define the LAN port and PC port VLAN dedicated to the terminals. They are not mandatory for simple networks (do not make any entry on the line concerned and press **Enter)**.
- Answer "**Y**" to the question:

```
Do you want to apply your change Y(es)/N(o)/R(econfigure) ?
```

The procedure for configuring the system via **CTRL I** has ended and the system restarts.

4.7.8 RESTARTING MITEL 5000 GATEWAYS SYSTEMS

After the system is restarted, the automatic configuration phase last about 5 minutes.

During this period, the following main actions are taken:

- The DHCP server, integrated to manage the terminals is automatically configured.
- The new network parameters of the integrated FTP server are taken into account in the integrated downloading application.
- The global data configuration file used to deploy terminals is updated with the information entered previously using **CTRL+I.**

Note : In factory presetting, the global data configuration file used to deploy the terminals is automatically updated with the country-location and operation information.

The index of the global data configuration file of terminals, which can be used by integrated TMA, is updated. An action is automatically started by the integrated TMA application to update the system data (the index of the global data configuration file used for deployment and by the TMA application remains identical. This prevents, after the first manual login of the terminal, a terminal update request by the system).

Note : In factory presetting:

- **The production software release of the integrated TMA is automatically configured with the software releases contained in MiVoice 5000.**
- **The software releases of the terminals contained in the MiVoice 5000 release are moved to the working directories of the embedded TMA (symbolic links are present in the deployment_67xxi deployment directory: these symbolic links point to the TMA working directory where the Mitel 6000 SIP Phone production software version is stored. There is no change for the global deployment configuration file aastra.cfg which remains physically present in this location).**
- **Some automatic actions are automatically started by the integrated TMA to update the software releases and global data configuration file of the terminals (respectively localdb.config.ftp and aastra.cfg).**

Automatic terminal configuration is activated by default as well as automatic update of the dialling plan and system keys of Mitel 6000 SIP Phones, the management of the programmable keys, languages and pictures of Mitel 6000 SIP Phones (Menu **Telephony Service>Subscribers>Terminals and Applications>6xxxi parameters**).

The checks to be made before deploying the terminals are indicated in the following sections.

To access the configuration menus of the integrated TMA, click the **Terminal service** menu from Web Admin.

4.7.9 CHECKING THE CONFIGURATION OF THE DHCP SERVER INTEGRATED INTO A MITEL 5000 GATEWAYS SYSTEM

The **network** dedicated to MiVoice 5300 IP Phone, Mitel 6000 SIP Phone and i7xx is automatically configured using **CTRL + I**:

All terminal models associated with these three terminal ranges can be configured for the **network.** The **network** is also automatically configured with the information entered with **CTRL + I**:

- Subnet name
- Sub-network address
- Subnet mask
- IP address range
- Lease duration
- Router IP address.

For each terminal range concerned, the DHCP options are equally configured automatically using the information entered with **CTRL + I**:

- Integrated download server IP address
- Main PBX IP address...

4.7.10 CHECKING THE CONFIGURATION OF THE DOWNLOAD SERVER INTEGRATED INTO A MITEL 5000 GATEWAYS SYSTEM

The directories used for the daily management and deployment of MiVoice 5300 IP Phone, Mitel 6000 SIP Phone and MiVoice 5300 Digital Phone are automatically created in the Mitel 5000 Gateways system. The main directory under which these directories are located is called **opt/a5000/infra/sip_sets**.

Each storage directory is accessible via an account (login/password) which defines the possible actions according to user type and terminal type.

The configuration of the integrated download server used by the integrated TMA is automatically defined and can be viewed in the **Servers configuration** menu (Action: **Modify the server**).

4.7.11 CHECKING THE CONFIGURATION OF THE PRODUCTION SOFTWARE RELEASE OF MITEL 6000 SIP PHONES

The production terminal software release is automatically defined after the factory pre-configuration made in the integrated TMA and in the Mitel 5000 Gateways system data.

The **Software management** menu is used to check the production terminal software release for each terminal range.

The information is displayed in the **Production software release** field.

4.8 DEPLOYING TERMINALS ON A NEW MITEL 5000 GATEWAYS INSTALLATION (AND MIVOICE 5000 SERVER)

After the pre-configuration made in Section 0, Mitel 6000 SIP Phones can be deployed using the following three methods:

- Deployment through manual login on the terminal
- Deployment via the MiVoice 5000 User Portal from a single label identifying the terminal.
- Automatic deployment by assigning a subscription number to the terminal.
- Deployment from a dedicated Excel file.

4.8.1 DEPLOYMENT THROUGH MANUAL LOGIN OF MITEL 6000 SIP PHONES

4.8.1.1 *Principle*

This deployment method consists in making a manual login on Mitel 6000 SIP Phones without having to indicate the specific configuration file **@MAC.cfg**. The production software release and global data configuration file downloaded by terminals Mitel 6000 SIP Phones during this deployment phase are available in the storage folder **deployment_67xxi**. This directory is accessible to Mitel 6000 SIP Phones via the account connexio/connexio, the default factory account of Mitel 6000 SIP Phones.

4.8.1.2 *Procedure*

Prerequisites:

- The subscription of the Mitel 6000 SIP Phone on which manual login must be performed must be declared in the Mitel 5000 Gateways system.
- A directory record must exist for this subscription.
- Login via PC should not be activated:
- In the Web Admin menu **Telephony service**>**Subscribers**>**Terminals and Applications**>**6xxxi parameters**, the parameter **Login** via PC should not be ticked (default value).

ATTENTION : It is advisable to restore the factory configuration before any deployment operation via manual login.

Procedure:

- Connect the terminal to the network in question.
- The terminal is initialised and connects to the integrated DHCP server. The integrated DHCP server will then assign an IP address to the terminal. The integrated DHCP server will also provide the Mitel 6000 SIP Phone with the IP address of the integrated download server and the account (connexio/connexio) to which the Mitel 6000 SIP Phone will connect to download its production software release and global deployment data configuration file.
- After the new production software release and global configuration file are downloaded, the terminal screen shows that the terminal is a general-purpose terminal (without subscriber).
- Press the **Ident** key which lights up by default (key 4).

- Enter the subscription number of the Mitel 6000 SIP Phone then press **Enter** to confirm.
- Enter the password (**0000** by default) and press **Enter** or **OK** to confirm.
- A wait message appears and the terminal logs on to its subscription.
- The terminal is operational; the idle screen is displayed.

4.8.2 DEPLOYMENT VIA THE MIVOICE 5000 USER PORTAL OF MITEL 6000 SIP PHONES

4.8.2.1 *Principle*

The purpose of this deployment method is to perform a login via the MiVoice 5000 User Portal application. The user selects a terminal on which to login from his/her system label. This label is unique and is automatically generated by the Mitel 5000 Gateways system.

Note : The user can connect to the MiVoice 5000 User Portal application via his/her User Portal specific password or in SSO mode.

4.8.2.2 *Procedure*

Prerequisites:

- The subscription of the Mitel 6000 SIP Phone on which manual login must be performed must be declared in the Mitel 5000 Gateways system.
- A directory record must exist for this subscription.
- Login via PC must be activated:
  - In the Web Admin menu **Telephony service>Subscribers>Terminals and Applications>6xxxi parameters**, the parameter **Login via PC** must be checked (default value).
- A default label must be configured:
  - In the Web Admin menu **Telephony Service>Terminals and Applications>6xxxi parameters**, the parameter **Label format** must be configured (an example of a label is indicated from the configured format).
- This default label may be modified:
  - individually, in the Web Admin menu **Telephony Service>Subscribers>Terminals and Applications>Terminal label management**.
  - massively, by exporting/importing the **csv** files of all labels

ATTENTION : It is advisable to restore the terminal's factory configuration before any deployment operation.

Procedure:

- Connect the terminal to the network in question.
- The terminal is initialised and connects to the integrated DHCP server. The integrated DHCP server will then assign an IP address to the terminal. The integrated DHCP server will also provide the Mitel 6000 SIP Phone with the IP address of the integrated download server and the account (connexio/connexio) to which the Mitel 6000 SIP Phone will connect to download its production software release and global deployment data configuration file.
- After the new production software release and global data configuration file are downloaded, the terminal screen displays the label defined for this terminal.

Note : Being configured in unsecured mode, the user can also perform a manual login directly on his/her terminal via the Ident key.

- Connect to the MiVoice 5000 User Portal application (in SSO mode or via the directory number of your subscription and User Portal password).
- Select Menu **Terminals>Login/Logout.**
- Select a free terminal by its label, either by selecting a terminal available in the history, or by entering a new terminal.
- Click **Login**.
- The terminal logs on to its subscription.
- The terminal is operational; the idle screen is displayed.

4.8.3 AUTOMATICALLY DEPLOYING MITEL 6000 SIP PHONES

4.8.3.1 *Principle*

The principle of this deployment method is to automatically login Mitel 6000 SIP Phones by automatically assigning a directory number to each terminal identified by its unique label.

4.8.3.2 *Procedure*

Prerequisites:

- The subscription of the Mitel 6000 SIP Phone on which automatic login must be performed must be declared in the Mitel 5000 Gateways system.
- A directory record must exist for this subscription.
- Login via PC must be activated:
  - In the Web Admin menu **Telephony service>Subscribers>Terminals and Applications>6xxxi parameters**, the parameter **Login via PC** must be ticked.
- A default label must be configured:
  - In the Web Admin menu **Telephony Service>Terminals and Applications>6xxxi parameters**, the parameter **Label format** must be configured (an example of a label is indicated from the configured format).
  - This default label may be modified:
  - individually, in the Web Admin menu **Telephony Service>Subscribers>Terminals and Applications>Terminal label management**
  - massively, by exporting/importing the **csv** files of all labels
  - A directory number must be assigned to each label:
  - individually, in the Web Admin menu **Telephony Service>Subscribers>Terminals and Applications>Terminal label management**
  - massively, by exporting/importing the **csv** files of all labels

ATTENTION : It is advisable to restore the terminal's factory configuration before any deployment operation.

Procedure:

- Connect the terminal to the network in question.
- The terminal is initialised and connects to the integrated DHCP server. The integrated DHCP server will then assign an IP address to the terminal. The integrated DHCP server will also provide the Mitel 6000 SIP Phone with the IP address of the integrated download server and the account (connexio/connexio) to which the Mitel 6000 SIP Phone will connect to download its production software release and global deployment data configuration file.
- After the new production software release and global data configuration file are downloaded, the terminal screen displays the label defined for this terminal.

- The terminal logs on automatically to its subscription.
- The terminal is operational; the idle screen is displayed.

4.8.4 DEPLOYMENT VIA EXCEL FORM OF MITEL 6000 SIP PHONES

4.8.4.1 *Principle*

This method consists in deploying the terminals via an Excel form provided with the MiVoice 5000 software CDROM dedicated to the deployment of Mitel 6000 SIP Phones. This method requires modifying the DHCP server configuration so Mitel 6000 SIP Phone connects to the download server used for day-to-day management.

A form is provided with the MiVoice 5000 software CDROM. From this form, the terminals' global and specific data is collected and exported in .csv format. Specific data is indexed by terminal MAC address.

Note : After the configuration performed previously with CTRL + I, the integrated download server is configured automatically.

Note : The terminal software package associated with the MiVoice 5000 software was installed automatically and defined as production release, after the configuration performed previously with CTRL I.

The operator selects:

- The global and specific data of Mitel 6000 SIP Phones in .csv format to be imported into TMA
- The terminal software package to be deployed
- Possibly other files such as template files **modelle.cfg** or a certificate
- The integrated download server on which this data must be stored.

The operator validates the deployment operation: the terminal software, language files, global and specific data are then automatically sent to the integrated download server via some symbolic links.

The operator connects the terminal to the local area network and this latter registers to its reference site via automatic login using the login site optimisation mechanism if necessary.

Procedure

4.8.4.1.1 Collecting global and specific data via the Excel form

The Excel form **TMA_provisionning_67xxi@R***X.Y*_67xxi_*xx_yy*.xls is available on the MiVoice 5000 software CD-ROM, in the directory **sip_sets_tma**.

The Excel form contains four tabs:

- The **Import_CSV_TMA** tab**:** useful only for the TMA EP application, refer to Manual AMT/PTD/TR/0027 for more details.
- The **67xxi Global** tab in which the global data of Mitel 6000 SIP Phones is defined
- The **67xxi Specific** tab in which the specific data of Mitel 6000 SIP Phones is defined
- The **67xxi All** tab in which all the parameters used by terminals Mitel 6000 SIP Phones are defined
- The **68xxi_Teleworker** tab useful for the remote worker function, refer to Manual AMT/PTD/PBX/0161 for more details.

All or part of the parameters in the **67xxi All** tab may or may not be managed in the global or specific data, depending on the required distribution of the parameters.

To add a parameter in the **67xxi Global** tab, copy from the **67xxi All** tab the parameter concerned, located in the **#KEY** column then paste it on the first free line of the **67xxi Global** tab.

To add a parameter in the**67xxi Specific** tab, copy from the **67xxi All** the parameter concerned, located in the **#KEY** column then paste it on the first free column of the **67xxi Specific** tab.

After data distribution, you can collect and export data in .csv format.

4.8.4.1.2 Saving the global and specific data in .csv format

- To save the global data in .csv format:
  - Go to the **67xxi Global** tab.
  - Click Menu **File**>**Save As...**.
  - Go to the right directory, enter a file name then select Type of file **CSV (separator: semicolon) (*.csv)**.
  - Click **Save**.
  - Confirm the next two information messages by clicking **OK** then **YES**.
- To save the specific data in .csv format:
  - Go to the **67xxi Specific** tab.
  - Click Menu **File**>**Save As...**.
  - Go to the right directory, enter a file name then select Type of file **CSV (separator: semicolon) (*.csv)**.
  - Click **Save**.
  - Confirm the next two information messages by clicking **OK** then **YES**.
- Close the Excel form.

ATTENTION : Never modify the content of .csv files directly. The modifications must be made in the Excel form then saved in .csv format.

4.8.4.1.3 Deploying the terminal software release and configuration files on the integrated download server

To deploy the terminal software release, language files and configuration files for the global and specific data of Mitel 6000 SIP Phones on the integrated download server, proceed as follows.

- From the integrated TMA, click the **Deployment** menu.
- Select the **6xxxi** range.
- In the **List of servers** column, click the integrated server on which the terminal software release and configuration files will be placed.

Note : If only one server is defined, this will be selected by default.

- Select the **Software version** to be deployed.

Note : If only one software release is installed, it will be selected by default.

- Select the **Global (csv) file** to be deployed:
  - Click **Browse** then select the .csv file to import and which corresponds to the global data of Mitel 6000 SIP Phones from the collection. Click **Open.**
- Select the **Specific (csv) file** to be deployed:
  - Click **Browse** then select the .csv file to import and which corresponds to the specific data of Mitel 6000 SIP Phones from the collection. Click **Open.**
- It is also possible to download other files such as certificates, template files (**modele.cfg**) via the **Other file (template, certificate, etc.)** field. These downloaded files are stored locally and can be downloaded again via the **Previously downloaded files** field.
- Click **Validate** to start deploying the terminal software release and the configuration files of Mitel 6000 SIP Phones: a message indicates that deployment is in progress.

- The following files are then placed automatically by TMA in the storage directory of the integrated download server by creating symbolic links:
    - The terminal software releases **<type poste>.st**
    - The global data file **aastra.cfg**
    - The specific data files @MAC.cfg (example: 00085D3A2451.cfg).
    - The language pack: **lang_<ISO 639>_<ISO 3166>.txt** or **lang_<ISO 639>.txt** (example: lang_fr_ca.txt or lang_de.txt).
    - Possibly template files or certificates.

Note : The global and specific data is automatically changed to a format that is compatible with Mitel 6000 SIP Phones by TMA.

The terminals' global and specific data files are also copied automatically to the integrated TMA work directories. This prevents the global and specific data from being entered twice in TMA for day-to-day management of these terminals.

4.8.4.1.4 Checking that the deployment process is working correctly

This operation is used to ensure that the deployment operation has been performed correctly.

- Click the **Action monitoring** menu.
- Check in **Action monitoring,** the status of the deployment operation:
    - If the deployment operation was successful, the status indicates: **Successful.**
- Check in the **Event log,** the status of the deployment operation:
    - If the deployment operation was successful, the status indicates: Action successful. Action on MiVoice 5000 taken into account.
    - The number of transferred files is used to ensure that all the files have actually been placed in the integrated ownloading server storage directory.

4.8.4.1.5 Connecting the terminals to the local area network

The operator connects the terminal to the local area network:

- The terminal retrieves the IP address of the integrated download server from the DHCP server.
- The terminal connects to the integrated server and updates its software release if necessary. The terminal also retrieves its global and specific data configuration files.
- The terminal registers automatically to its reference site from the information contained in its global and specific data configuration files and is then visible in the TMA inventory.

4.8.5 MULTI-COMPANY CONFIGURATION

For a multi-company configuration, if the subscription on which Mitel 6000 SIP Phone is deployed is not in company 0, authorise the EAS user to access the terminal company.

If an attempt is made to deploy a Mitel 6000 SIP Phone on a subscription that does not belong to company 0 and the action is rejected with the message **PBX subscription not declared,** proceed as follows:

- Authorise deployment on the company associated with the subscription:
    - Open the menu **External applic. server users** (4.4.7 in a single-site configuration).
    - Click the digit for the column which corresponds to the EAS user "saesae" (generally 1).
    - Tick the box authorising access to the company associated with the subscription.

4.8.6 INVENTORY OF MITEL 6000 SIP PHONES

After the deployment of Mitel 6000 SIP Phones, it is necessary to check that they are visible in the integrated TMA inventory, with a software release corresponding to the production software release defined in the integrated TMA.

Note : The inventory lists all the terminals on the installation.

The **Inventory** menu is used to check the software release of Mitel 6000 SIP Phones after the deployment operation. Logged and unlogged terminals are listed.

- Click the Inventory menu.
- Select the 67xxxi range and possibly the model.
- Information about each terminal saved on its reference site is displayed.
    - The terminals associated with a production software release appear in green in the **Software version** column.
    - The terminals associated with a test software release appear in orange in the **Software version** column.
    - The terminals associated with any other software release appear in red in the **Software version** column.
    - Information display depends on the filter used. This filter is activated by clicking the **Magnifying glass** icon.
- If possible, apply a filter to the current inventory based on:
    - The terminal subscription number
    - The terminal IP address
    - The terminal software release (production, test release, etc.)
    - The terminal global data index
    - The terminal specific data index
    - The terminal MAC address
- Terminal encryption configuration:
    - SRTP (and TLS) mode activated
    - TLS mode activated
    - No encryption activated

Note : The joker * may be applied to the parameters Number, IP address and Mac address by placing it at the end of the parameter value.

- Click **Filter** to apply the filter to the current inventory.

The version of the terminals in the **Software release** column is green in colour if it is the same as the terminal software release defined as the production software release.

The logged column is used to indicate whether the Mitel 6000 SIP Phone is registered on its reference site (green tick) or whether the terminal is not registered on its reference site (red cross).

The **Periodic Logout** column is used to indicate whether or not the Mitel 6000 SIP Phone can periodically log out.

If the terminal is not registered on its reference site, a tooltip indicates the possible reason why the registration failed or whether the terminal is a general-purpose one.

The **Security** column indicates the encryption status of Mitel 6000 SIP Phones:

- Encrypted terminal in SRTP (and TLS):
- Encrypted terminal in TLS
- Terminal not encrypted: Empty
- Information not available:

(configuration file not present or encryption parameters not found)

4.9 PREPARING THE DEPLOYMENT OF TERMINALS FOR A NEW MIVOICE 5000 SERVER INSTALLATION

4.9.1 PRINCIPLE

For the MiVoice 5000 Server, the TMA, FTP and DHCP services are available and managed via Web Admin to facilitate terminal deployment. The FTP* and DHCP services must first be installed while starting the MiVoice 5000 Server in STANDARD or TOTAL RECONFIGURE mode before being managed via Web Admin.

ATTENTION : A service should only be installed if it is not used by the client for its own needs, especially the DHCP service. An installed service cannot be uninstalled.

Note : In general, MiVoice 5000 Server is integrated into a multi-site architecture and associated with the MiVoice 5000 Manager in which the FTP* and DHCP services are external.

Note : See also Implementing Mitel 5000 Gateways and MiVoice 5000 Server - AMT/PTD/PBX/0151* for more information about implementing an installation.

*: Required in the case of an upgrade or as long as there are terminals 53xxip in the installation.

4.9.2 CONFIGURING THE SYSTEM VIA CTRL I

It is possible to configure the telephony network IP address by double-clicking the **Standard reconfigure** shortcut, available on the MiVoice 5000 Server PC desktop.

Note : For a redundant MiVoice 5000 Server configuration, the Standard Reconfigure shortcut must be started from the active MiVoice 5000 Server PC:

If necessary, change the telephony network IP address.

Confirm the input by typing in **Y**.

4.9.3 CONFIGURING FLOW SEPARATION IN MIVOICE 5000 SERVER

The screen then displays the flow separation configuration for signals and data.

ATTENTION : Answer "N" and go to the next screen. If necessary, refer to the flow separation operating manual (AMT/PTD/PBX/0101*).

4.9.4 INSTALLATION OF INTEGRATED SERVICES IN MIVOICE 5000SERVER

This screen is used to install the integrated services on MiVoice 5000 Server which must be managed by Web Admin. By default, only the TFTP, ANNOUNCEMENT and IVR services are installed.

Note : The integrated DHCP service is available on a redundant MiVoice 5000 Server configuration.

- Type in "Y" to modify the configuration and configure the installation of the DHCP and Syslog services.
- Press "Y" to confirm the input.

4.9.5 AUTOMATIC START OF THE INTEGRATED SERVICES ON MIVOICE 5000 SERVER

The screen below is used to define the status of the integrated services during start-up.

By default, the TMA service is started automatically.

Note : These services can also be started later from Web Admin.

- Press "Y" to modify the configuration and set automatic start of the integrated FTP and DHCP services.
- Press "Y" to confirm the input.

4.9.6 CONFIGURING THE PARAMETERS FOR AUTOMATIC DEPLOYMENT OF MITEL 6000 SIP PHONES IN THE MIVOICE 5000 SERVER

The screen below is used to define the parameters for automatically deploying Mitel 6000 SIP Phones.

- Press "N". Press "Y" to modify the default configuration, if necessary.

See Section 6 for details and meaning of the parameters.

4.9.7 AUTOMATIC CONFIGURATION OF THE INTEGRATED DHCP SERVER PARAMETERS ON MIVOICE 5000 SERVER

The following screen is used to define the configuration parameters of the integrated DHCP server in the MiVoice 5000 Server. This menu is used to define the parameters that allow the integrated DHCP server to be configured automatically for the terminals.

Note : Manual configuration of the DHCP server is available from Web Admin and allows the modification of the automatic configuration defined via this menu. Refer to Section 6.

- Enter successively the configuration parameters of the integrated DHCP server, using the **Enter** key to change line.
- Press "Y" to confirm the input.
- Answer "**Y**" to the question:

```
Warning
Applying changes implies a iPBX restart
Do you want to apply your change Y(es) / N(o)/ R(econfigure)?
```

The procedure for configuring the system via **STANDARD RECONFIGURE** is completed and the system restarts.

4.9.8 RESTARTING MIVOICE 5000 SERVER

After the system is restarted, the automatic configuration phase last about 5 minutes.

During this period, the following main actions are taken:

- The DHCP server, integrated to manage the terminals is automatically configured.
- The new network parameters of the integrated FTP server are taken into account in the integrated downloading application.
- The production software release of the integrated TMA is automatically configured with the terminal software releases contained in MiVoice 5000.
- The global data configuration file used to deploy terminals is updated with the information entered previously during **STANDARD RECONFIGURE.**
- Some automatic actions are automatically started by the integrated TMA to update the software releases and global data configuration file of the terminals.

Note : In factory presetting, the global data configuration file used to deploy the terminals is automatically updated with the country-location and operation information.

Automatic terminal configuration is activated by default as well as automatic update of the dialling plan and system keys the terminals, the management of the terminals' programmable keys, languages and pictures (Menu **Telephony Service>Subscribers>Terminals and Applications>6xxxi parameters**).

The checks to be made before deploying the terminals are indicated in the following sections.

To access the configuration menus of the integrated TMA, click the **Terminal service** menu from Web Admin.

4.9.9 CHECKING THE CONFIGURATION OF THE DHCP SERVER INCORPORATED INTO MIVOICE 5000 SERVER

The **network** dedicated to terminals is automatically configured during **STANDARD RECONFIGURE**.

All models of the terminals associated with the terminal ranges can be configured for the **network**.

The **network** is also automatically configured with the information entered during **STANDARD RECONFIGURE**:

- Subnet name
- Sub-network address
- Subnet mask
- IP address range
- Lease duration
- Router IP address.

For this terminal range, the DHCP options are equally configured automatically using the information entered during **STANDARD RECONFIGURE**:

- Integrated download server IP address
- Main PBX IP address...

4.9.10 CHECKING THE CONFIGURATION OF THE DOWNLOAD SERVER INCORPORATED INTO MIVOICE 5000 SERVER

The storage directories used for day-to-day management and deployment of terminals are automatically created in the MiVoice 5000 Server system.

The configuration of the integrated download server used by the integrated TMA is automatically defined and can be viewed in the **Servers configuration** menu (Action: **Modify**:

4.9.11 CHECKING THE CONFIGURATION OF THE PRODUCTION SOFTWARE RELEASE OF TERMINALS

The production terminal software release is automatically defined after the factory pre-configuration made in the integrated TMA and in the Mitel 5000 Gateways system data.

The **Software management** menu is used to check the production terminal software release for each terminal range.

The information is displayed in the **Production software release** field.

4.10 DEPLOYING THE TERMINALS ON A NEW MIVOICE 5000 SERVER INSTALLATION

The procedure is identical to the one described for a Mitel 5000 Gateways system. See Section 4.8.

4.11 MANUAL DEPLOYMENT OF MITEL 6000 SIP PHONES

4.11.1 PRINCIPLE

This chapter describes how to manually update Mitel 6000 SIP Phones.

Once a Mitel 6000 SIP Phone is known in the TMA inventory, this terminal is managed by TMA, and it can be updated on a daily basis.

Note : Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.

Note : Mitel 6000 SIP Phone software and global data can be updated without any Mitel 6000 SIP Phone being physically connected to the network.

The terminal may also be updated **automatically** while updating the iPBX (see Section

Deploying and automatically updating).

The update may concern:

- The software release of Mitel 6000 SIP Phones
- The software of all Mitel 6000 SIP Phones regardless of their model and corresponds to the software update.
- The global data of Mitel 6000 SIP Phones
- The update of the global data of Mitel 6000 SIP Phones concerns all Mitel 6000 SIP Phones regardless of their model.
- The specific data of Mitel 6000 SIP Phones
- The software of all Mitel 6000 SIP Phones regardless of their model. This update applies to a list of terminals which may contain one, several terminals or all the terminals of a site.

Note : Updating the terminal data requires distributing the parameters first (refer to Section Distributing the new test release**).**

- **The first step** consists in:
  - Installing a new terminal software release in TMA
  - Updating the terminals' global data in TMA
  - Updating the terminals' specific data in TMA from a list.
- **The second step** consists in starting the following operations from TMA:
  - Terminal software release update
  - Terminal global data update
  - Specific data update for terminals on a list

Note : All or part of these three actions can be started consecutively.

This update operation makes it possible to place the following data in the storage directory of the download server concerned:

- The new terminal software release
- The new terminal global data file
- The new terminal specific data files on a list.

For each set of data managed, an indicator (version or index) is used to identify the transmitted file without ambiguity.

Note : All or part of this data may be available in the storage directory, depending on the actions started previously.

This update operation also updates in the PBX:

  - Information about the new terminal release to update
  - The new values of the global and specific data index.

- **The third step** will enable the terminal to be updated automatically:
  - Next time the REGISTER is transmitted by the terminal, the data contained in the REGISTER is returned to the PBX. This data contains, among others, the current version of the terminal and the current values of the terminal's global and specific data index.
  - The PBX compares this terminal data with the data stored and saved previously in the PBX in step 2.

- If at least any set of this data is different, the PBX transmits to the terminal an update order containing the IP address of the download server to which to connect, the account to use and the type of update to make.
- This update order is followed by a terminal restart order. The terminal will then connect to the right download server and transfer the files concerned by the type of ordered update to the terminal.

ATTENTION : The processing method used by TMA is asynchronous. The terminal update order also depends on REGISTER reception, the default rate of which is 1 hour.

4.11.2 GLOBAL DATA UPDATE

This procedure allows the global data of all Mitel 6000 SIP Phones to be updated.

- Click the Terminal configuration menu.
- Select the 6xxxi range.
- In the Version to configure field, select the version concerned by the global data update.
- Click the Modify global parameters link:
- A new window opens.

This enables you to check the criteria concerned by global data update:

- The Terminal range concerned: 6xxxi.
- The terminal model concerned: all models.
- The terminal software concerned.
- The list of terminals concerned: global_file (this information indicates that the global data update concerns all terminals known in Mitel 6000 SIP Phones).

A distribution of the parameters in form of tabs is only displayed for Mitel 6000 SIP Phones:

- **Encryption**: encryption parameters for Mitel 6000 SIP Phones
- **Config**: the usual configuration parameters
- **TimeZone**: date and time, NTP server, time zone configuration parameters
- **Network**: network parameters (DHCP, VLAN, LLDP,..)
- **RFC2833**: RFC2833 / SIP INFO configuration parameters
- **802.1X**: 802.1X configuration parameters
- **RTCP**: RTCP configuration parameters
- **Directory:** configuration parameters for access to the LDAP directory and Exchange contacts (function available as of R6.2)
- **Expert**: all the other parameters not available in the previous tabs
- This window also presents a table containing four columns:
- The **Parameters** column lists the parameters contained in the global data configuration file available in TMA. This list is from the distribution made previously.
- The **Default values** column displays the default values of the parameters contained in the factory description file available in TMA.
- The **Current values** column displays the current values of the parameters contained in the global data configuration file available in TMA.

ATTENTION : After manual deployment via TMA, these values will be those imported via the global .csv file. For a deployment through manual login, these values will be the ones contained by default in the factory description.

- The **Values to transfer** column displays the values to update in the global data configuration file available in TMA.
- Update the value of the parameter concerned in the **Values to transfer** column then click **Next**.

Note : Pop-ups give information on how to enter the value of each of the parameters. These latter appear when the cursor is placed over the current value of the parameter.

Note : The Default values button is used to initialise the values to transfer with the default values for the tab in question.

Note : A consistency check is made while validating the modifications. The number of errors is displayed and incorrect parameters appear with a message specifying the expected format (values outside the limit, for instance).

A new window opens.

This indicates the criteria concerned by global data update:

- The Terminal range concerned: 6xxxi.
- The terminal model concerned: all models.
- The terminal software concerned.
- The list of terminals concerned: global_file (this information indicates that the global data update concerns all terminals known in Mitel 6000 SIP Phones).

The **Number of global data files to transfer** is also indicated.

- Enter the Action name.
- Select the Type of update:
  - Immediate
  - Deferred: specify the date in DD/MM/YYYY format and time in HHMM format.

Note : Clicking the  **icon opens the calendar so the date can be selected directly.**

- Click **Confirm** to start global data update.

ATTENTION : Any action started in deferred mode defers the transfer of data to the download server and the iPBX data update order.

4.11.2.1 *Checking that the global data update process is working correctly*

This operation is used to ensure that the global data update operation has been performed correctly.

- Click the Action monitoring menu.
- Check in Action monitoring, the status of the global data update operation:
  - if the operation was successful, the status indicates: **Successful.**
- Click the **Magnifying glass** icon to view the progress of the on-going global data update operation.
  - A colour code is used to check whether the terminal's global data is actually in the expected index (green colour) or not (red colour). This colour code is only significant for the last action of this type. The information displayed may or may not be filtered with this criterion.
- Check in the **Event log,** the status of the global data update operation.
- If the operation was successful, the status indicates: Action successful. Action on MiVoice 5000 PBX taken into account.
- The number of transferred files is used to check that the global file is actually placed in the storage directory of the download server used for day-to-day terminal management.
- The report also indicates the system concerned by the action.

4.11.3 SPECIFIC DATA UPDATE

4.11.3.1 *Updating common specific data*

This procedure applies once a terminal is registered on its reference site via any of the deployment methods described in the previous sections and when it appears in the TMA inventory. This procedure updates the common specific data of a list of Mitel 6000 SIP Phones. For example, if you wish to configure encryption for all the terminals on a list.

Note : Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.

Note : See Section Managing the list of terminals for Mitel 6000 SIP **for terminal list management.**

This procedure updates the specific data for a list of terminals.

Click the **Terminal configuration** menu.

- Select the **6xxxi** range.
- In the field **Version to configure**, select the version concerned by the specific data update.
- Click the link **Modify specific parameters**.
- A new window opens.

This indicates the criteria concerned by specific data update:

- The Terminal range concerned: 6xxxi.
- The terminal model concerned: all models.
- The terminal software concerned.
- Select the list of terminals concerned by the specific data update.

Note : The "All" list is defined by default and contains all the terminals known to the inventory for the terminal range, the terminal model and multisite concerned. See Section Managing the list of terminals for Mitel 6000 SIP **for list management.**

A distribution of the parameters in form of tabs is only displayed for Mitel 6000 SIP Phones:

- **Encryption**: encryption parameters for Mitel 6000 SIP Phones
- **Config**: the usual configuration parameters
- **TimeZone**: date and time, NTP server, time zone configuration parameters
- **Network**: network parameters (DHCP, VLAN, LLDP,..)
- **RFC2833**: RFC2833 / SIP INFO configuration parameters
- **802.1X**: 802.1X configuration parameters
- **RTCP**: RTCP configuration parameters
- **Directory:** configuration parameters for access to the LDAP directory and Exchange contacts (function available as of R6.2)
- **Expert**: all the other parameters not available in the previous tabs

This window also presents a table containing three columns:

- When ticked, the **C** column is used to select a specific parameter for which the new value entered will be the same for all the terminals on the previously selected list.
- The **Parameters** column lists the parameters contained in the specific data configuration file available in TMA. This list is from the distribution made previously.
- The **Common values** column is used to enter the new value of a specific parameter selected via the **C** column.

Note : Pop-ups give information on how to enter the value of each of the parameters. These latter appear when the cursor is placed over the current common value of the parameter.

- Select one or more parameters then enter the new value for this parameter/these parameters.

Note : A consistency check is made while validating the modifications. Incorrect parameters appear with a message specifying the expected format (values outside the limit, for instance).

- Click **Save**. If no parameter is incorrect, a new window opens.
- This indicates the criteria concerned by specific data update:
  - The Terminal range concerned: 6xxxi.
  - The terminal model concerned: all models.
  - The terminal software concerned.
  - The List of terminals concerned

This window also presents a table containing five columns:

  - When ticked, the **C** column is used to select one or more terminals for which some specific data will be entered if necessary based on terminals (see next chapter for implementation).
  - The other columns display the **Subscription number**, **Software release**, **IP address** and **Mac address** of each of the terminals on the previously selected list.

- Do not tick any terminal in the **C** column then click **Confirm**.
- A new window opens.

This indicates the criteria concerned by specific data update:

- The Terminal range concerned: 6xxxi.
- The terminal model concerned: all models.
- The terminal software concerned.
- The List of terminals concerned

The **Number of specific data files to transfer** is also indicated.

- Enter the Action name.
- Select the Type of update:
  - Immediate
  - Deferred: specify the date in DD/MM/YYYY format and time in HHMM format.

Note : Clicking the  **icon opens the calendar so the date can be selected directly.**

- Click **Confirm** to start specific data update for a list of terminals.

ATTENTION : Any action started in deferred mode defers the transfer of data to the download server and the iPBX data update order.

4.11.3.2 *Updating individual specific data*

This procedure updates the particular specific data of one or more terminals on a list of terminals. For example, if you wish to update the VLAN_ID of a list of terminals.

- Click the Terminal configuration menu.
- Select the 6xxxi range.
- In the Version to configure field, select the version concerned by the specific data update.
- Click the link Modify specific parameters.
- A new window opens.

This indicates the criteria concerned by specific data update:

- The Terminal range concerned: 6xxxi.
- The terminal model concerned: all models.
- The terminal software concerned.
- Select the list of terminals concerned by the individual specific data update.

Note : The "All" list is defined by default and contains all the terminals known to the inventory for the terminal range, the terminal model and multisite concerned. See Section Managing the list of terminals for Mitel 6000 SIP **for list management.**

A distribution of the parameters in form of tabs is only displayed for Mitel 6000 SIP Phones:

- **Encryption**: encryption parameters for Mitel 6000 SIP Phones
- **Config**: the usual configuration parameters
- **TimeZone**: date and time, NTP server, time zone configuration parameters
- **Network**: network parameters (DHCP, VLAN, LLDP,..)
- **RFC2833**: RFC2833 / SIP INFO configuration parameters
- **802.1X**: 802.1X configuration parameters
- **RTCP**: RTCP configuration parameters
- **Directory:** configuration parameters for access to the LDAP directory and Exchange contacts (function available as of R6.2)
- **Expert**: all the other parameters not available in the previous tabs

This window also presents a table containing three columns. This is the common data for the terminal list. Their meaning is described in the previous chapter.

  - If possible, select one or more parameters then enter the new common value for this parameter/these parameters.
  - Click **Save:** a new window opens.

This indicates the criteria concerned by specific data update:

- The Terminal range concerned: 6xxxi.
- The terminal model concerned: all models.
- The terminal software concerned.
- The List of terminals concerned.

This window also presents a table containing five columns:

- When ticked, the **C** column is used to select one or more terminals for which some particular specific data will be entered based on terminals.
- The other columns display the **Subscription number**, **Software release**, **IP address** and **Mac address** of each of the terminals on the previously selected list.

- Select one, more or all the terminals by ticking them in the **C** column.
- Click **Validate**.
- A new window opens.

This indicates the criteria concerned by particular specific data update:

- The Terminal range concerned: 6xxxi.
- The terminal model concerned: all models.
- The terminal software concerned.
- The List of terminals concerned
- The subscription number concerned.
- The MAC address of the subscription concerned.

This window also presents by tab a table containing four columns:

- The **Parameters** column lists the parameters contained in the specific data configuration file available in TMA. This list is from the distribution made previously.
- The **Default values** column displays the default values of the parameters contained in the factory description file available in TMA.
- The **Current values** column displays the current values of the parameters contained in the specific data configuration file of the terminal concerned, available in TMA.

ATTENTION : After manual deployment via TMA, these values will be those imported via the specific .csv file. For a deployment through manual login, these values will be the ones contained by default in the factory description.

- The **Values to transfer** column displays the values to update in the specific data configuration file of the terminal concerned in TMA.

Note : Pop-ups give information on how to enter the value of each of the parameters. These latter appear when the cursor is placed over the current value of the parameter.

Note : The Default values button is used to initialise the values to transfer with the default values for the tab in question.

- Update the value of the parameter(s) concerned in the **Values to transfer** column then click **Next** to go to the next terminal.

Note : The Initialize button allows you to reset all terminal parameters to their current value.

Note : A consistency check is made while validating the modifications. Incorrect parameters appear with a message specifying the expected format (values outside the limit, for instance).

- After modifying the last terminal selected, click **Create action**.
- A new window opens.

This indicates the criteria concerned by specific data update:

- The Terminal range concerned: 6xxxi.

- The terminal model concerned: all models.
- The terminal software concerned.
- The List of terminals concerned

The **Number of specific data files to transfer** is also indicated.

- Enter the Action name.
- Select the Type of update:
  - Immediate
  - Deferred: specify the date in DD/MM/YYYY format and time in HHMM format.

Note : **Clicking the  icon opens the calendar so the date can be selected directly.**

- Click **Validate** to start specific data update for a list of terminals.

ATTENTION : Any action started in deferred mode defers the transfer of data to the download server and the PBX data update order.

4.11.3.3 *Checking that the specific data update process is working correctly*

This operation is used to ensure that the specific data update operation has been performed correctly.

- Click the Action monitoring menu.
- Check in Action monitoring, the status of the specific data update operation:
  - if the operation was successful, the status indicates: **Success**
- Click the **Magnifying glass** icon to view the progress of the on-going specific data update operation.
- A colour code is used to check whether the terminal's specific data is actually in the expected index (green colour) or not (red colour). This colour code is only significant for the last action of this type. The information displayed may or may not be filtered with this criterion.
- Check in the **Events log** the status of the specific data update operation.
  - if the operation was successful, the status indicates: Action successful. Action on MiVoice 5000 PBX taken into account.
  - The number of transferred files is used to check that all the specific files are actually placed in the storage directory of the download server used for day-to-day terminal management. The report also indicates the system concerned by the action.

4.11.4 UPDATING THE SOFTWARE RELEASE OF MITEL 6000 SIP PHONES

This procedure allows the software release of all Mitel 6000 SIP Phones to be updated.

Note : Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.

4.11.4.1 *Installing the new software release to be deployed*

The new packages must have been loaded on the Repository server.

As of R6.5, only the Repository Update method allows the terminal software update.

See the document Upgrading by repository AMT/PTD/PBX/0155/2, Edition 2 minimum for R6.5).

The integrated TMA then connects directly to the upgrade server to list the available **terminal**packages.

- Click the Software management menu.
- Select the 6xxxi range.
- Click Change.
- Click the Add versions link.

This application is used to query the upgrade functions.

After selecting the range, a combo box shows the packages available on the server.

A new window opens, showing the list of available software releases.

- Select the release concerned.

Once the release has been selected, the list of components in this package is displayed.

The components corresponding to the managed models are preselected.

- Tick or untick if necessary the terminal models to be updated.
- Click **Download.**

The download of software updates is then launched to the iPBX for managed models.

Once the download is successful, close the window.

The new releases are available for configuration, either as a production release or as a test release on the terminals in question. See the following sections.

4.11.4.2 *Defining the new production release*

This procedure is used to define the new production software release.

- Click the Software management menu.
- Select the 6xxxi range.
- Click Change.
- Click the link Configure production software release.
    - Select the new release and click **Validate**.

Note : The new software release is now the production release and all the terminals can appear in red in the inventory (terminals seen in another software release).

4.11.4.3 *Starting the update of the new production release*

- Click **Return**.
- A new window opens.

This indicates the criteria concerned by the update of the new software release:

- The Terminal range concerned: 6xxxi

- The Production software release concerned:

- Enter the Action name.
- Select the **Software release** concerned:
- Select the **Type of update**:
  - Immediate
  - Deferred: specify the date in DD/MM/YYYY format and time in HHMM format.

Note :
Clicking the  icon opens the calendar so the date can be selected directly.

- Click **Validate** to start updating the software release of all Mitel 6000 SIP Phones.

4.11.4.4 *Checking that the production software release update is working correctly*

This operation is used to ensure that the new software release has been correctly updated.

- Click the **Action monitoring** menu.
- Check in **Action monitoring,** the status of the production release update operation:
  - if the operation was successful, the status indicates: **Successful.**
- Click the **Magnifying glass** icon to view the progress of the on-going production release update operation.
- A colour code is used to check whether the terminals have the expected software release (green colour) or not (red colour). This colour code is only significant for the last action of this type. The information displayed may or may not be filtered with this criterion.
- Check in the **Events log** the status of the terminal software release update operation.
- if the operation was successful, the status indicates: Action successful. Action on MiVoice 5000 PBX taken into account.
- The number of transferred files is used to check that all new software release files have actually been placed in the storage directory of the download server used for day-to-day terminal management. The system concerned by the action is also indicated.

4.11.5 DISTRIBUTING THE NEW PRODUCTION VERSION PARAMETERS

This procedure is used to distribute the parameters associated with a new software release installed in TMA. The range of each parameter is given.

A parameter is defined either:

- In the Mitel 6000 SIP Phones' global data configuration file
- In the specific data configuration file of Mitel 6000 SIP Phones
- In the DHCP server
- Or in none of the previous ranges, so this parameter is not managed.

This distribution must be made for each software release installed and configured in TMA as production release or test release.

- Click the Terminal configuration menu.
- Select the 6xxxi range.
- In the field Version to configure, select the version concerned by the distribution.

A distribution of the parameters in form of tabs is only displayed for Mitel 6000 SIP Phones:

- **Encryption**: encryption parameters for Mitel 6000 SIP Phones
- **Config**: the usual configuration parameters
- **TimeZone**: date and time, NTP server, time zone configuration parameters

- **Network**: network parameters (DHCP, VLAN, LLDP,...)
- **RFC2833**: RFC2833 / SIP INFO configuration parameters
- **802.1X**: 802.1X configuration parameters
- **RTCP**: RTCP configuration parameters
- **Directory:** configuration parameters for access to the LDAP directory and Exchange contacts (function available as of R6.2)
- **Expert**: all the other parameters not available in the previous tabs

Note : To facilitate the introduction of certain features (encryption, etc.), some parameters are available twice in the tab:
- in the upper part, the parameters have a range and some fixed values.
- in the lower part, the same parameters have a default value which may differ and a range set to ignored.

- Select a tab and define its range for each parameter present in this tab.

Note : Following an upgrade of the iPBX, the range defined in terminal software release n-1 is retained in terminal software release n. The range of the new parameters introduced in the new terminal software release must be defined.

- Click **Save**:
  - Clicking **Distribute** displays a confirmation message before the distribution of parameters is locked for this software release.
  - The **Initialise** button restores the factory distribution of the parameters associated with this software release.

Note : The parameters managed by DHCP, or ignored, are displayed for information purposes only.

Note : It is possible to unlock the distribution of parameters and make a new distribution. In this case, the global and specific data must be updated in order to update the values of the parameters whose assignment has been changed.

4.11.6 MANAGING THE LIST OF TERMINALS FOR MITEL 6000 SIP PHONES

This procedure is used to define a list of terminals for all Mitel 6000 SIP Phone models.

This list is used either:

- In nominal mode, to update some specific data on a global or restricted range, or
- In test mode, to update the terminals' software release, global data and specific data on a limited range.

ATTENTION : A terminal may be assigned only to one list at a time.

The list used in test mode to update the terminal software release must be the same as the one used to update the global data and specific data.

4.11.6.1 *Defining a new list by entering the terminals one by one*

- Click the **Inventory** menu.
- Select the **6xxxi** range and possibly the **model**.
- Click **List management:**

A new window opens. This window gives the criteria concerned by the list creation:

- The Terminal range concerned: 6xxxi.
- The Terminal model concerned.

- Click Add new list.

A new window opens. This window allows you to enter one by one the terminals contained in the list.

- In the right input area, for each terminal to be added to the list, enter the directory number of the terminal then click **Add set**.

Note : To delete a terminal from the currently edited list, select the terminal then click Delete.

- In the right area, enter the **List name** then click **Validate**.
  - This message appears: the list has been successfully saved.
- Close the window either by clicking the **Close window** link, or by clicking on the top right side of the window.
- The list management window is refreshed and then displays:
  - The list name
  - The number of terminals contained in the list
  - The **Action** field used to delete or modify the displayed list.
- Click **Return** to return to the **Inventory** window.

4.11.6.2 *Modifying a list*

- Click the **Inventory** menu.
- Select the **6xxxi** range and possibly the **model**.
- Click **List management:**

A new window opens. This window gives the criteria concerned by the list creation:

- The Terminal range concerned: 6xxxi.
- The Terminal model concerned.

- In the **Action** field, click the  icon of the list to modify.
- Modify the list by adding or deleting a terminal.
- Click **Validate**.
  - This message appears: the list has been successfully saved.
- Close the window either by clicking the **Close window** link, or by clicking on the top right side of the window.
- The **List management** window is refreshed and then displays:
  - The list name
  - The new number of terminals contained on the list.
- Click **Return** to return to the **Inventory** window.

4.11.6.3 *Deleting a list*

- Click the **Inventory** menu.
- Select the **6xxxi** range and possibly the **model**.
- Click **List management:**

A new window opens. This window gives the criteria concerned by the list creation:

  - The Terminal range concerned: 6xxxi.
  - The Terminal model concerned.

- In the **Action** field, click the  icon of the list to delete:
  - A confirmation message is displayed so you can confirm or cancel the list deletion.
- The **List management** window is refreshed and the deleted list no longer appears.
- Click **Return** to return to the **Inventory** window.

4.12 TEST MODE FOR MITEL 6000 SIP PHONES

Test mode is used to update the terminals' software release, global data and specific data. This function is used to test a new terminal software application or new function/configuration on a small number of terminals before exposing it to all the terminals.

The list of terminals used in test mode to update the terminal software release must be the same as the one used to update the global data and specific data of the tested terminals.

The different files (terminal software, global or specific data) are stored in the **test directory** defined in the external download server configuration.

4.12.1 UPDATING THE SOFTWARE RELEASE OF MITEL 6000 SIP PHONES IN TEST MODE

This procedure applies once a terminal is registered on its reference site via any of the deployment methods described in the previous chapters and when it appears in the TMA inventory. This procedure is used to update the software release of the Mitel 6000 SIP Phones known to the inventory and defined on a list containing at most 10 terminals.

In the example below:

- The production release = **R6.2_67xxi_A5_00**
- The test release = **R6.2_67xxi_A6_00**

ATTENTION : In test mode, only one software release update operation can be performed at a time for a list of terminals.

4.12.1.1 *Defining a test list*

See Section Managing the list of terminals for Mitel 6000 SIP for how to define a list of terminals containing a maximum of 10 terminals.

This list, called **test** , will be used in the procedure described below.

ATTENTION : A list used by an on-going test cannot be deleted or modified.

4.12.1.2 *Defining the new test release*

This procedure is used to define the new test software release.

- Click the **Software management** menu.
- Select the **6xxxi** range.
- Click **Change**.
- Click the link **Configure test software release**:
- Select the previously installed terminal software package **R6.2_67xxi_A6_00** then click **Validate**.

Note : Terminal software package R6.2_67xxi_A6_00 is now the test terminal software package.

4.12.1.3 *Starting the update of the new test version*

- Click **Return**.
- A new window opens.

This indicates the criteria concerned by the update of the new software release:

- The Terminal range concerned: 6xxxi.
- The Production software release concerned: R6.2_67xxi_A5_00.
- The Test software release concerned: R6.2_67xxi_A6_00

Note : The Details button is used to know the content of the terminal software package.

- Enter the Action name.
- Select the test Software release: R6.2_67xxi_A6_00.
- Select the list to use in test mode: **test**
  - The **List details** link is used to display the terminals contained in the selected list.
- Select the Type of update:
  - Immediate
  - Deferred: specify the date in DD/MM/YYYY format and time in HHMM format.

Note : Clicking the  **icon opens the calendar so the date can be selected directly.**

- Click **Validate** to start updating the software release of all Mitel 6000 SIP Phones.

4.12.1.4 *Checking that the test software release update is working correctly*

This operation is used to ensure that the new test software release has been correctly updated.

- Click the **Action monitoring** menu.
- Check in **Action monitoring**, the status of the test software release update operation: if the action is successful, the status indicates: **Success**

- Click the **Magnifying glass** icon to view the progress of the on-going test software release update operation.
    - A colour code is used to check whether the terminals have the expected software release (green colour) or not (red colour). This colour code is only significant for the last action of this type. The information displayed may or may not be filtered with this criterion.
- The **List** field displays the list used in test mode: **test**
- The **Test** field is used to check whether or not the on-going operation is in test mode.
- Check in the **Events log** the status of the test software release update operation.
- if the operation was successful, the status indicates: Action successful. Action on MiVoice 5000 PBX taken into account.
- The number of transferred files is used to check that all new test software release files have actually been placed in the test storage directory of the download server used for day-to-day terminal management in test mode.

4.12.2 DISTRIBUTING THE NEW TEST RELEASE PARAMETERS

See Section Distributing the new test release for how to define the distribution of the new test software release parameters.

4.12.3 UPDATING THE GLOBAL DATA OF TERMINALS IN THE TEST SOFTWARE RELEASE

This procedure is used to update the global data of Mitel 6000 SIP Phones in the test software release.

- Click the Terminal configuration menu.
- Select the 6xxxi range.
- In the field Version to configure, select the test version concerned by the global data update (R6.2_67xxi_A6_00 in the example).
- Click the Modify global parameters link:
- A new window opens.

This enables you to check the criteria concerned by global data update on the test software release:

- The Terminal range concerned: 6xxxi.
- The terminal model concerned: all models.
- The terminal software concerned. R6.2_67xxi_A6_00.
- The list of terminals concerned: test (this information shows that the global data update applies to the test list, currently used in test mode). The List details link is used to display the terminals contained in the selected list.

See the section concerned for information on how to program the global data update in test mode, except that the list concerned by the action is not the **global_file** list but the list in test mode, called **test** in our example.

4.12.3.1 *Checking that the global data update process is working correctly in test mode*

This operation is used to ensure that the global data update in test mode has been performed correctly.

- Click the **Action monitoring** menu.
- Check in **Action monitoring,** the status of the global terminal data update in test mode. If the action is successful, the status indicates: **Successful.**
- Click the **Magnifying glass** icon to view the progress of the on-going global data update operation.
    - The **List** field displays the list used in test mode: **test.**
    - The **Test** field is used to check whether or not the on-going operation is in test mode.

- A colour code is used to check whether the terminal's global data is actually in the expected index (green colour) or not (red colour). This colour code is only significant for the last action of this type. The information displayed may or may not be filtered with this criterion.

- Check in the **Event log** the status of the global terminal data update in test mode.
  - if the operation was successful, the status indicates: Action successful. Action on MiVoice 5000 PBX taken into account.
  - The number of transferred files is used to check that the global file has actually been placed in the test storage directory of the download server used for terminal test mode.

4.12.4 UPDATING THE SPECIFIC DATA OF TERMINALS IN THE TEST SOFTWARE RELEASE

This procedure is used to update the specific data of Mitel 6000 SIP Phones in the test software release.

4.12.4.1 *Updating the common specific data of terminals in the test software release*

This procedure is used to update the specific data of terminals in the test software release.

- Click the Terminal configuration menu.
- Then select the 6xxxi range.
- In the field Version to configure, select the test release concerned by the specific data update. (R6.2_67xxi_A6_00 in the example).
- Click the link Modify specific parameters.
- A new window opens.

This indicates the criteria concerned by specific data update:

- The Terminal range concerned: 6xxxi
- The terminal model concerned: all models.
- The terminal software concerned: R6.2_67xxi_A6_00
- The list of terminals concerned: test (this information shows that the specific data update applies to the test list, currently used in test mode).

Note : It is not possible in test mode to start a specific data update operation on the production release using the "All" list.

4.12.4.2 *Updating the individual specific data of terminals in the test software release*

This procedure is used to update the special specific data of terminals in the test software release.

- Click the Terminal configuration menu.
- Then select the 6xxxi range.
- In the field Version to configure, select the test release concerned by the specific data update. (R6.2_67xxi_A6_00 in the example).
- Click the link Modify specific parameters.
- A new window opens.

This indicates the criteria concerned by specific data update:

- The Terminal range concerned: 6xxxi
- The terminal model concerned: all models.
- The terminal software concerned: R6.2_67xxi_A6_00
- The list of terminals concerned: test (this information shows that the specific data update applies to the test list, currently used in test mode).

Note : It is not possible in test mode to start a specific data update operation on the production release using the "All" list.

Note : The greyed out values represent the canonical values of each parameter.

See Section **Erreur ! Source du renvoi introuvable.** for information on how to program the i ndividual specific data update in test mode, except that the list concerned by the action is the list in test mode, called test in our example.

4.12.4.3 *Checking that the specific data update process is working correctly in test mode*

This operation is used to ensure that the specific data update in test mode has been performed correctly.

- Click the **Action monitoring** menu.
- Check, in **Action monitoring,** the status of the specific data update in test mode. If the action is successful, the status indicates: **Successful.**
- Click the **Magnifying glass** icon to view the progress of the on-going specific data update operation.
    - The **List** field displays the list used in test mode: **test**
    - The **Test** field is used to check whether or not the on-going operation is in test mode.
    - A colour code is used to check whether the terminal's specific data is actually in the expected index (green colour) or not (red colour). This colour code is only significant for the last action of this type. The information displayed may or may not be filtered with this criterion.
- Check in the **Event log** the status of the specific data update operation.
- if the operation was successful, the status indicates: Action successful. Action on MiVoice 5000 PBX taken into account.
- The number of transferred files is used to check that all the specific files have actually been placed in the test storage directory of the download server used for terminal test mode.

4.12.6 EXITING THE TEST MODE

This procedure is used to leave the test mode at the end of the test phase.

Two possibilities are available:

- The tested new release is satisfactory: in this case, all the terminals on the installation must be updated with the new test software.
- The tested new release is not satisfactory: in this case, only the tested terminals must be updated with the current production software release.

4.12.6.1 *Switching from test mode to production mode*

In this case, the test software release must be defined as the new production software release, and an update operation for this new production software release started on all the terminals.

In the example below the initial situation is as follows:

- production release = R6.2_67xxi_A5_00
- test release = R6.2_67xxi_A6_00
- Click the Software management menu.
- Select the 6xxxi range.
- Click Change.
- Click the link Configure production software release.
    - Select the release **R6.2_67xxi_A6_00** and click **Validate**.
    - The situation is now:
    - The production release = **R5.3_67xxi_A9_00**
    - No test version defined.
- Click **Return**.
- A new window opens.

  This indicates the criteria concerned by the update of the new software release:
    - The Terminal range concerned: 6xxxi
    - The Production software release concerned: R6.2_67xxi_A6_00
- Enter the Action name.
- Select the software release concerned: R6.2_67xxi_A6_00.
- Select the Type of update:
    - Immediate
    - Deferred: specify the date in DD/MM/YYYY format and time in HHMM format.

Note :

Clicking the  icon opens the calendar so the date can be selected directly.

- Click **Validate** to start updating the new production software release of all Mitel 6000 SIP Phones.

4.12.6.2 *Returning to the current version*

In this case, the test software release is not satisfactory. The terminals on the test list must be downgraded with the current production release. An update for this production software release must be started on all the terminals.

In the example below the initial situation is as follows:

- production release = **R6.2_67xxi_A5_00**
- test release = **R6.2_67xxi_A6_00**

- Click the **Software management** menu.
- Select the **6xxxi** range.
- Enter the **Action name**.
- Select the **Software release** concerned: **R6.2_67xxi_A5_00**
- Select the **Type of update**:
  - Immediate
  - Deferred: specify the date in DD/MM/YYYY format and time in HHMM format.

Note : Clicking the  icon opens the calendar so the date can be selected directly.

- Click **Validate** to start updating the current production software release of all Mitel 6000 SIP Phones.

Note : Only the terminals with the test software release will be updated with the current production software release because all the other terminals are already in the right version.

4.13 ADDITIONAL TMA FUNCTIONS

4.13.1 DOWNLOADING FILES INDIVIDUALLY

A single file can be uploaded to the FTP server(s).

This feature allows you to make the following available, for Mitel 6000 SIP Phones, on the FTP server(s):

- Template files **(model.cfg**),
- Certificates **(ca.crt**) when encryption is enabled and an external certificate is used.

To download a file individually, proceed as follows:

- Click the **Deployment** menu.
    - Select the (**6xxxi**) range.
    - From the **List of servers**, select the server to which the template file or certificate must be downloaded.
- In the **Other file** field import, by clicking **Browse**, the template file (Mitel 6000 SIP Phone.cfg) or certificate (ca.crt) to be downloaded.
- Click **Validate**.
- Enter the **Action name**.
- Select **the type of update** (immediate or deferred).
- Click **Validate**.
- In **Action monitoring** check that the file is correctly downloaded individually to the download server.

ATTENTION : A server must be selected. Only one file is allowed per deployment operation.

ATTENTION : Some file name checks are made.

- **This file cannot be a global data file; therefore, the name must be different from aastra.cfg (if the 6xxxi range is selected).**
- **If configuration file encryption is activated, the *.cfg files downloaded individually are encrypted before being sent to the download server because they will not be taken into account.**

ATTENTION : The terminal must be restarted so the template file or certificate can be taken into account.

These files are backed up in the local TMA directory and proposed again for downloading via the combo box **Files previously downloaded** in the **Deployment** menu.

After selecting a file previously downloaded individually, the following actions may be taken on these backed up files:

- Viewing (via the **View** button): a new window opens, displaying the content of the file,
- Deletion (via the **Delete** button): after confirmation, the file is locally deleted; it will still be available on the download servers on which it may have been deployed.

4.13.2 EXPORTING THE DATA CONTAINED IN THE CONFIGURATION FILES OF MITEL 6000 SIP PHONES

The global and specific data of terminals with a production or test software release may be exported in **.csv** format from the **Terminals configuration export** menu.

- Click the Terminal configuration **Export** menu.

- Select the range and possibly the model.
- To export the data of terminals with the production software release:
- Click **Prod data**.
- Click the global data file link to export the global data of terminals with the production software release.
- Click **Save** to back up the file export_global.csv.
- Click Save again after selecting the target directory.
- Click the specific data file link to export the specific data of terminals with the production software release.
- Click **Save** to back up the file **export_specific.csv**.
- Click **Save** again after selecting the target directory.
- To export the data of terminals with the test software release:
- Click **Test data**.

Then proceed as described above to save the export files.

4.13.3 EXPORTING THE DATA CONTAINED IN THE INVENTORIES OF MITEL 6000 SIP PHONES

Export is only possible on the terminals available in the inventory. A filter can be applied before exporting the data.

- Click the **Inventory** menu.
- Select the **range** and possibly the **model**.
- Information about each terminal saved on its reference site is displayed.
    - The terminals associated with a production software release appear in green in the **Software version** column.
    - The terminals associated with a test software release appear in orange in the **Software version** column.
    - The terminals associated with any other software release appear in red in the **Software version** column.
    - Information display depends on the filter used. This filter is activated by clicking the  icon.
- If possible, apply a filter to the current inventory based on:
    - The terminal subscription number
    - The terminal IP address
    - The terminal software release (production, test release, etc.)
    - The terminal global data index
    - The terminal specific data index
    - The terminal MAC address
    - Terminal encryption configuration:

      SRTP (and TLS) mode activated (terminals 53xxip and 6xxxi)

      TLS mode activated (terminals 6xxxi)

      No encryption activated.

Note : The joker * may be applied to the parameters Number, IP address and Mac address by placing it at the end of the parameter value.

- Click **Filter** to apply the filter to the current inventory.
- Click the  icon to start exporting the data available in the inventory.
- Click **Save** to save the file as **journal.csv**.
- Click **Save** again after selecting the target directory.

Note : The export function is also available from Action monitoring.

4.13.4 PRINTING THE DATA CONTAINED IN THE INVENTORIES OF MITEL 6000 SIP PHONES

The terminal data displayed in the inventory can be printed out. A filter can be applied before printing the data.

See Section Exporting the data contained in the inventories for how to select the terminals displayed in the inventory.

- Click the  icon to start printing the data available in the inventory.
- The data can be previewed in a window before being printed.
- Click **Print** to start printing the data.

Note : The print function is also available from Action monitoring.

4.13.5 EVENT LOG

The event log is basically used to check the status of the following actions:

- Deployment
- Terminal software release update
- Terminal global data update
- Terminal specific data update

Each action is identified by the following information:

- The **Date** on which the action was started
- The **Time** the action was started
- The name of the **User** who started the action
- The type of**Action** concerned
- The **Name of the action** concerned
- The **Status** of the action concerned

The information displayed may be filtered with certain criteria:

- Click the Events log menu.
- Select any of the following:
    - User
    - Action

- Status
- Start date and End date

Note : Clicking the  icon opens the calendar so the start and end dates can be selected directly.

- Click **Filter** for the filtering criteria to become effective.

Note : Clicking Initialise deletes the filter criteria and displays the entire information.

In case of operation error, the events log is used to identify the cause of the error: The following cases are taken into account:

- Network problem: no response to PING (problem accessing the MiVoice 5000 PBX)
- APACHE problem: HTTPS request timed out (problem accessing the MiVoice 5000 PBX web server)
- **MMC** service is stopped (problem accessing the MiVoice 5000 PBX MMC).
- Incorrect **login/password** (problem authenticating to the MiVoice 5000 PBX)
- Problem while sending the **.csv** file (problem sending files to the MiVoice 5000 PBX)
- Error when sending the terminal update request: error code logging, but no error interpretation (MMC request problem (error code xx) on the MiVoice 5000 PBX).

4.13.6 DELETING A SOFTWARE RELEASE

This function deletes a software release installed in TMA.

The deletion is only possible if the software release is not configured as the production or test software release.

Proceed as follows:

- Click the Software management menu.
- Select the range.
- Click Change.
- Click the link Delete a software version:
  - select the version to delete then click **Confirm**.

The selected software release is deleted from TMA.

Note : The selected software release is not deleted by TMA from the external download server storage directory. This operation must be performed manually on the external download server.

4.14 PROGRAMMING SYSTEMS KEYS FOR MITEL 6000 SIP PHONES (TEMPLATE MANAGEMENT)

Mitel 6000 SIP Phone keys are divided into two categories: systems keys and programmable keys.

In addition to the configuration of Mitel 6000 SIP Phone keys, possible on AMP **Menu Telephony service>Subscribers>Terminals and applications> 67xxi keys**, TMA completes the possibilities to program the **System** keys (speed-dial for example).

The programming for these **System** keys will be generally applied by terminal model:

- 6920 IP,
- 6930 IP,
- 6940 IP,
- 6970 IP Conference Phone,
- 6905 IP,
- 6910 IP,
- 6863 SIP,
- 6865 SIP
- 6867 SIP,
- 6869 SIP,
- 6873 SIP,
- 6710 SIP,
- 6730 SIP,
- 6731 SIP,
- 6735 SIP,
- 6737 SIP,
- 6739 SIP,
- 6753 SIP,
- 6755 SIP,
- 6757 SIP

Note : This type of programming is not applicable to terminal 6751 SIP (no programmable key on this model).

The programming of these **System** keys must be entered, for each terminal model, in a specific, pre-formatted file called "**TEMPLATE**". These files are available in the **sip_sets_tma** directory of the MiVoice 5000 CD-ROM.

Procedure:

- Create a file from the model provided and save it respecting the syntax **modele.cfg** (example 6755i.cfg).
- From Menu **Deployment** via the parameter **Other File**, successively download all the "**Templates**" files concerned to the download servers.

ATTENTION : The terminal must be restarted so the template file can be taken into account.

4.15 DEPLOYING AND CONFIGURING NEW TERMINALS MITEL 6000 SIP PHONES IN A WORKING INSTALLATION

This procedure describes the step to take in order to deploy and re-configure Mitel 6000 SIP Phones in a working installation.

We consider that TMA has been correctly configured for already deployed and working Mitel 6000 SIP Phones:

- The integrated download server is now configured.
- A production release has been defined.
- All the terminals are in the production release.
- The terminal inventory is up to date.
- The distribution of parameters has been defined for the production release.
- The global and specific configuration files have been defined in TMA for the production release.
- The integrated download server storage directory, used for day-to-day terminal management, contains the production software release as well as the global and specific data configuration files.

4.15.1 AUTOMATICALLY DEPLOYING NEW MITEL 6000 SIP PHONES

To automatically deploy new Mitel 6000 SIP Phones, refer to Section 4.8.3.

4.15.2 CHECKING THE DEPLOYMENT OF MITEL 6000 SIP PHONES

See Section Multi-company for how to check that the deployment of new terminals via manual login has been completed correctly.

4.15.3 DAILY MANAGEMENT OF THESE NEW MITEL 6000 SIP PHONES

See Section 4.11 for the day-to-day management of these new Mitel 6000 SIP Phones.

4.16 DEPLOYING AND AUTOMATICALLY UPDATING MITEL 6000 SIP PHONES WHILE UPGRADING A MIVOICE 5000 SYSTEM

The integrated TMA allows the deployment and automatic update of Mitel 6000 SIP Phones while updating a MiVoice system in a simplified network architecture, using the integrated downloading and DHCP servers.

ATTENTION : This procedure applies only in the following cases:

- **the software release of the Mitel 6000 SIP Phones contained in the terminal software package available in the new MiVoice 5000 system release is ≥ the production software release configured in the integrated TMA,**
- **if the integrated TMA service is enabled.**

ATTENTION : See the document AMT/PTD/PBX/0151* for a detailed description of the upgrade procedures.

4.16.1 PRINCIPLE

The following operations are performed automatically during MiVoice 5000 software upgrade.

- The integrated TMA is automatically configured with the integrated download server.
- The production software release of the integrated TMA is configured with the new terminal software releases contained in the new MiVoice 5000.
- The software releases of the terminals contained in the new MiVoice 5000 release are moved to the work directories of the integrated TMA (the new version of Mitel 6000 SIP Phones is also available in the deployment directory **deployment_67xxi** via symbolic links).
- The global data configuration file of he terminals is generated:
  - From the parameters contained in the global data configuration file in the old MiVoice 5000 release and the new, mandatory global parameters contained in the new MiVoice 5000 release.
- The global data configuration file used to deploy Mitel 6000 SIP Phones is automatically updated with the operation information.
- Some automatic actions are automatically started by the integrated TMA to update the new software releases and global data configuration file of the terminals.
- If some specific files are used for Mitel 6000 SIP Phones (**MAC@.cfg** and/or **locadb.config.MAC@.ftp**), these files are kept after upgrading MiVoice 5000 and located both in the new storage directories used by these terminals and in the work directories of TMA.

4.16.2 UPGRADING MIVOICE 5000

See the document Upgrading by repository AMT/PTD/PBX/0155, Edition 2 minimum).

4.16.3 AUTOMATIC UPDATE OF MITEL 6000 SIP PHONES

After the MiVoice 5000 system is started, some automatic actions are automatically started by the integrated TMA to update the new software releases and global data configuration file of the terminals (respectively the files **localdb.config.ftp** and **aastra.cfg**).

During the first **REGISTER** transmitted by the terminals already assigned to a subscription, a request to update the terminals' software and global data configuration file is sent by the MiVoice 5000 system to these terminals.

The terminals automatically restart to take into account the new terminal software releases defined as production software releases in the integrated TMA.

They will also take into account the new global data configuration file that is automatically updated when upgrading from the parameters contained in the global data configuration file of the old version and the new mandatory global parameters contained in the new version.

4.16.4 AUTOMATICALLY DEPLOYING NEW MITEL 6000 SIP PHONES

To deploy new Mitel 6000 SIP Phones, refer to Section 4.8.3.

4.16.5 CHECKING THE DEPLOYMENT OF MITEL 6000 SIP PHONES

See Section 4.7.11 to check that the automatic update of terminals has taken place correctly, as well as the deployment of the new terminals via manual login.

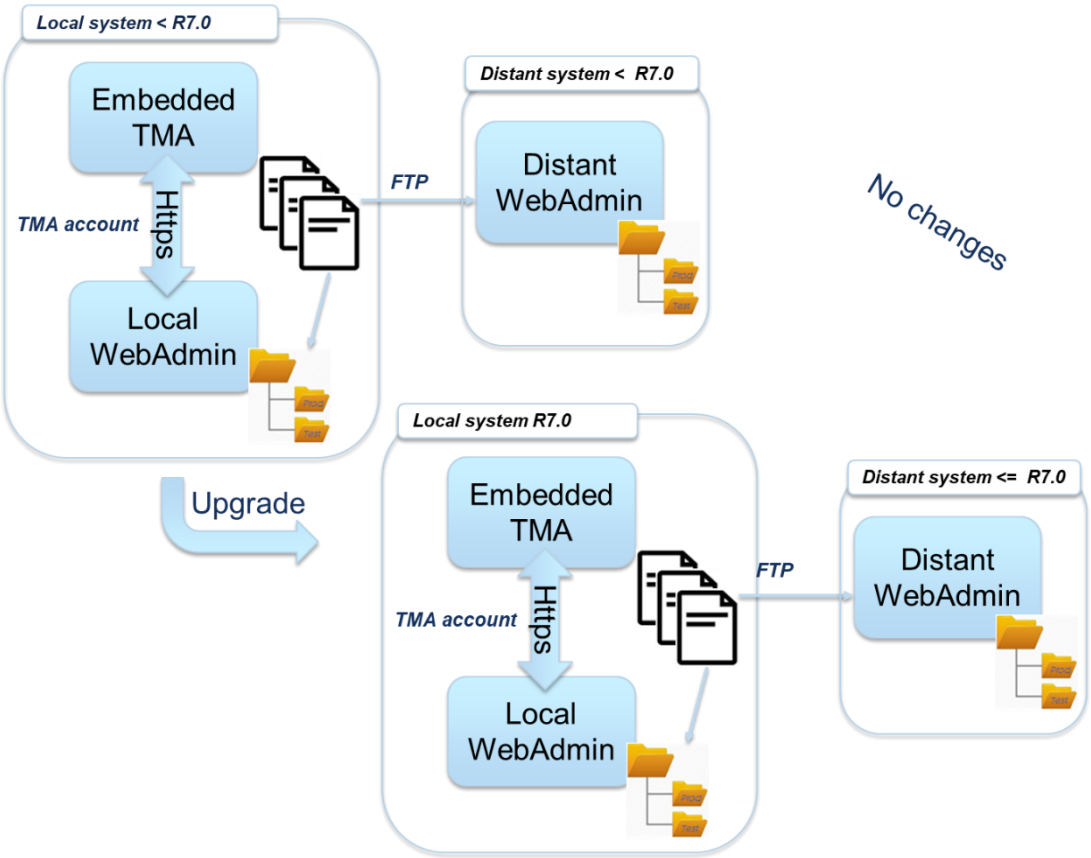
4.17 ADDITIONAL INFORMATION ABOUT THE STATUS OF DOWNLOAD SERVERS FOLLOWING AN UPDATE TO R7.X

Following an update to R7.x, all existing servers are kept with their FTP configuration.

Administration is done by FTP for remote servers and directly on the file system for the integrated server.

All servers previously "not embedded" are considered as "not embedded" download servers.

Example of upgrade:

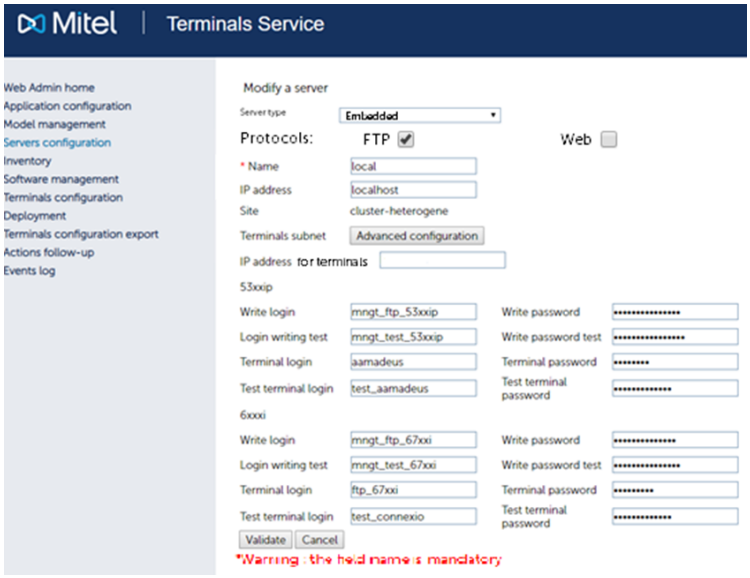


The different cases are:

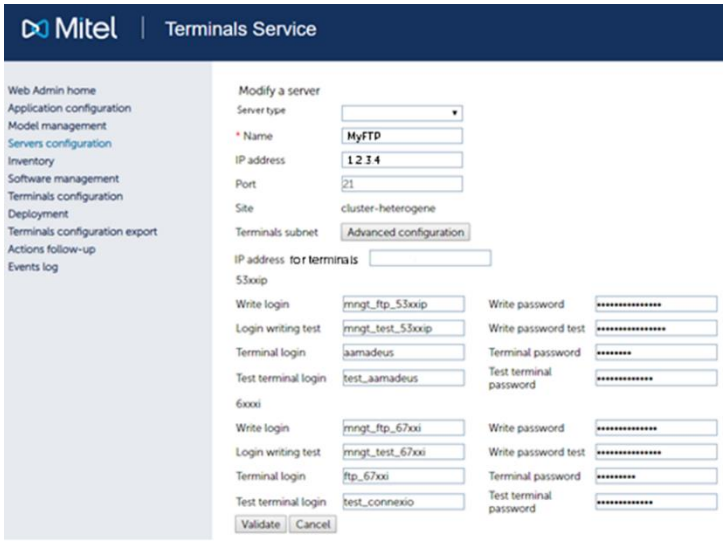
- Embedded server to Embedded with FTP protocol
- Not embedded to Unidentified external server with FTP protocol

Embedded server to Embedded with FTP protocol

Example:



Not embedded to Unidentified external server with FTP protocol



The **Select Type** field is empty, as the system cannot determine whether the remote server is a Mitel 5000 server or a third-party server.

Until the administrator has changed the server type, it is not possible to access new fields or other choices to configure web downloading.

Following the update:

- All new servers created after the upgrade are configured by default to work only with the Web protocol.
- When a new server is created, the administrator can choose to declare an embedded server only if no other embedded server is already defined.
- The administrator can modify this configuration to allow FTP to be used. It must check and perhaps configure FTP access on a remote system.
- If web support is added to an existing server (by ticking the dedicated box) and the server is not local, new settings are displayed to choose between a download server on an MV5000 or a third-party system (Optional).
- This choice (with radio button), dedicated to the Web protocol, defines the parameters to be displayed.
- After configuration and validation, terminals 6xxxi will no longer use FTP to download the software, but the Web when it is activated (HTTP on Mitel 5000 Gateway and HTTPS on others).
- Space management for the terminals will always be done directly on the file system for the embedded server (local), but via HTTPS for the others, which may require additional information (login / password, path, etc.).

5 MANAGING TERMINALS WITH THE TMA HOSTED BY MIVOICE 5000 MANAGER

5.1 PRESENTATION AND PRINCIPLES

TMA can either be embedded into a MiVoice 5000 Server system (accessible from Web Admin), or centralised on a MiVoice 5000 Manager.

This chapter deals specifically with the TMA on the MiVoice 5000 Manager for the deployment and management of Mitel 6000 SIP Phone updates.

Note : For information about management from the TMA integrated into MiVoice 5000 (Mitel 5000 Gateways or Mitel 500 Server), see Chapter 4.

The TMA service must be deactivated on the iPBX when the TMA of MiVoice 5000 Manager is used.

The TMA on MiVoice 5000 Manager is compatible with the download server integrated into Mitel 5000 Gateways and MiVoice 5000 Server, as well as with external download servers.

The TMA on the MiVoice Manager copies the files (software and configuration files) from the TMA directories to the download server directories (External-MiVoice 5000 or Third Party servers).

Note : If the configuration file encryption function is enabled, the encrypted configuration files are physically copied into the integrated download server storage directories.

Note : During each terminal update operation (software, configuration), TMA checks the accessibility of the sites and external download servers concerned by the action. In case of error during this check, the action is not performed.

As of R7.0, access to the directories containing the software releases may be via HTTP/HTTPS protocols and no longer via FTP, thus improving security.

TMA uses the HTTPS protocol to install TMA packages.

ATTENTION : In R7.x, updating files and administering production and test areas is no longer possible with FTP on all MiVoice 5000 systems.

No specific additional licence is required to use TMA. However, the **Subscriber management** licence must be unlocked in MiVoice 5000 Manager to access the TMA start menu.

Note : During each terminal update operation (software, configuration), TMA checks the accessibility of the sites and external download servers concerned by the action. In case of error during this check, the action is not performed.

Case of third-party download servers

On third-party servers, the connection is managed in HTTPS.

Administration is still via FTP and, possibly, via FTPS, to ensure the encryption of all outgoing traffic from the iPBX.

The following table describes the protocols used to download terminals or to manage download spaces (Admin).

The 53xxip terminals are indicated for information purposes but are not subject to any software upgrade as of R7.0.

FTP: simply an FTP access.

WEB: HTTPS or HTTP, because HTTPS is not possible on Mitel 5000 Gateway.

FTP + WEB: The two protocols for accessing the download areas are available, FTP for 53xxip terminals and WEB for 6xxxi.

X: Not supported

TMA Manager/EP		MiVoice 5000 download server			Third party server		
		FTP	*FTP+WEB*	*WEB*	*FTP*	*FTP+WEB*	*WEB*
Admin		FTP	HTTPS	HTTPS	FTP	FTP or FTPS	FTP or FTPS
Download	53xxip	FTP	FTP	X	FTP	FTP	X
	6xxxi	FTP	WEB	WEB	FTP	HTTPS	HTTPS

5.2 LAUNCHING THE TMA

Start TMA from the MiVoice 5000 Manager Client application on a Windows Client PC:

- Click the **Telephony** menu then the **Terminal management** menu.
- For a configuration with several multi-site architectures, a new window opens: select the region, multi-site/isolated site then click **Continue**.
- Enter the login and password assigned by the administrator: the TMA welcome window opens.

The following menus are accessible in the left column:

- **Call Dist**: This menu is used to return to the Web Admin home page.
- **Configuration of the application**
- This menu is used to:
    - Deactivate the management of global and specific data files and to retain only software update actions on the terminals, in the actions managed by TMA
    - Activate configuration file encryption mode
    - Activate the **Remote worker** function: see the document Remote Worker via MBG - AMT/PTD/PBX/0161 for more information about the deployment of this function.
    - Enable certificate verification between the iPBX and the download server.
- **Model management**: This menu allows you to activate or deactivate the management of the model in question.
- **Servers configuration**: This menu is used to define the parameters of the external storage FTP server(s).
- **Inventory**: This menu is used to view the inventory of installation terminals and manage the list of terminals.
- **Software management**: This menu is used to install and manage the terminal software releases and start terminal update actions.
- **Terminals configuration**: This menu is used to distribute the global and specific parameters and to start data update on the terminal.
- **Deployment**: this menu is used to deploy the terminals manually. This menu is also used to make available to the FTP server(s) the template files (**modele.cfg**) and the certificates (**ca.crt**) used by Mitel 6000 SIP Phones.
- **Terminals configuration export**: This menu is used to export in **.csv** format the global and specific data about Mitel 6000 SIP Phones.
- **Actions display**: This menu is used to track the actions started on the terminals (deployment, terminal software, global and specific data).
- **Events log**: This menu displays the events log.
- **iPBX configuration**:

This menu is used to send a request to an iPBX in order to delete the TDW tables containing the data version and index information expected for the terminals. This menu must be used after a TMA /TMA-EP operation. This function is only available for sites as of R5.2 SP1.

This menu is also used to manage the integrated download server, i.e. to delete the content of the file servers on an iPBX (as of R6.3). This function can be useful if you wish to use an integrated download server in TMA in MiVoice 5000 Manager.

5.3 CONFIGURING TMA

5.3.1 ACTIVATING AND DEACTIVATING TMA-EP MODE (EXPERT)

See TMA-EP operating manual (AMT/PTD/TR/0027*)

5.3.2 CONFIGURING THE TERMINALS

Refer to Section 4.3.1.

Note : The management or non-management of terminal configuration files concerns all the multi-site architectures and sites managed by MiVoice 5000 Manager.

5.3.3 ENCRYPTING CONFIGURATION FILES

Refer to Section 4.3.2.

Note : The activation or deactivation of configuration file encryption concerns all the multi-site configurations and sites managed by MiVoice 5000 Manager.

5.3.4 ENABLING AND DISABLING REMOTE WORKER MANAGEMENT

See the document **Remote Worker via MBG - AMT/PTD/PBX/0161** for more information about the deployment of this function.

Note : The remote worker management function concerns all the multi-site architectures and sites managed by MiVoice 5000 Manager.

5.3.5 CHECKING CERTIFICATES

The **Check certificates** checkbox strengthens the security of the HTTPSconnection between TMA and iPBX by checking the certificates on both sides.

TMA uses the certification authority stored in the certification authority base to check the certificates.

Certificates issued to terminals have the same certification authority as the iPBX to which they are attached.

By default, certificates are checked on a system after a first installation and not after an upgrade.

5.3.6 EXCLUDING ONE OR MORE SITES

The **Sites under maintenance** menu is used to exclude one or more sites.

The sites concerned are no longer managed by TMA, with the following restrictions and impacts:

- The terminals of an **excluded** site always appear in the inventory.
- It is not possible to create a site-based list on this site. However, when a list is being created by entering numbers, the terminals of this site can always be added to a list.
- For download server configuration, excluded sites no longer appear on the list of available sites associated with a download server.
- If a download server is associated with **excluded** sites only, during (software or data) update, the update files will not be transferred to it.
- During a software or global data update, the tables of MiVoice 5000 systems concerned are not updated. During an action that requires the use of a list (software update in test mode, specific data update), if the list contains some terminals from **excluded** sites, this action is not authorised: an information message appears.

- The menu used to exclude some sites is not accessible if some actions are programmed.

ATTENTION : If a download server is associated with several sites, it will be updated during an action even if any of the associated sites is considered as "excluded". If any of the these sites is restarted, it will retrieve some data not compatible with the content of the site tables.

- To exclude one or more sites, select the **Application configuration** menu from the TMA main menu.
- Click **Sites under maintenance**.
- In the site exclusion window, tick the site(s) concerned then click **Save** to confirm.
- Close the window.

5.3.7 TESTING THE CONFIGURATION

The **Application configuration** menu allows you to check the accessibility of download sites and servers before launching an action. The list of download servers and sites that will be tested depends on the action configured by the operator.

A new "TestConfig" action is available in the events log and gives the result of the configuration test.

To test the configuration, select the **Application configuration** menu from the TMA main menu.

- Click **Test configuration**.
- In the next window, select:
- The terminal range concerned by the test: **53xxip** or **6xxxi** or **53xx**
- The list concerned: **all** or a list defined by the user
- The action name
- Click **Validate**.

5.4 MODEL MANAGEMENT

Model management makes it possible to draw a list of models taken into account in the software update and provisioning actions (TMA EP):

- sending only managed model files to download servers.
- For software update, only the update is sent to the iPBX for the managed models.

5.5 DOWNLOAD SERVER CONFIGURATIONS

5.5.1 PRINCIPLE

TMA is generally in charge of providing configuration software and files on one or more download servers, especially during deployment.

In a multi-site configuration, TMA is started from MiVoice 5000 Manager and the download servers must be manually defined in the **Server configuration** menu.

The integrated TMA in MiVoice 5000 Manager requires the use of one or more external download servers:

- **For an external dedicated download server**, the integrated TMA in MiVoice 5000 Manager uses some FTP accounts to copy the files (configuration software and files) from the TMA application directories to the external download server directories.
- **For an external download server integrated into MiVoice 5000**, the integrated TMA in MiVoice 5000 Manager uses the MiVoice 5000 Manager account to copy the files (configuration software and files) from the TMA directories to the integrated download server directories.

Note : It should be possible to manage the third-party server in FTP.

Note : During each terminal update operation (software, configuration), TMA checks the accessibility of the sites and external download servers concerned by the action. In case of error during this check, the action is not performed.

All the network parameters required by the terminal to work properly are from the DHCP server and the configuration files downloaded from the download server.

DHCP server configuration according to terminal type is described in Section 7.

On the iPBX side

All the subscribers must be declared on the multi-site sites.

5.5.2 CONFIGURATION WITH SEPARATING TELEPHONY AND ADMINISTRATION FLOWS

If the server to be configured is a local server with Web access (Https, FTP), the address to be entered in the **Server configuration** menu must be the one defined for the **Telephony network>IP address field for the terminals.**

5.6 DEPLOYING MITEL 6000 SIP PHONES

Prerequisites:

- The DHCP and download servers are working.
- Subscriptions exist on each iPBX.

It is possible to log in Mitel 6000 SIP Phones via the MiVoice 5000 User Portal application. A new parameter in the 6xxxi global parameters allows this feature to be opened. The user selects a terminal on which to log in via the MiVoice 5000 User Portal application from his/her system label. This label is unique and is automatically generated by the Mitel 5000 Gateways system. This label can be modified individually or massively.

A global parameter can be configured to disable the free seating feature. In this case (parameter unticked), the impact is as follows:

- On Mitel 6000 SIP Phones, the **Ident** key is no longer displayed and manual login from the terminals is denied for all Mitel 6000 SIP Phones in the installation.

This parameter is accessible via Menu **Telephony service>Subscribers>Terminals and applications>6xxxi parameters**, and is called **Manual login authorisation on any type of terminal**. By default, this parameter is enabled (ticked). This parameter is accessible if the login function via the MiVoice 5000 User Portal application is open.

A mechanism for deploying Mitel 6000 SIP Phones through automatic login is configurable by automatically assigning a directory number to each terminal identified by its unique label. Automatic login is performed at the next REGISTER of the terminal. This mechanism concerns all subscriptions (secure or not).

It is possible to secure the login mechanism during the deployment phase of Mitel 6000 SIP Phones. A new parameter at the subscription level allows you to carry out this configuration:

- In unsecured mode, the parameter **Login via PC only** is not ticked (default value): the user can perform a manual login via the Ident key or via the corresponding facility code (*44 by default).
- In secure mode, the parameter **Login via PC only** is ticked: the user cannot perform a manual login via the Ident key or via the corresponding feature code (*44 by default).

Access to the MiVoice 5000 User Portal can be further secured by configuring and using SSO mode (refer to document AMT/PTD/PBX/0080* for SSO mode configuration).

Mitel 6000 SIP Phones can be deployed using the following methods:

- Deployment through manual login on the terminal
- Deployment via the MiVoice 5000 User Portal from a single label identifying the terminal.
- Automatic deployment by assigning a subscription number to the terminal
- Deployment from a dedicated Excel file.

5.6.1 DEPLOYING MITEL 6000 SIP PHONES THROUGH MANUAL LOGIN:

Refer to Section 4.8.1 for the principle and procedure to follow to deploy Mitel 6000 SIP Phones through manual login.

The external DHCP Server will provide Mitel 6000 SIP Phone with the IP address of the external download server and allow the terminal to connect to download its production software release and global deployment data configuration file.

When the terminal is registered for the first time (first REGISTER), so*me* logout/login operations are performed on the terminal, or when the terminal software release is updated, some SNMP traps are sent by the iPBX to MiVoice 5000 Manager, and the TMA inventory is updated.

For the daily management of these terminals with the TMA application, see Section 4.11.

Note : This deployment method does not need the use of the TMA deployment function.

5.6.2 DEPLOYMENT VIA THE MIVOICE 5000 USER PORTAL OF MITEL 6000 SIP PHONES

Refer to Section 4.8.2 for the principle and procedure to follow to deploy Mitel 6000 SIP Phones via MiVoice 5000 User Portal.

The external DHCP Server will provide Mitel 6000 SIP Phone with the IP address of the external download server and allow the terminal to connect to download its production software release and global deployment data configuration file.

When the terminal is registered for the first time (first REGISTER), so*me* logout/login operations are performed on the terminal, or when the terminal software release is updated, some SNMP traps are sent by the iPBX to MiVoice 5000 Manager, and the TMA inventory is updated.

For the daily management of these terminals with the TMA application, see Section 4.11.

Note : This deployment method does not need the use of the TMA deployment function.

5.6.3 AUTOMATICALLY DEPLOYING MITEL 6000 SIP PHONES

Refer to Section 4.8.3 for the principle and procedure to follow to automatically deploy Mitel 6000 SIP Phones.

The external DHCP server will provide Mitel 6000 SIP Phone with the IP address of the external download server and the account (connexio/connexio) to which the Mitel 6000 SIP Phone will connect to download its production software release and global deployment data configuration file.

When the terminal is registered for the first time (first REGISTER), so*me* logout/login operations are performed on the terminal, or when the terminal software release is updated, some SNMP traps are sent by the PBX to MiVoice 5000 Manager, and the TMA inventory is updated.

For the daily management of these terminals with the TMA application, see Section 4.11.

Note : This deployment method does not need the use of the TMA deployment function.

5.6.4 DEPLOYMENT VIA EXCEL FORM OF MITEL 6000 SIP PHONES

For the deployment phase itself, it is similar to the one described in Section 4.8.4.

5.6.4.1 *Inventory of the configuration*

TMA gives the configuration inventory of Mitel 6000 SIP Phones, after first deployment.

Note : The inventory lists all the terminals on the installation.

When the terminal is first registered, an SNMP trap is sent by the PBX to MiVoice 5000 Manager. This trap contains the data stored in MiVoice 5000 Manager and which is used by TMA to update the information displayed in the inventory concerning Mitel 6000 SIP Phones.

The main data contained in the trap for a Mitel 6000 SIP Phone includes:

- The terminal directory number
- The label associated with the terminal
- The possibility or not of periodically logging out the terminal
- The reference site
- The terminal range and model
- The terminal software release
- The terminal IP address
- The terminal MAC address
- The extension number (for a multi-line terminal)
- The index associated with the terminal's global data file
- The index associated with the terminal's specific data file

The other fields do not concern this environment.

To display the inventory of Mitel 6000 SIP Phone configuration in TMA, proceed as follows:

- Click the **Inventory** menu.
- Select the **6xxxi** range and possibly the **model**.
- By default, the index associated with the terminal's global data file is "**1**".
- Information display depends on the filter used. This filter is activated by clicking the **Magnifying glass** icon.
- If possible, apply a filter to the current inventory based on:
    - The subscription’s community
    - The subscription’s reference site
    - The terminal subscription number
    - The terminal IP address
    - The terminal software release (production, test release, etc.)
    - The terminal global data index
    - The terminal specific data index
    - The terminal MAC address

Terminal encryption configuration:

- SRTP (and TLS) mode activated
- TLS mode activated
- No encryption activated.

Note : The joker * may be applied to the parameters Number, IP address and Mac address by placing it at the end of the parameter value.

- Click**Filter** to apply the filter to the current inventory.

The logged column is used to indicate whether the Mitel 6000 SIP Phone is registered on its reference site (green tick) or whether the terminal is not registered on its reference site (red cross).

Note : If the terminal is not registered on its reference site, a tooltip indicates the possible reason why the registration failed or whether the terminal is a general-purpose one.

The **Encryption** column indicates the encryption status of Mitel 6000 SIP Phones:

- Encrypted terminal in SRTP (and TLS):
- Encrypted terminal in TLS
- Terminal not encrypted: Empty
- Information not available: (configuration file not present or encryption parameters not found)

5.6.5 DEFINING THE PRODUCTION TERMINAL SOFTWARE PACKAGE

This procedure is used to define the production terminal software package.

- Click the **Software management** menu.
- Select the **6xxxi** range.
- Click **Change**.
- Click the link **Configure production software release**:
- Select the previously installed terminal software package then click **Validate**.

5.6.6 DISTRIBUTING THE PARAMETERS OF PRODUCTION TERMINAL SOFTWARE PACKAGE

For a given software release, this procedure is used to assign the parameters for each terminal range. The range of each parameter is given.

Note : This distribution is only necessary if you wish to update the terminal data.

A parameter is defined either:

- In the Mitel 6000 SIP Phones' global data configuration file (Range = Global)
- In the specific data configuration file of Mitel 6000 SIP Phones (Range = Specific)
- In the DHCP server (Scope = DHCP)
- Or in none of the previous scopes; so this parameter is not managed (Scope = Ignored).
- This distribution must be made for each software release installed.
- Click the **Terminal configuration** menu.
- Select the **6xxxi** range.
- In the field **Version to configure**, select the terminal software package concerned by the distribution.

A distribution of the parameters in form of tabs is only displayed for Mitel 6000 SIP Phones:

- **Encryption**: encryption parameters for Mitel 6000 SIP Phones
- **Config**: the usual configuration parameters
- **TimeZone**: date and time, NTP server, time zone configuration parameters
- **Network**: network parameters (DHCP, VLAN, LLDP,...)
- **RFC2833**: RFC2833 / SIP INFO configuration parameters
- **802.1X**: 802.1X configuration parameters
- **RTCP**: RTCP configuration parameters
- **Directory:** configuration parameters for access to the LDAP directory and Exchange contacts (function available as of R6.2)
- **Expert**: all the other parameters not available in the previous tabs

Note : To facilitate the introduction of certain features (encryption, etc.), some parameters are available twice in the tab:

- **in the upper part, the parameters have a range and some fixed values.**
- **in the lower part, the same parameters have a default value which may differ and a range set to ignored.**

- Select a tab and define the range of each parameter present in this tab, like in the Excel form during data collection.

Note : Pop-ups are used to obtain the definition of each parameter. They appear when the cursor is placed over the name of the parameter.

- Click **Save**:
- Clicking Distribute displays a confirmation message before the distribution of parameters is locked for this software release.

Note : It is possible to unlock the distribution if necessary. In this case, it is mandatory after the new parameter allocation to start some global and specific data update actions so as to take into account the parameter values whose assignment has changed.

- The **Initialise** button restores the factory distribution of the parameters associated with this software release.

Note : The parameters managed by DHCP, or ignored, are displayed for information purposes only.

After the distribution operation, it is possible to perform, if necessary, an update of the global and specific data of Mitel 6000 SIP Phones. Refer to Sections Global data update and Specific data update for more information about the procedure to follow.

5.7 MANUAL UPDATE OF MITEL 6000 SIP PHONES

This chapter describes how to manually update Mitel 6000 SIP Phones.

Once a Mitel 6000 SIP Phone is known in the TMA inventory, this terminal is managed by TMA, and it can be updated on a daily basis.

Note : Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.

Note : Mitel 6000 SIP Phone software and global data can be updated without any Mitel 6000 SIP Phone being physically connected to the network.

5.7.1 PRINCIPLE

The principle of manually updating Mitel 6000 SIP Phones from the TMA embedded in MiVoice 5000 Manager is the same as that described in the TMA embedded in Mitel 5000 Gateways & MiVoice 5000 Server systems (see Section 4.11).

Note : When the terminal is registered for the first time (first REGISTER), some logout/login operations are performed on the terminal, or when the terminal software release is updated, some SNMP traps are sent by the PBX to MiVoice 5000 Manager, and the inventory of the TMA integrated into MiVoice 5000 Manager is updated.

5.7.2 GLOBAL DATA UPDATE

This procedure allows the global data of all Mitel 6000 SIP Phones to be updated.

Note : Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.

The global data of Mitel 6000 SIP Phones is updated from the TMA integrated into MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Section 4.11.2).

5.7.3 SPECIFIC DATA UPDATE

This procedure applies once a terminal appears in the TMA application inventory. This procedure updates the common specific data of a list of Mitel 6000 SIP Phones.

Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.

The specific data of Mitel 6000 SIP Phones is updated from the TMA integrated into MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Section 4.11.3).

5.7.4 UPDATING THE SOFTWARE RELEASE OF MITEL 6000 SIP PHONES

This procedure allows the software release of all Mitel 6000 SIP Phones to be updated.

Logged and unlogged terminals are visible in the TMA inventory and are managed by TMA.

The software release of Mitel 6000 SIP Phones is updated from the TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Section 4.11.4).

The only difference is:

1 - For the list of components to download in the Software management menu:

Once the version has been selected, when the list of package components is presented, it is given for information purposes (grey boxes).

No changes are possible because all components are available for downloading.

5.7.5 DISTRIBUTING THE PARAMETERS OF THE NEW PRODUCTION RELEASE

This procedure is used to distribute the parameters associated with a new software release installed in TMA. The range of each parameter is given.

A parameter is defined either:

- In the Mitel 6000 SIP Phones' global data configuration file
- In the specific data configuration file of Mitel 6000 SIP Phones
- In the DHCP server
- Or in none of the previous ranges, so this parameter is not managed.

The parameters of the new production release of Mitel 6000 SIP Phones are distributed from the TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Section 4.11.5).

5.7.6 MANAGING THE LIST OF TERMINALS FOR MITEL 6000 SIP PHONES

This procedure is used to define a list of terminals for all Mitel 6000 SIP Phone models.

This list is used either:

- In nominal mode, to update some specific data on a global or restricted range, or
- In test mode, to update the terminals' software release, global data and specific data on a limited range.

ATTENTION : A terminal may be assigned only to one list at a time.

The list used in test mode to update the terminal software release must be the same as the one used to update the global data and specific data.

5.7.6.1 *Defining a new list by entering the terminals one by one*

A new list is defined from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Section 4.11.6).

5.7.6.2 *Defining a new list from a site*

- Click the **Inventory** menu.
- Select the **6xxxi** range and possibly the **model**.
- Click **List management:**
    - The Terminal range concerned: 6xxxi.
    - The Terminal model concerned.
- Click Create a list from a site.

A new window opens. This allows you to define a list of terminals from the terminals known to the inventory for this site and for the series of terminals concerned.

- Select any of the sites presented in the window by clicking it.
- In the right area, enter the **List name** then click **Validate**.
    - This message appears: the list has been successfully saved.
- Close the window either by clicking the **Close window** link, or by clicking on the top right side of the window.
- The list management window is refreshed and then displays:

- The list name
- The number of terminals contained on the list
- The **Action** field used to delete or modify the displayed list.

- Click **Return** to return to the **Inventory** window.

5.7.6.3 *Modifying a list*

A list is modified from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Section 4.11.6.2).

5.7.6.4 *Deleting a list*

A list is deleted from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Section 4.11.6.3).

5.8 TEST MODE FOR MITEL 6000 SIP PHONES

Test mode is used to update the terminals' software release, global data and specific data. This function is used to test a new terminal software application or new function/configuration on a small number of terminals before exposing it to all the terminals.

The list of terminals used in test mode to update the terminal software release must be the same as the one used to update the global data and specific data of the tested terminals.

The different files (terminal software, global or specific data) are stored in the **test directory** defined in the external download server configuration.

5.8.1 UPDATING THE SOFTWARE RELEASE OF MITEL 6000 SIP PHONES IN TEST MODE

This procedure applies once a terminal is registered to its reference site through any of the deployment methods described in the previous sections. This procedure is used to update the software release of the Mitel 6000 SIP Phones known to the inventory and defined on a list containing at most 10 terminals.

The software release of Mitel 6000 SIP Phones en mode est is updated from the integrated TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Section 4.12.1).

5.8.2 DISTRIBUTING THE NEW TEST SOFTWARE RELEASE PARAMETERS

The parameters of the new test release of Mitel 6000 SIP Phones are distributed from the TMA in MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Section 4.12.2).

Note : In the field Version to configure, select the test release concerned by the distribution.

5.8.3 UPDATING THE GLOBAL DATA OF TERMINALS IN THE TEST SOFTWARE RELEASE

This procedure is used to update the global data of Mitel 6000 SIP Phones in the test software release.

The global data of Mitel 6000 SIP Phones in test software release is updated from the TMA integrated into MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Section 4.12.3).

Note : In the field Version to configure, select the test release concerned by the distribution.

5.8.4 UPDATING THE SPECIFIC DATA OF TERMINALS IN THE TEST SOFTWARE RELEASE

This procedure is used to update the specific data of Mitel 6000 SIP Phones in the test software release.

5.8.4.1 *Updating the common specific data of terminals in the test software release*

This procedure is used to update the specific data of terminals in the test software release.

The common specific data of Mitel 6000 SIP Phones in test software release is updated from the TMA integrated into MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Section 4.12.4.1).

Note : In the field Version to configure select the test release.

5.8.4.2 *Updating the individual specific data of terminals in the test software release*

This procedure is used to update the special specific data of terminals in the test software release.

The individual specific data of Mitel 6000 SIP Phones in test software release is updated from the TMA integrated into MiVoice 5000 Manager in the same way as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Section 4.12.4.2).

Note : In the field Version to configure select the test release.

5.8.5 EXITING THE TEST MODE

This procedure is used to leave the test mode at the end of the test phase.

Two possibilities are available:

- The tested new release is satisfactory: in this case, all the terminals on the installation must be updated with the new test software.
- The tested new release is not satisfactory: in this case, only the tested terminals must be updated with the current production software release.

5.8.5.1 *Switching from test mode to production mode*

In this case, the test software release must be defined as the new production software release, and an update operation for this new production software release started on all the terminals.

The procedure for changing from test mode to production mode from the integrated TMA in MiVoice 5000 Manager is the same as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Section 4.12.6.1).

5.8.5.2 *Returning to the current version*

In this case, the test software release is not satisfactory. The terminals on the test list must be downgraded with the current production release. An update for this production software release must be started on all the terminals.

The procedure for restoring the current release from the integrated TMA in MiVoice 5000 Manager is the same as described in the TMA integrated into Mitel 5000 Gateways & MiVoice 5000 Server (see Section 4.12.6.2).

5.9 ADDITIONAL TMA FUNCTIONS

5.9.1 DOWNLOADING FILES INDIVIDUALLY

This feature allows you to download a single file to the file server(s). This feature allows you to make available on the FTP server(s) the template files (**model.cfg**) used by Mitel 6000 SIP Phones and certificates (**ca.crt**) when encryption is enabled and an external certificate is used.

To download a file individually, proceed as follows:

- Click the **Deployment** menu.
- Select the (**6xxxi**) range.
- From the **List of download servers**, select the server to which the template file or certificate must be downloaded.
- In the **Other file** field import, by clicking **Browse**, the template file (Mitel 6000 SIP Phone.cfg) or certificate (ca.crt) to be downloaded.
- Click **Validate**.
- Enter the **Action name**.
- Select **the type of update** (immediate or deferred).
- Click **Validate**.
- In **Action monitoring** check that the file is correctly downloaded individually to the download server.

ATTENTION : A download server must be selected. Only one file is allowed per deployment operation.

ATTENTION : Some file name checks are made:
This file cannot be a global data file; therefore, the name must be different from aastra.cfg (if the 6xxxi range is selected).
If configuration file encryption is activated, the *.cfg files downloaded individually are encrypted before being sent to the download server because they will not be taken into account.

These files are backed up in the local TMA directory, in the tree structure of the multi-site configuration selected while starting the TMA application, and proposed again for downloading via the combo box **Files previously downloaded** in the **Deployment** menu.

After selecting a file previously downloaded individually, the following actions may be taken on these backed up files:

- Viewing (via the **View** button): a new window opens, displaying the content of the file,
- Deletion (via the **Delete** button): after confirmation, the file is locally deleted; it will still be available on the download servers on which it may have been deployed.

5.9.2 EXPORTING THE DATA CONTAINED IN THE CONFIGURATION FILES OF MITEL 6000 SIP PHONES

The global and specific data of terminals with a production or test software release may be exported in **.csv** format from the **Terminals configuration export** menu.

Refer to Section 4.13.2 for more information about the procedure.

- Select the **range** and possibly the **model**.

The **Specific site data** button is used to export in **.csv** format only the specific data of terminals in site-based production software release. This export is saved in the file **export_specific_site**. This function is used to export the specific data meant to be used by TMA-EP.

5.9.3 EXPORTING THE DATA CONTAINED IN THE INVENTORIES OF MITEL 6000 SIP PHONES

The terminal data displayed in the inventory can be exported to a **.csv** file.

Refer to Section 4.13.3 for more information about the procedure.

- Select the **range** and possibly the **model**.
- If possible, apply a filter to the current inventory based on:
    - The subscription's community
    - The subscription's reference site
    - The terminal subscription number
    - The terminal IP address
    - The terminal software release (production, test release, etc.)
    - The terminal global data index
    - The terminal specific data index
    - The terminal MAC address

Note : The joker * may be applied to the parameters Number, IP address and Mac address by placing it at the end of the parameter value.

Note : The export function is also available from Action monitoring.

5.9.4 PRINTING THE DATA CONTAINED IN THE INVENTORIES OF MITEL 6000 SIP PHONES

The terminal data displayed in the inventory can be printed out.

Refer to Section 4.13.4 for more information about the procedure.

- Select the **range** and possibly the **model**.

Note : The print function is also available from Action monitoring.

5.9.5 EVENT LOG

The event log is basically used to check the status of the following actions:

- Deployment
- Terminal software release update
- Terminal global data update
- Terminal specific data update
- Each action is identified by the following information:
- The **Date** on which the action was started
- The **Time** the action was started
- The **Multisite** concerned by the action
- The name of the **User** who started the action
- The type of**Action** concerned
- The **Name of the action** concerned
- The **Status** of the action concerned
- The information displayed may be filtered with certain criteria:
- Click the **Event log** menu.
- Select any of the following:
    - User
    - Action
    - Status
    - Start date and End date

Note : Clicking the  icon opens the calendar so the start and end dates can be selected directly.

- Click **Filter** for the filtering criteria to become effective.

Note : Clicking Initialise deletes the filter criteria and displays the entire information.

In case of operation error, the events log is used to identify the cause of the error: The following cases are taken into account:

- Network problem: no response to PING (problem accessing the MiVoice 5000 PBX)
- APACHE problem: HTTPS request timed out (problem accessing the MiVoice 5000 PBX web server)
- "MMC" service is stopped (problem accessing the MiVoice 5000 PBX MMC)
- Incorrect "login/password" (problem authenticating to the MiVoice 5000 PBX)
- Problem while sending the ".csv" file (problem sending files to the MiVoice 5000 PBX)
- Error when sending the terminal update request: error code logging, but no error interpretation (MMC request problem (error code xx) on the MiVoice 5000 PBX).

5.9.6 DELETING A SOFTWARE RELEASE

This function deletes a software release installed in TMA.

The deletion is only possible if the software release is not configured as the deployment or test software release.

Proceed as follows:

- Click the **Software management** menu.
- Select the **Range**.
- Click **Change**.
- Click the link **Delete a software version**:
    - select the version to delete then click **Confirm**.

The selected software release is deleted from TMA.

Note : The selected software release is not deleted by TMA from the external download server storage directory. This operation must be performed manually on the external download server.

5.9.7 IPBX CONFIGURATION

5.9.7.1 *Managing tables*

This procedure is used to erase the data concerning the operations previously performed by TMA, saved in the tables of all the multi-site systems (as of R5.2 SP1). These tables contain, among others, information about the terminal release and index of the global configuration file in nominal mode and test mode, as well as information about **download** servers.

This procedure must be used in the following cases:

- While changing to TMA-EP mode (See the TMA-EP operating manual (AMT/PTD/TR/0027*)
- While returning to TMA mode (See the TMA-EP operating manual (AMT/PTD/TR/0027*)
- While stopping the terminal service (TMA).
- The procedure to use is as follows:
- In the TMA-EP application, select the **iPBX configuration** menu.
- Select the **Site** on which the TDW tables must be reset.
- In the **Table management** part:
    - Tick the terminal range(s) on which to perform the reset.
    - Click **Reset tables** then confirm the iPBX table configuration reset when the warning message is displayed.
- Check in the events log that this operation is taken into account.

5.9.7.2 *Managing the integrated download server*

This procedure is used to implement the previously described table management procedure on all ranges, but also to delete the content of the integrated FTP areas on a MiVoice 5000 system.

This procedure must be used if you wish to define in the integrated TMA on a MiVoice 5000 Manager an integrated download server on a MiVoice 5000 system, and if, depending on the prior configuration of this system, some links may exist in this latter's FTP areas.

This procedure only applies to systems as of R6.3.

- Select the **iPBX configuration** menu.
- Select the **Site**.
- In the **Server management** part
    - if the selected site is a cluster site, select **Node** (seen in the cluster server as node).
    - Otherwise, the list of nodes is empty.
- Click "**Clean integrated FTP server area**" to confirm the table reset and the deletion of the content of the FTP area.
- Check in the events log that this action has been taken into account.

5.10 PROGRAMMING SYSTEMS KEYS FOR MITEL 6000 SIP PHONES (TEMPLATE MANAGEMENT)

Mitel 6000 SIP Phone keys are divided into two categories: systems keys and programmable keys.

In addition to the configuration of Mitel 6000 SIP Phone keys, possible on AMP **Menu Telephony service>Subscribers>Terminals and applications> 67xxi keys**, TMA completes the possibilities to program the **System** keys (speed-dial for example).

The programming for these **System** keys will be generally applied by terminal model:

- 6920 IP,
- 6930 IP,
- 6940 IP,
- 6970 IP Conference Phone,
- 6905 IP,
- 6910 IP,
- 6865 SIP
- 6867 SIP,
- 6869 SIP,
- 6873 SIP,
- 6710 SIP,
- 6730 SIP,
- 6731 SIP,
- 6735 SIP,
- 6737 SIP,
- 6739 SIP,
- 6753 SIP,
- 6755 SIP,
- 6757 SIP

Note : This type of programming is not applicable to terminal 6751 SIP (no programmable key on this model).

The programming of these **System** keys must be entered, for each terminal model, in a specific, pre-formatted file called "**TEMPLATE**". These files are available in the **sip_sets_tma** directory of the MiVoice 5000 CD-ROM.

Procedure:

- Create a file from the model provided and save it respecting the syntax **modele.cfg** (example 6755i.cfg).
- From Menu **Deployment** via the parameter **Other File**, successively download all the "**Templates**" files concerned to the download servers.

ATTENTION : The terminal must be restarted so the template file can be taken into account.

5.11 TROUBLESHOOTING SOLUTIONS

5.11.1 INVENTORY IS NOT UPDATED AUTOMATICALLY

If the information contained in the TMA inventory is not updated automatically, the data on the site concerned must be imported from MiVoice 5000 Manager in the following cases:

- If only the data of a MiVoice 5000 Server or Mitel 5000 Gateways system is restored
- If the data and code of a MiVoice 5000 Server or Mitel 5000 Gateways system are restored.
- In case of switchover to the inactive partition of a MiVoice 5000 Server or Mitel 5000 Gateways system.

This import guarantees the consistency of the information about the traps stored both in MiVoice 5000 Server or Mitel 5000 Gateways systems and in the MiVoice 5000 Manager database.

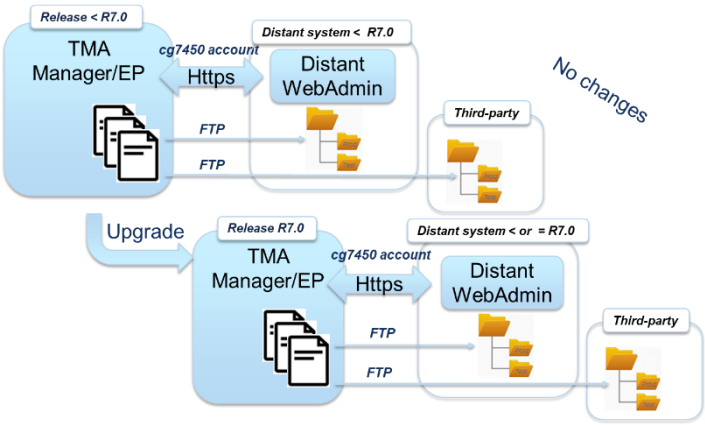
To import data from the site concerned in MiVoice 5000 Manager, proceed as follows:

- From the MiVoice 5000 Manager client terminal on a Windows Client PC:
    - Click the Administration menu then the Network topology menu.
    - Select the multi-site concerned then click the Configuration menu.
    - In the area Import a new site in the multisite, select the site concerned then click Import.
    - Do not tick Import site local directory data.
    - Click Start.

5.12 ADDITIONAL INFORMATION ABOUT THE STATUS OF DOWNLOAD SERVERS FOLLOWING AN UPDATE TO R7.X

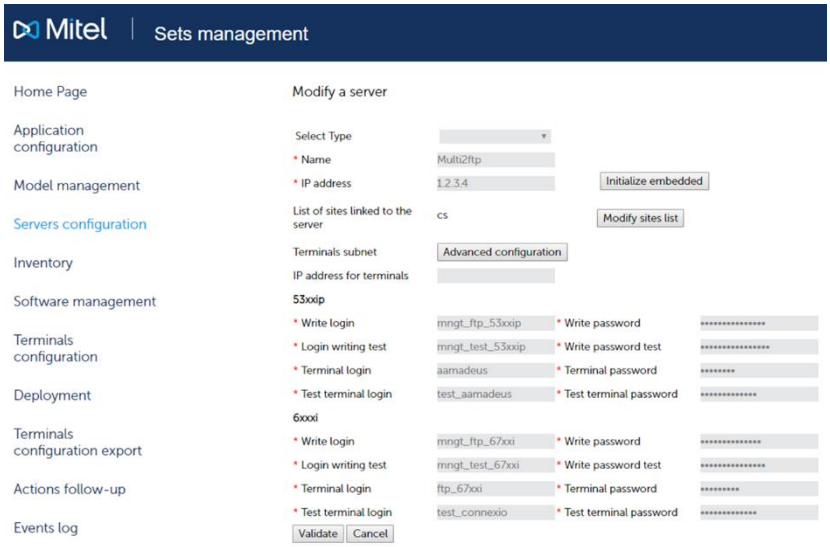
Following an update to R7.x on TMA (or TMA-EP), all existing servers are kept with their FTP configuration.

The administration is carried out by FTP.



After the update:

- All new servers created after the upgrade are configured by default to work only with the Web protocol.
- The administrator can modify this configuration to allow FTP to be used.



The **Select Type** field is empty, as the system cannot determine whether the remote server is a Mitel 5000 server or a third-party server.

Until the administrator has changed the server type, it is not possible to access new fields or other choices to configure web downloading.

6 CONFIGURING THE DHCP SERVICE INTEGRATED INTO MIVOICE 5000 SYSTEMS

6.1 INTRODUCTION

The server embedded in the Mitel 5000 Gateways and MiVoice 5000 Server systems allows the management of the following Mitel terminals, according to the protocol, IPV4 or IPV6:

In IPV4, the following terminals are managed:

- Mitel 6000 SIP Phones
- MiVoice 5300 IP Phones
- Mitel DECT/SIP/IP base stations
- WIFI terminals 312i
- Terminals I7xx
- Blustar 8000i

In IPV6, the following terminals are managed:

- 6863i SIP Phones
- 6865i SIP Phones
- 6867i SIP Phones
- 6869i SIP Phones
- 6873i SIP Phones
- 6920 IP Phones
- 6930 IP Phones
- 6940 IP Phones
- 6905 IP Phones
- 6910 IP Phones
- 6970 IP Conference Phone
- 6900 (Minet), UC360, 5304 Model
- Mitel DECT/SIP/IP base stations
- Models TA7102i/7104i

Combination of IPV4/IPV6

- The DHCP server and the DHCP Client, support IPv4 and IPv6. However, the client and server can only manage one protocol at a time.
- For dual support, they must be started separately for IPv4 and IPv6.
- The start is to be carried out from Menu **Telephony service>System>Configuration>Services**.

The embedded DHCP server responds to requests from equipment without a Vendor Class (servers, PCs, etc.) and to requests from equipment with specific Vendor Classes different from those already taken into account by the embedded DHCP Server (see list above).

In the latter case, template files describing the Vendor Class parameters associated with these devices can be imported into the Embedded DHCP Server.

The DHCP server can deliver IP addresses for one or more subnets.

The DHCP server can supply data to Mitel terminals connected to different systems (multi-site configuration) within the limit of the planned capacity.

The DHCP server embedded in MiVoice 5000 Server systems is limited to configurations with a maximum of 500 IP terminals and 4 subnets.

In the case of a redundant MiVoice 5000 Server configuration, the DHCP server embedded in MiVoice 5000 Server systems is available. In this case, the virtual IP address is configured in the embedded DHCP server.

6.2 DHCP SERVICE HOME PAGE (V4 AND V6)

From the web browser, connect to the system's MiVoice 5000 Web Admin.

Click the **DHCP Service** menu.

The DHCP Service configuration menu appears.

The following menus are accessible in the left column:

- **Web Admin home page**: For returning to the Web Admin home page.
- **DHCP - Creation**: For defining a new DHCP configuration.
- **Operation DHCP**: For modifying the current DHCP configuration
- **Templates management**: For managing a new device by importing a template file in XML format.
- **Restore - Delete**: For restoring or deleting an archive*
- **Restart DHCP service**: For restarting the DHCP service**.
- **DHCP service status**: Displays the current status of the DHCP service.
- **Display of DHCP configuration**: Displays the dhcpd.conf file (current or operational) in HTML format
- **Visualization of DHCP leases**: Displays the file dhcpd.leases in HTML format.

* Restoring an archive allows you to work on a new configuration but the working configuration remains valid.

** The current configuration becomes operational.

6.3 EMBEDDED IP V4 SERVICE

6.3.1 CREATING A NEW DHCP V4 CONFIGURATION

- From Menu **DHCP - Creation**

A confirmation message appears:

- Click the **Validate** button to confirm the overwriting of the current configuration data and the creation of a new, current configuration.

The general parameters configuration window opens.

- Store the current configuration before overwriting it.

6.3.2 CONFIGURING THE GENERAL PARAMETERS

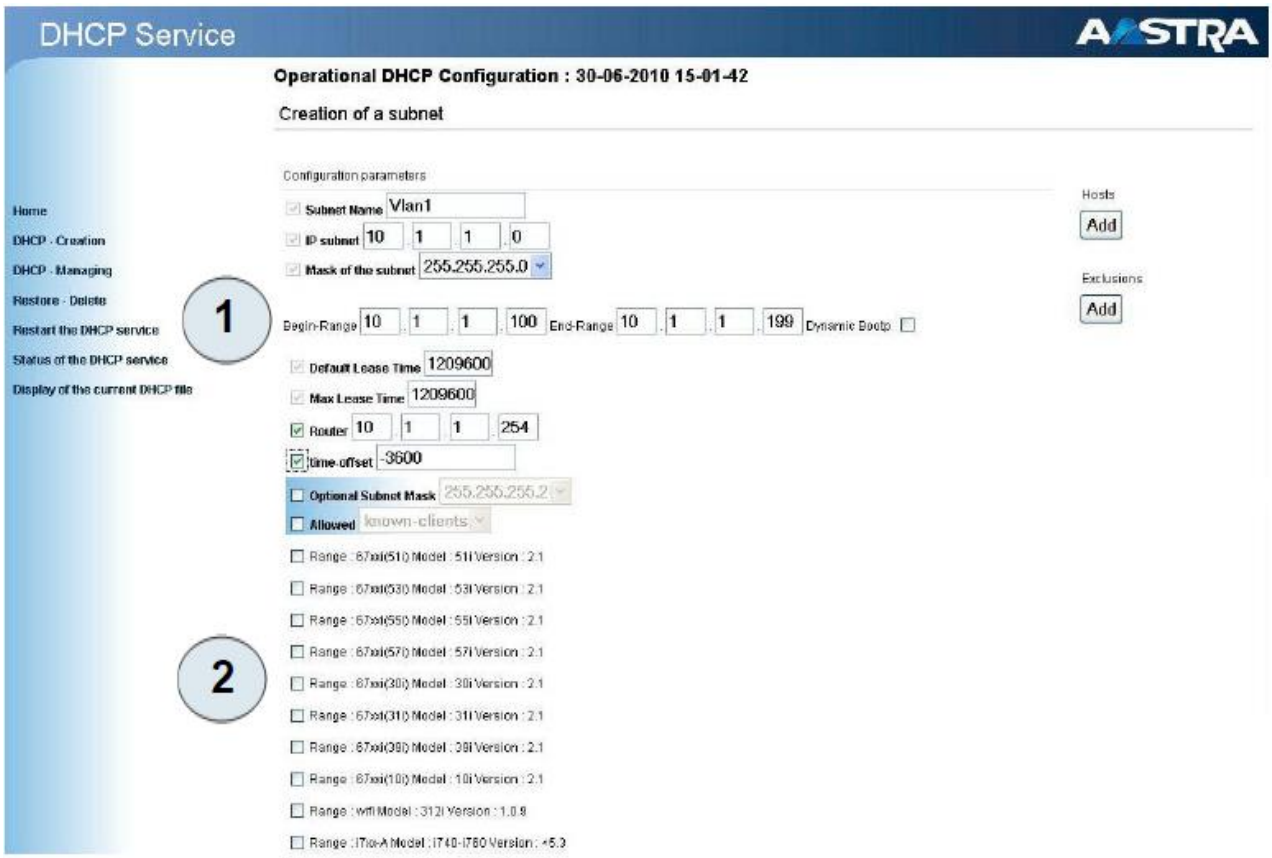
Leave the default values of the DHCP general parameters:

- **Type of DDNS update***: none
- The network exercises authority*: yes (ticked)
- **Ignore***: not ticked (by default, all the requests are accepted).
- **Local address**: for a redundant configuration, this parameter is used to indicate the virtual IP address on which the embedded DHCP server will send its DHCP messages.
- **Server identification**: For a redundant configuration, this parameter allows you to specify the virtual IP address used to identify the DHCP server.

Note : * The meaning of these parameters is indicated in Appendix 2.

- Select the Mitel terminal(s) to be configured in the DHCP server by ticking the appropriate box.
- Click **Add** (in the **Subnet** column on the top right side) to create a subnet.

The following configuration window opens:



The upper part (**1**) defines the standard network parameters associated with the subnet in question.

The lower part (**2**) defines the specific network parameters of each type of terminal associated with the subnet in question. The terminal types concerned are:

- Mitel 6000 SIP Phone Models 6730 SIP, 6731 SIP, 6751 SIP, 6753 SIP, 6755 SIP and 6757 SIP (version 2.1 and later)
- Mitel 6000 SIP Phone Model 6739i (version 3.0 and later)
- Mitel 6000 SIP Phone Models 6735 SIP and 6737i (version 3.2 and later)
- Mitel 6000 SIP Phone Models 6863 SIP, 6865 SIP, 6867 SIP and 6869 SIP (version 3.3 and later)
- Mitel 6000 SIP Phone Model 6873 SIP (version 4.2 and later)
- Mitel 6000 SIP Phone Model 6920 IP (version 5.0 and later)
- Mitel 6000 SIP Phone Model 6930 IP (version 5.0 and later)
- Mitel 6000 SIP Phone Model 6940 IP (version 5.0 and later)
- Mitel 6000 SIP Phone Model 6905 IP (version 5.0 and later)
- Mitel 6000 SIP Phone Model 6910 IP (version 5.0 and later)
- Mitel 6000 SIP Phone Model 6970 IP Conference Phone (version 5.0 and later)
- Mitel 6000 SIP Phone all_models: all Mitel 6000 SIP Phone models are configured in the same way.

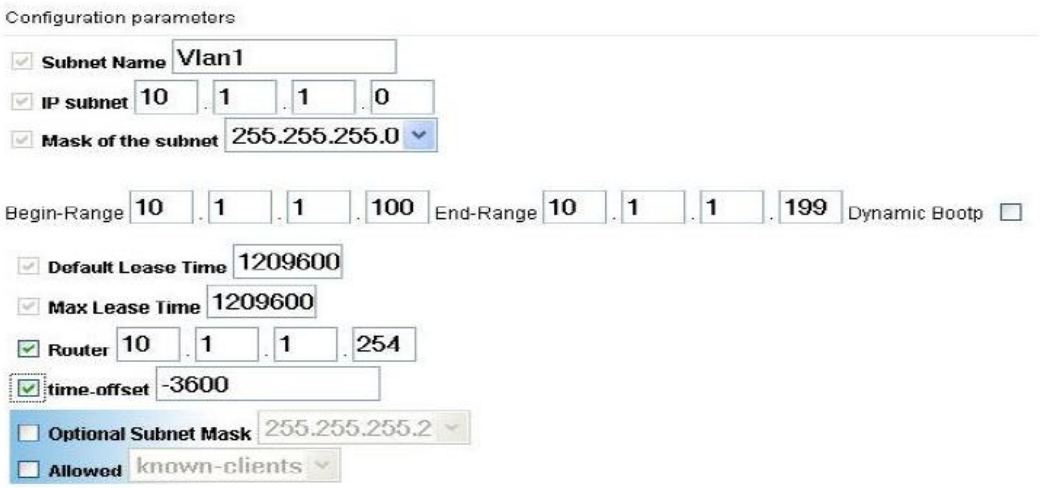
Reminder: The other ranges are not handled in this document.

Note : For the Mitel 6000 SIP Phone range, you can use either the all_models option or select the models one by one.

The terminal types are associated with the profiles whose unique identifier is the terminal's supplier class. This supplier class is the discriminating condition displayed above in the MMI used to filter and accept only DHCP requests from this terminal.

ATTENTION : If you want the embedded DHCP server to also respond to requests from devices without a Vendor Class (servers, PC, etc.), you must set the parameter *Permit* to *All clients*.

6.3.3 CONFIGURING THE STANDARD PARAMETERS OF THE SUBNET



Enter the following parameters:

- Subnet name: indicate, for instance, the membership VLAN or the actual name.
- Subnet IP: enter the subnet IP address.
- Subnet mask: select the subnet mask.
- Start of segment: enter the first IP address available in the segment.
- End of segment: enter the last IP address available in the segment.
- Default lease duration: 14 days by default (this value is expressed in seconds and can be modified if necessary). Lease assigned to the client who has not asked for a specific duration
- Max. lease duration: 14 days by default (this value is expressed in seconds and can be modified if necessary). maximum duration of a lease assigned to a client who has asked for a specific duration
- Interface: device name corresponding to the network interface of the system connected to the client's local network (default is **eth0**)
- All of these parameters are necessary and obligatory (checkbox in reverse video).
- The following parameters are required but may be optional depending on the client's network configuration:
- Router: specifies the gateway (router) IP address used to leave the subnet
- Permit: used to indicate whether only known clients are managed by the embedded DHCP server or whether all clients are managed by the embedded DHCP server. Known clients must have a Vendor Class defined with specific parameters associated with them. New devices can be

managed via the Template management menu. These new devices are necessarily associated with a new Vendor Class.

- Optional subnet mask*
- NTP server address*
- DNS server address*
- Domain name*.

6.3.4 CONFIGURING SPECIFIC SUBNET PARAMETERS FOR MITEL 6000 SIP PHONES

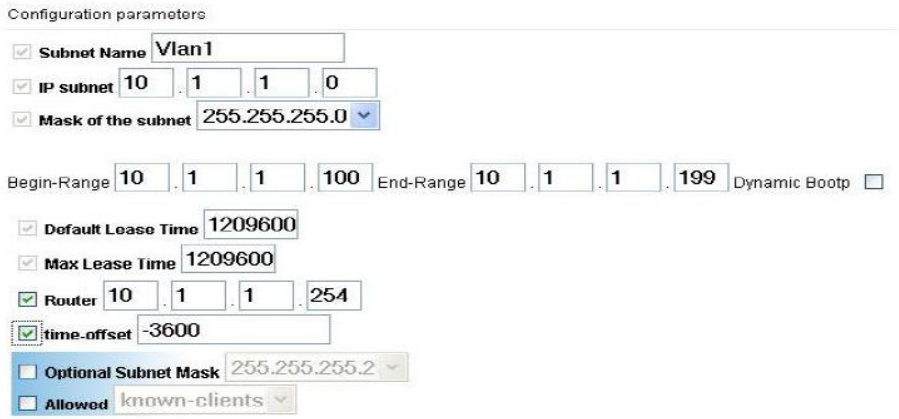
ATTENTION : For the Mitel 6000 SIP Phone range, you can use either the all_models option or select the models one by one.

Tick the **6xxxi Model all_models** range if any of the following terminal models is available on the subnet in question and must be managed by the integrated DHCP server:

- Models 6730 SIP, 6731 SIP, 6751 SIP, 6753 SIP, 6755 SIP and 6757 SIP (version 2.1 and later)
- Model 6739i (version 3.0 and later)
- Model 6735 SIP and 6737 SIP (version 3.2 and later)
- Model 6863 SIP, 6865 SIP, 6867 SIP and 6869 SIP (version 3.3 and later)
- Model 6873 SIP (version 4.2 and later)
- Model 6920 IP, 6930 IP 6940 IP,6905 IP, 6910 IP and 6970 IP conference phone (version 5.0 and later).

Note : If the 6xxxi Model all_models range is not ticked, it is possible to select the terminal models one by one by ticking the Mitel 6000 SIP Phone model concerned.

No matter the Mitel 6000 SIP Phone model selected, the configuration is the same.



The **upper part** defines the **specific network parameters negotiated via option 43** with the terminals for the subnet in question.

Fill in the following specific parameters**(parameters of option 43**):

- **cfg-server-address**: IURL of the download server on which the firmware and configuration files are stored. For a simplified configuration, enter the URL of the download server embedded on Mitel 5000 Gateways or MiVoice 5000 server systems.
  For this range of terminals, indicate the URL to reach **http://IP/6xxxi/deploy where IP is the IP address of the download server.**

- **RCS contact**: The parameter used to disable the RCS (Redirection & Configuration Server): If this parameter is not ticked, the RCS is disabled.

The **lower part** defines the **standard network parameters** negotiated with Mitel 6000 SIP Phones for the subnet in question.

The following standard parameters are optional, depending on the client's network configuration:

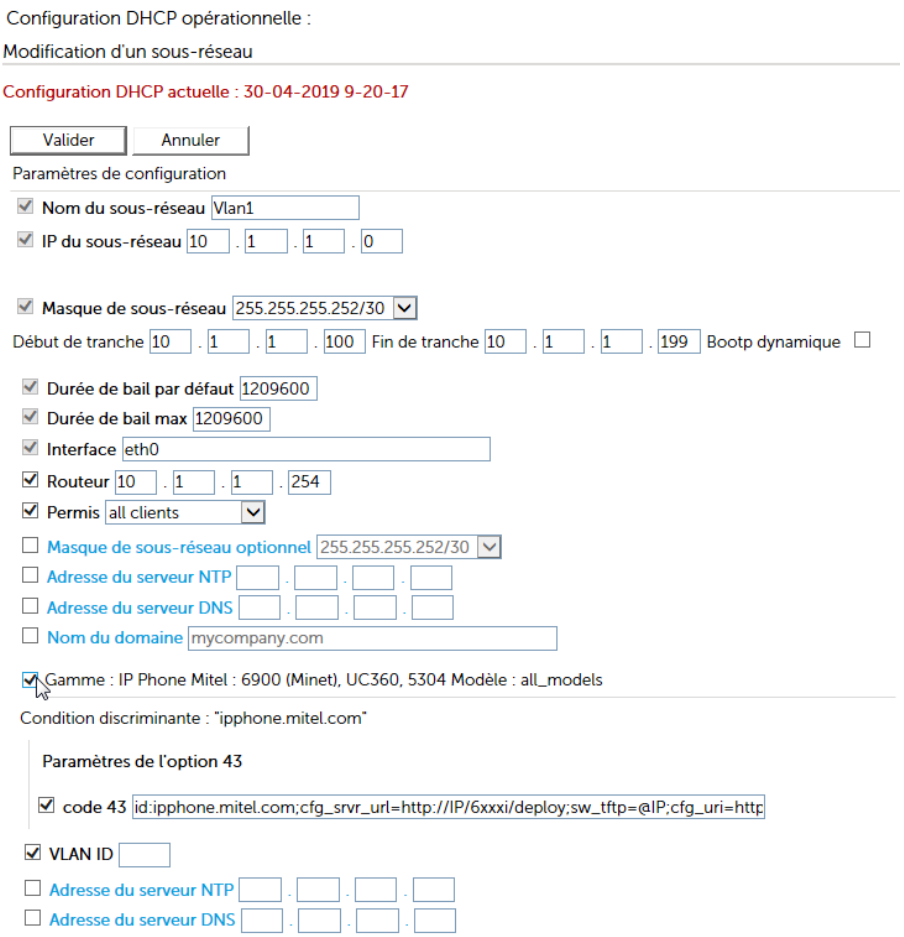
- **Id of the VLAN** that can be configured in the configuration files (MN_Generic.cfg, MN_@MAC;cfg).
- **NTP server address**
- **DNS server address**

Note : If these parameters are entered, they are taken into account instead of those defined in the subnet's general parameters.

- Confirm the current configuration by clicking the **Validate** button.

6.3.5 CONFIGURING SPECIFIC SUBNET PARAMETERS FOR TERMINALS 6900

Tick **Range**: **Mitel IP Phone: 6900 (Minet), UC360, 5304 Model: all_models** if one of the following workstation models is present on the subnet concerned and must be managed by the DHCP server:



The **upper part** defines the **specific network parameters negotiated via Option 43** with terminals 6900, UC360 and 5304 for the subnet in question.

Fill in the parameter **cfg-server-address** for negotiation via Option 43:

- **cfg-server-address**: IURL of the download server on which the firmware and configuration files are stored. For a simplified configuration, enter the URL of the download server embedded on Mitel 5000 Gateways or MiVoice 5000 server systems.
  For this range of terminals, indicate the URL to reach **http://IP/6xxxi/deploy where IP is the IP address of the download server.**

Example of a chain

id:ipphone.mitel.com;**cfg_srvr_url=http://10.10.0.5/6xxxi/deploy**;sw_tftp=@IP;cfg_uri=http://@IPserver/path;call_srv=@IP;mode=sip;dscp=2;\0x000

In IPV6, if Minet is compatible, indicate the IPV6 link.

- **RCS contact**: The parameter used to disable the RCS (Redirection & Configuration Server): If this parameter is not ticked, the RCS is disabled.

The **lower part** defines the **standard network parameters negotiated** with terminals 6900, UC360 and 5304 for the subnet in question.

The following standard network parameters are optional, depending on the subnet configuration:

- **VLAN ID** that can be configured in the configuration files (MN_Generic.cfg, MN_@MAC;cfg).
- NTP server address
- DNS server address

Note : If these parameters are entered, they are taken into account instead of those defined in the subnet's general parameters.

Confirm the current configuration by clicking the **Validate** button.

6.3.6 INTEGRATION OF TERMINALS 6900 INTO THE EMBEDDED DHCP OF A MIVOICE 5000 SOLUTION

Terminals 6900 work with two different software programs: MINET (default mode, factory default) and SIP. MiVoice 5000 does not support terminals 6900 in MINET, but only in SIP.

A preliminary step is therefore necessary so that terminal 6900 in MINET can be updated in SIP.

Terminals 6900 offer two different vendor classes (= Option 60), depending on the software downloaded:

- If the terminal has the software MINET, the vendor class is "**ipphone.mitel.com**", regardless of the model. In the DHCP embedded in the MiVoice 5000 solution, this corresponds to the "**Mitel IP Phone: 6900 (Minet), UC360, 5304**".
- If the workstation has the SIP software, the vendor class is in the following format: "**AastraIPPhone69x0**" (**AastraIPPhone6920**, **AastraIPPhone6930**, **AastraIPPhone6940, AastraIPPhone6970, AastraIPPhone6905, AastraIPPhone6910**). In the DHCP embedded in the MiVoice 5000 solution, this corresponds to the device "**6xxxi/all_models**" for global management or respectively "**6xxxi/6920**", "**6xxxi/6930**" and "**6xxxi/6940**", "**6xxxi/6905**", "**6xxxi/6910**", "**6xxxi/6970**", for management specific to each model.

ATTENTION : To manage terminals 6900 at the level of the DHCP embedded in the MiVoice 5000 solution, it is therefore necessary to select these two types of devices, knowing that these devices do not require the same DHCP parameters.

For MiVoice 5000 system upgrades, an automatic update of the DHCP configuration is provided for only in the case below, if in the DHCP configuration:

- The equipment "**6xxxi/all_models**" is selected,
- AND the device "**MiVoice Conference Unit**" is not selected,
- AND "**IP Phone Mitel / UC360_5304**" is not selected.

This automatic update adds the management of the new equipment "***IP Phone Mitel: 6900 (Minet), UC360, 5304***" *by initialising the parameter values with those entered for the equipment "****6xxxi/allmodels****" for each subnetwork managing these workstations* ***"6xxxi/allmodels"*** *and deleting the template files "****templateUC360.xml*** **" and** ***"templateIpPhoneMitel.xml*** **".**

Other upgrade cases, with the addition of terminal 6900, require a manual update of the DHCP configuration. We will distinguish the following cases:

- The "**6xxxi/all_models**" (or specific 6xxxi models) and "**MiVoice Conference Unit**" (via the template file templateUC360.xml) are selected.
- *The equipment "*6xxxi/all_models" (or specific 6xxxi models) and "IP Phone Mitel / UC360_5304" (using the template file templateIpPhoneMitel.xml*) are selected*.

6.3.6.1 *Description of the parameters*

To manage the new "**Mitel IP Phone: 6900 (Minet), UC360, 5304**", the DHCP server embedded in the MiVoice 5000 solution offers the following DHCP parameters, specific to each subnet:

- **Option 43**: string of characters, respecting the following syntax:

  ```
  id:ipphone.mitel.com;cfg_srvr_url=http://IP/6xxxi/deploy;sw_tftp=@IP;
  cfg_uri=http://@IPserver/path;call_srv=@IP;mode=sip;dscp=2;\0x000
  ```

  where

- ***cfg_srvr_url=ftp:// IP/6xxxi/deploy/***: useful for terminal 6900 in MINET mode, must contain the ~~FTP~~ address of the deployment directory containing the SIP software,
- ***sw_tftp=@IP***Useful for Mitel MiVoice 5304 IP Phone, TFTP address of the directory containing the files needed for the station,
- ***cfg_uri=http://@IPserver/path***: useful for the MiVoice Conference Unit, must contain the HTTP address of the directory containing the necessary files.
- ***call_srv=@IP:*** useful parameter for the MiVoice Conference Unit and Mitel MiVoice 5304 IP Phone, IP address of the call server,
- ***Mode=sip:***: useful for Mitel MiVoice 5304 IP Phone to force operation in SIP mode, the value is already set,
- ***Dscp=2***: useful for Mitel MiVoice 5304 IP Phone, for QoS.
- **Option 132**: VLAN ID.

Note : For these "ipphone.mitel.com" devices, the VLAN can also be specified in the string of Option 43, by adding the "vlan" parameter.

6.4 EMBEDDED IP V6 SERVICE

6.4.1 CREATING A NEW DHCP V6 CONFIGURATION

- From Menu **DHCP - Creation**

A confirmation message appears:

- Click the **Validate** button to confirm the overwriting of the current configuration data and the creation of a new, current configuration.

The general parameters configuration window opens.

- Store the current configuration before overwriting it.

6.4.2 CONFIGURING THE GENERAL PARAMETERS

6.4.3 EDITING THE GENERAL PARAMETERS

- **DDNS update type***: none > Leave this default value.
- **The network is authoritative***: yes (ticked) > Leave this default value.
- **DHCP renewal time (Optional)**: Between 0 and 100000
- **DHCP binding time (Optional**): Between 0 and 100000
- **Info Refresh Time (Optional)**: Between 0 and 100000
- **DNS Server (Optional)**: DNS server ipv6 address

6.4.4 CREATING A SUBNET

From the previous screen:

Click **Add** (in the Subnet column on the top right side).

Enter the following parameters:

Subnet name: indicate, for instance, the membership VLAN or the actual name.

Network prefix: enter the subnet IPV6 address.

Subnet mask: select the subnet mask.

Start of segment: enter the first IP address available in the segment.

End of segment: enter the last IP address available in the segment.

Default lease duration: 14 days by default (this value is expressed in seconds and can be modified if necessary). Lease assigned to a client who has not asked for a specific duration.

Max. lease duration: 14 days by default (this value is expressed in seconds and can be modified if necessary).

maximum duration of a lease assigned to a client who has asked for a specific duration

Preferred service life:

7 days by default.

Interface: device name corresponding to the network interface of the system connected to the client's local network (by default eth0).

All of these parameters are necessary and obligatory (checkbox).

The following parameters are required but may be optional depending on the client's network configuration:

Permit: used to indicate whether only known clients are managed by the embedded DHCP server or whether all clients are managed by the embedded DHCP server. Known clients must have a Vendor Class defined with specific parameters associated with them. New devices can be managed via the **Template management** menu. These new devices are necessarily associated with a new Vendor Class.

NTP server address*:

Domain name*: FQDN of the domain.

Note: * The meaning of these parameters is indicated in Appendix 2. If these parameters are configured, the defined values are common to all devices without Vendor Class.

7 CONFIGURING AN EXTERNAL DHCP SERVER

7.1 CONFIGURING THE EXTERNAL DHCP SERVER FOR MITEL 6000 SIP PHONES

7.1.1 STANDARD PARAMETERS OR DHCP OPTIONS MANAGED BY MITEL 6000 SIP PHONES

Mitel 6000 SIP Phones have an integrated DHCP client.

The table below describes the standard options managed by Mitel 6000 SIP Phones.

STANDARD PARAMETER OR DHCP OPTION	NOTE
IP address and subnet mask (option 1)	parameter required in option 55
Gateway IP address (option 3)	parameter required in option 55
DNS server IP address (option 6)	parameter required in option 55
NTP server IP address (option 42)	parameter required in option 55
Vendor-specific option (option 43)	parameter required in option 55
Vendor-class-specific information (option 60)	* See the name in the table below.
Downloading server IP address (option 66)	cfg-server-address: IURL of the download server on which the firmware and configuration files are stored. For a simplified configuration, enter the URL of the download server embedded on Mitel 5000 Gateways or MiVoice 5000 server systems. For this range of terminals, indicate the URL to reach http://IP/6xxxi/deploy where IP is the IP address of the download server.
VLAN ID (option 132)**	parameter required in option 55

SET MODEL	VENDOR CLASS
A6751SIP	AastraIPPhone51i
6753 SIP	AastraIPPhone53i
6755 SIP	AastraIPPhone55i
6757 SIP	AastraIPPhone57i
6730 SIP	AastraPPhone6730i

6731 SIP	AastraIPPhone6731i
6735 SIP	AastraPPhone6735i
6737 SIP	AastraIPPhone6737i
6739 SIP	AastraPPhone6739i
6863 SIP	AastraIPPhone6863i
6865 SIP	AastraIPPhone6865i
6867 SIP	AastraIPPhone6867i
6869 SIP	AastraIPPhone6869i
6873 SIP	AastraIPPhone6873i
6920 (SIP)	AastraIPPhone6920
6930 (SIP)	AastraIPPhone6930
6940 (SIP)	AastraIPPhone6940
6970 (SIP)	AastraIPPhone6905
6905 (SIP)	AastraIPPhone6910
6910 (SIP)	AastraIPPhone6970
6920 (Minet)	ipphone.mitel.com
6930 (Minet)	ipphone.mitel.com
6940 (Minet)	ipphone.mitel.com
6970 (Minet)	ipphone.mitel.com
6905 (Minet)	ipphone.mitel.com
6910 (Minet)	ipphone.mitel.com
Mitel IP Phone: 6900 (Minet), UC360, 5304	ipphone.mitel.com
BluStar 8000i	AastraBluStar8000i

The DHCP negotiation of option 132 requires the parameter dhcp option 132 vlan id enabled to be set to 1 in the global or specific configuration file used by Mitel 6000 SIP Phones (aastra.cfg or<mac>.cfg).

* Name of the Vendor Class used by Mitel 6000 SIP Phones according to terminal model:

The priority order in which the VLAN ID is taken into account by Mitel 6000 SIP Phones is as follows:

- 1 VLAN ID negotiated via LLDP (highest priority)
- 2 VLAN ID negotiated via DHCP (option 43 higher priority than option 132)
- 3 VLAN ID configured via the terminal’s WEB interface
- 4 VLAN ID configured via aastra.cfg or <mac>.cfg

7.1.2 DHCP SPECIFIC PARAMETERS MANAGED BY MITEL 6000 SIP PHONES VIA OPTION 43

Mitel 6000 SIP Phones send option 60 of the DHCP protocol (vendor class identifier) in the DHCP request (discover/request) to identify themselves. Moreover, Mitel 6000 SIP Phones ask the DHCP server for vendor specific information, by specifying option 43 in its list of requests for parameters associated with option 55. If the DHCP server is configured to react to the vendor specific identifier, it will add option 43 (vendor specific information) to these replies.

The table below describes all the parameters that can be negotiated via option 43 with Mitel 6000 SIP Phones:

SPECIFIC PARAMETERS (OPTION 43)	CODE	HEX. VALUE CODE	LENGTH/ TYPE	NOTE
cfg-server-address	02	02	String	URL of the download server. http//IP/6xxxi/deploy
cfg-contact-rcs	03	03	Booleen	Disabling RCS: set the value to **false**
VLAN_ENABLED	08	08	16 bytes/text	Value in hexa: 41 61 73 74 72 61 20 54 65 6c 65 63 6f 6d 20 20 (corresponds to "Aastra Telecom" followed by 2 spaces)
VLAN_ID	09	09	4 bytes/integer	Specifies the VLAN ID used by the terminal's VLAN port (example: 00 00 00 64 for vlan 100)

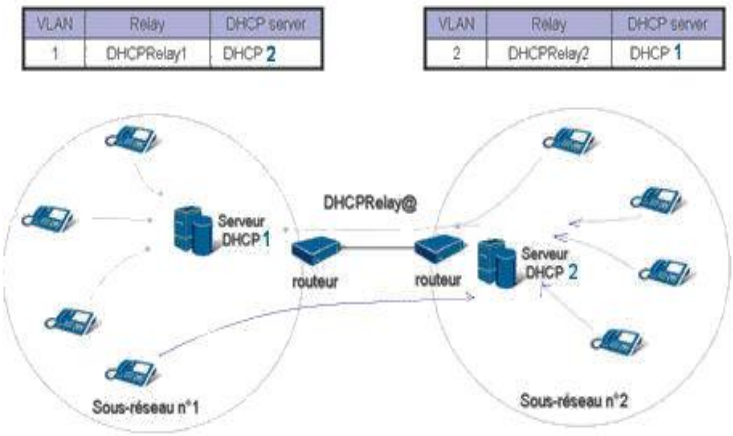
ATTENTION : Set the parameter cfg-contact-rcs to false. Codes 08 and 09 must be negotiated together.

7.2 CONFIGURING THE EXTERNAL DHCP SERVICE IN A REDUNDANT MIVOICE 5000 SERVER ARCHITECTURE

Two external DHCP servers can be activated simultaneously to duplicate the DHCP service.

Each DHCP server (1 & 2) must be able to provide IP addresses for all Mitel 6000 SIP Phones on each site. For this, each site's IP subnet declaration will be shared between the two DHCP servers in order to avoid IP address duplication. The number of available IP addresses per server must be enough to provide the required amount if any of the two DHCP servers fails.

ATTENTION : For the DHCP request sent by a terminal to be processed correctly, a DHCP RELAY function is implemented on each router setting up connection to the terminal VLAN on the site. The DHCP request must be sent to the two DHCP servers installed and configured on each MiVoice Server platform. The DHCP service is external. It is not installed and managed by the MiVoice 5000 Server Web Admin.



8 APPENDICES

8.1 MANUALLY CONFIGURING MITEL 6000 SIP PHONES

Manual configuration of Mitel 6000 SIP Phones may be envisaged for implementing some terminals on a single-site Mitel 5000 Gateways system for which the integrated TMA application is not used. This solution requires the availability of an integrated or external download server. The network parameters required by the terminal to work well are declared manually, either from the terminal or from the WEB interface.

These network parameters can also be configured and downloaded from the download server.

In this case, the integrated download server IP address, login and password associated with the user account used by Mitel 6000 SIP Phones are the only network parameters that require a manual configuration.

Configuration files are made available manually on the download server storage area by the administrator.

8.1.1 DEFAULT CONFIGURATION WHEN THE TERMINAL IS INSTALLED FOR THE FIRST TIME

A new terminal has the following factory configuration (default configuration):

- The DHCP option is enabled.
- The terminal's default IP address is: 169.254.114.9
- The default sub-net mask value is: 255.255.255.0
- TFTP is enabled.

8.1.2 MANUAL CONFIGURATION FROM MITEL 6000 SIP PHONES

You can access the manual configuration of the terminal via the "Options" key.

A password is required for the parameters reserved for the administrator.

By default, this password is: 22222

You can choose menus with the navigation key and/or display keys (6755 SIP and 6757 SIP phones).

You can use the UP and DOWN arrow keys to display the different status and text messages on the LCD (if there is more than one status/text message line). You can also use these keys to scroll down the menu options, like the options list.

You can use the LEFT and RIGHT arrows to view the different call lines/functions.

If you are on the options list, you can use these keys to open or exit the current option. If you are editing inputs on the screen, the LEFT arrow deletes the character on the left while the RIGHT arrow confirms the option.

You can use the display keys to directly access a function, for instance, to take account of the parameters of a menu ('Done').

To configure each parameter, use the contextual keys:

- Change: to change the value or content of a parameter
- Done: to save the modification
- Cancel: to cancel the modification and return to the previous menu.

Note : * To access the administration menu of the 6751 SIP phones:
Press the Services key. Select the Options menu. Select an option and browse through the list, or press the number corresponding to the option.

8.1.3 CONFIGURING THE NETWORK PARAMETERS OF MITEL 6000 SIP PHONES

- Press the ‘Options’ key.
- In the parameter option list, select: **Administrator Menu** then press **Select**.
- Enter the administrator password (22222) then press ’Enter’ to confirm.
- Select **Network Settings** then press **Select**.
- Use the navigation key to access the different network parameters:

  1-DHCP

  2-IP Address

  3-Subnet Mask

  4-Gateway
- Set the **DHCP** field to **No**.
- Fill in the fields corresponding to the terminal IP address, subnet mask and gateway (router) IP address.

8.1.4 CONFIGURING THE MITEL 6000 SIP PHONE DOWNLOAD SERVER PARAMETERS

- Press the **Options** key.
- In the parameter option list, select: **Administrator Menu** then press **Select**.
- Enter the administrator password (22222) then press **Enter** to validate.
- Select **Configuration server** then press **Select**.
- Select **Download protocol** then press **Select**.
- Using the navigation key, select **use FTP** and confirm with the **Done** key.
- In the **Configuration Server** menu, select the parameter **FTP Settings**.
- In **FTP Server** menu, enter the download server IP address.
- In the **FTP Username** menu, enter the login of the download server account used by Mitel 6000 SIP Phones.
- In the **FTP Password** menu, enter the account password.

8.1.5 CONFIGURING THE SIP PARAMETERS OF MITEL 6000 SIP PHONES

- Press the **Options** key.
- In the parameter option list, select: **Administrator Menu** then press **Select**.
- Enter the administrator password (22222) then press **Enter** to validate.
- Select **SIP Settings** then press **Select**.
- Select **Proxy IP/Port** then press **Select**.
- Enter the SIP access point address (UCV card IP address) and the default port address (5060).
- Select **Registar IP/Port** then press **Select**.
- Enter the SIP access point address (UCV card IP address) and the default port address (5060).
- Select **User Name** then press **Select**.
- Enter the subscription number of the terminal declared in the iPBX.
- Select **Display Name** then press **Select**.
- Enter the name that must be displayed on the requested terminal screen.
- Select **Screen Name** then press **Select**.
- Enter the name that must be displayed on the terminal screen.

Note : These parameters may be configured in the files aastra.cfg and MAC@.cfg then downloaded to the terminal from the download server.

ATTENTION : UDP ports 5060 (signal flow) and 40000 (voice flow) must be open on the MiVoice 5000 Server if the firewall is enabled.

8.1.6 CONFIGURING THE VLAN SETTINGS OF THE MITEL 6000 SIP PHONE LAN PORT

- Press the **Options** key.
- In the parameter option list, select: **Administrator Menu** then press **Select**.
- Enter the administrator password (22222) then press **Enter** to validate.
- Select **Network Settings** then press **Select**.
- Select **VLAN Settings** then press **Select**.
- Select **VLAN Enable** and set the value to **Yes** to authorise frame marking.
- Select **LAN port VLAN** then **LAN port VLAN ID** and set the ToIP VLAN value.
- Select **VLAN priority** and set the value of the priority associated with the ToIP VLAN for signal (SIP) and audio (RTP) flows.

Note : These parameters may be configured in the file aastra.cfg then downloaded to the terminal from the download server.

8.1.7 CONFIGURING THE VLAN SETTINGS OF THE MITEL 6000 SIP PHONE PC PORT

- Press the **Options** key.
- In the parameter option list, select: **Administrator Menu** then press **Select**.
- Enter the administrator password (22222) then press **Enter** to validate.
- Select **Network Settings** then press **Select**.
- Select **VLAN Settings** then press **Select**.
- Select **PC port VLAN** then **PC port VLAN ID** and set the Data VLAN value.
- Select **PC port priority** then set the priority value associated with the Data VLAN.

Note : These parameters may be configured in the file aastra.cfg then downloaded to the terminal from the download server.

8.1.8 RESTARTING MITEL 6000 SIP PHONES

- Press the ‘Options’ key.
- From the options list, select the parameter ‘Restart Phone’ and press ‘Select’.
- Confirm the restart operation by selecting and pressing ‘Restart’.

The terminal restarts, taking account of the previously modified parameters. This will enable it to connect to the download server and to download the firmware, configuration files and language packs available in the server storage area.

8.1.9 CONFIGURE MITEL 6000 SIP PHONES IN ENGLISH LANGUAGE:

Note : The languages are available in the ‘languages pack’ and must be downloaded to the terminal for use. They can be downloaded from the download server, either by restarting the terminal manually, or by programming automatic update via the parameter Auto-Resync in Menu Advanced settings>Configuration server.

- Press the **Options** key.
- From the options list, select **Preferences** and press **Select**.
- In the **Preferences** menu, select **Language** then press **Select**.
- In the **Language** menu, select **Screen Language** then press **Select**.
- Change the language with the navigation key then confirm the selection with the **Done** key.
- In the **Language** menu, select ‘Input Language’ then press **Select**.
- Change the language with the navigation key then confirm the selection with the **Done** key.

8.2 MANUAL CONFIGURATION FROM THE WEB INTERFACE OF MITEL 6000 SIP PHONES

First define the terminal IP address via the terminal interface.

Connect via a WEB browser: http://@IP_poste_A6xxxi

- Access in User mode:
- Username: user
- Password: 11111
- Access in Administrator mode:
- Username: admin
- Password: 22222

8.2.1 CONFIGURING THE BASIC NETWORK PARAMETERS OF MITEL 6000 SIP PHONES

Procedure:

- Connect as Administrator.
- In Menu **Advanced settings > Network**, disable DHCP mode to automatically obtain an address and enter manually the IP address, subnet mask and default gateway of Mitel 6000 SIP Phone.
- Confirm your modifications by clicking **Save settings**.

8.2.2 CONFIGURING THE DOWNLOAD SERVER FOR MITEL 6000 SIP PHONES

The terminals' firmware release and configuration files are made available, by default, in the download server storage directory integrated into the system's UCV card.

This window allows you to enter the IP address of a download server so as to download files to the terminal (for updating the firmware, configuration files, and language packs).

Procedure:

- Connect as Administrator.
- In Menu **Advanced settings > Configuration server**, select **FTP** in the **Download protocol**, for an external server.
- Enter the download server IP address as well as the login and associated password.
- Confirm your modifications by clicking **Save settings**.

Note : For an embedded or MiVoice 5000 Manager-based download server, select the http or https protocol and enter only the IP address.

8.2.3 CONFIGURING THE SIP PARAMETERS OF MITEL 6000 SIP PHONES

This window allows you to define the terminal's global settings. The basic settings are:

- Screen Name and Screen Name 2: name displayed on the terminal,
- Phone Number: terminal subscription number,
- Proxy Server / Registrar Server: SIP access point IP address,
- Proxy Port / Registrar Port: use the standard value 5060,
- Registration Period: use the standard value 3600 (1h).

Procedure:

- Connect as Administrator.
- In Menu **Advanced settings > global SIP**, enter the parameters described above.
- Confirm your modifications by clicking **Save settings**.

Note : These parameters may be configured in the files aastra.cfg and MAC@.cfg then downloaded to the terminal from the download server.

8.2.4 RESTARTING MITEL 6000 SIP PHONES

Procedure:

- connect as Administrator.
- In Menu **Operation >Reset**, click **Restart Phone**.

The terminal restarts, taking account of the previously modified parameters. This will enable it to connect to the download server and to download the firmware, configuration files and language packs available in the server storage area.

8.2.5 CONFIGURING THE WEB INTERFACE LANGUAGE

To change the web interface language:

- connect as Administrator.
- In Menu **Basic Settings > Preferences**, select the language of your choice from those available in the parameter **Webpage Language**:
  - English
  - English
  - German
  - Italian
  - Spanish
- Confirm your modifications by clicking <**Save settings**>.

Note : The languages are available in the 'languages pack' and must be downloaded to the terminal for use. They can be downloaded from the download server, either by restarting the terminal manually, or by specifying the name of the language file to use. Programming an automatic update via the parameter Auto-Resync in Menu Advanced settings > Configuration server automates this downloading operation.

8.2.6 DOWNLOADING A LANGUAGE PACK TO MITEL 6000 SIP PHONES

A language pack can be downloaded to Mitel 6000 SIP Phone in two ways:

- Via the file aastra.cfg
- Via the web interface

Via the file aastra.cfg

You can use the configuration file aastra.cfg to specify the language pack to download using the following format:

lang_<ISO 639>-<ISO 3166>.txt or lang_<ISO 639>.txt where <ISO 639> is the language code specified in standards ISO 639 and <ISO 3166> is the country code specified in standard ISO 3166

<ISO 3166> is an optional attribute.

The addition or modification of a language pack is only taken into account when the terminal is restarted. The default language (English) can neither be modified nor deleted.

The following example describes the default configuration made in the file aastra.cfg to download the language packs French, Italian, German and Spanish to Mitel 6000 SIP Phones.

language 1: lang_fr.txt # French language file name

language 2: lang_de.txt # German language file name

language 3: lang_it.txt # Italian language file name

language 4: lang_es.txt # Spanish language file name

Via the web interface

- connect as Administrator.
- In Menu **Basic Settings > Preferences > Language Settings**, enter the language pack to download in language fields 1 to 4:
  - lang_fr.txt
  - lang_de.txt
  - lang_it.txt
  - lang_es.txt
- Confirm your modifications by clicking **Save settings**.

ATTENTION : You have to restart the terminal for the downloaded language pack to be taken into account.

8.2.7 RINGER CUSTOMISATION ACCORDING TO CALL TYPE ON MITEL 6000 SIP PHONE

8.2.7.1 *General information*

For terminals 6800/6900: According to Standard RFC 7462, when a call comes in, the phone uses the ring tone associated with "Internal calls", "External calls" for the (internal / external) paging group".

For each of these incoming call types, the ring tone of a phone can be customised according to those available in the particular phone model.

8.2.7.2 *Principle*

It is all about placing the alert type (external, internal or group alert) on the **Alert-info** header and to specify its origin:

- Example: **Alert-Info: info=alert-external**

The ring tone type to be emitted is determined in TMA when preparing for deployment (refer to paragraph 8.2.7.3.

The correspondence between **alert-info** and **Bellcore** ring tone is done in the SIP terminal and varies according to terminal type:

Bellcore Tone	Pattern ID	Pattern	Cadence	Min duration (ms)	Norm duration (ms)	Max duration (ms)
Standard	1	Ring tones	Ring 2s	1800	2000	2200
		Silence	Silence 4s	3600	4000	4400
Bellcore-dr2	2	Ring tones	Long	630	800	1025
		Silence		315	400	525
		Ring tones	Long	630	800	1025
		Silence	Long	3475	4000	4400
Bellcore-dr3	3	Ring tones	Short	315	400	525
		Silence		145	200	525
		Ring tones	Short	315	400	525
		Silence		145	200	525
		Ring tones	Long	630	800	1025
		Silence		2975	4000	4400
Bellcore-dr4	4	Ring tones	Short	200	300	525
		Silence		145	200	525
		Ring tones	Long	800	1000	1100
		Silence		145	200	525
		Ring tones	Short	200	300	525
		Silence		2975	4000	4400
Bellcore-dr5	5	Ring tones		450	500	550

The Bellcore ring tone type must be different for each type of incoming call (Internal, External and Group).

Handling the header when a call arrives

External call
When the parameter "**alert-external**" appears in the header of the INVITE request, the set Bellcore ring tone is applied to the IP terminal.

FORMAT Integer
DEFAULT VALUE 0 Normal ringing
RANGE 0 Normal ringing (default)
1 Bellcore-dr2
2 Bellcore-dr3
3 Bellcore-dr4
4 Bellcore-dr5
5 Silent
Example > alert external: 4

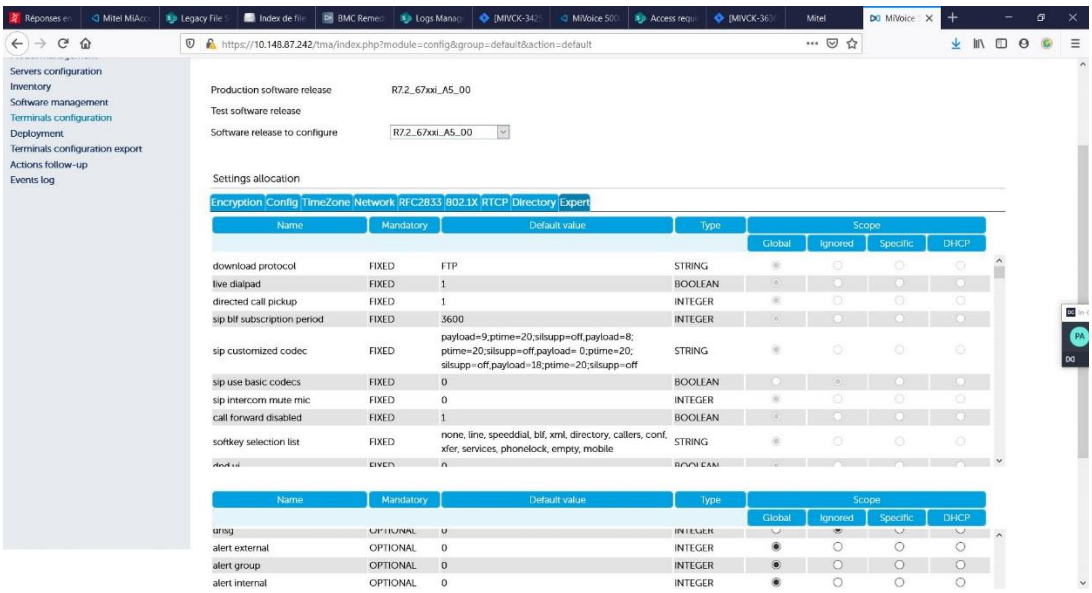
Internal call and Hunt group call
The same principle:
Example > alert group: 3
Example > alert internal: 1

8.2.7.3 *Configuring and deploying terminals via the file aastra.cfg*

The principle is to configure TMA for deployment with the following parameters:

alert group: 1
alert external: 3
alert internal: 2

These three keys are available in the area in the **Expert** tab of the **Terminals configuration** menu:



For these 3 parameters, also define the type of range (Global or specific).

Then the correspondence between **alert-info** and the **Bellcore** ring tone is done, during deployment, in the SIP terminal and varies according to terminal type.

For implementation, see Section 8.2.7.2.

8.2.8 ANALOGUE TERMINALS ON EX/GX/TA SYSTEMS

For all these analogue terminals seen as SIP terminals, the ring tone depends on the internal or external call type. There is no special Hunt group ring tone.

8.3 CONFIGURING MITEL 6000 SIP PHONES FOR THE DUAL HOMING FUNCTION

The dual Homing function enables a terminal to connect to a backup site when it is not possible to connect to its reference site, either because the reference site is out of service or because it is not accessible through the network.

The diagram below illustrates the architecture.

The parameters to define on Mitel 6000 SIP phones are:

- **sip backup proxy ip** => Specifies the IP address of the backup site SIP gateway
- **sip backup proxy port** => Specifies the listening port of the backup site SIP gateway
- **sip backup registrar ip** => Specifies the IP address of the backup site SIP gateway
- **sip backup** registrar port => Specifies the listening port of the backup site SIP gateway

These four parameters can be configured through any of the following two methods:

- Via the global configuration file **aastra**.cfg or specific configuration file <**MAC**>**.cfg**, depending on the client network architecture. By default, these parameters are defined in the file **aastra.cfg** , and the corresponding lines are in comments.
- Through manual configuration via the terminal's web configuration interface (Menu **Advanced Settings>Global SIP>Basic SIP Network Settings**).

ATTENTION : More information about the working of the Dual Homing function and the configuration to perform on Web Admin or MiVoice 5000 Manager is given in the Multi-site Operating Manual (AMT/PTD/PBX/0081*).

8.4 CONFIGURING MITEL 6000 SIP PHONES FOR THE AUTHENTICATION MD5 FUNCTION

8.4.1 OPERATING PRINCIPLE

The MD5 password is used to authenticate Mitel 6000 SIP Phones that connect to MiVoice 5000 Server and Mitel 5000 Gateways systems. This MD5 password is defined in the subscription of MiVoice 5000 Server and Mitel 5000 Gateways systems.

This control prevents another device with the same directory number from being registered mistakenly or maliciously.

A check is performed in the following two cases:

- Each time the terminal is registered on the iPBX
- Before each outgoing call.

Note : Incoming calls are not checked.

The MD5 password is defined both in Mitel 6000 SIP Phone and in the iPBX.

Mitel 6000 SIP Phone is not operational in the following two cases:

- The MD5 password is different between Mitel 6000 SIP Phone and the iPBX.
- The MD5 password is defined in the iPBX but not in Mitel 6000 SIP Phone.

Note : If the MD5 password is defined in Mitel 6000 SIP Phone but not in the iPBX, the terminal will be operational.

8.4.2 CONFIGURING MD5 PASSWORD IN THE IPBX

To configure the MD5 password in MiVoice 5000 Server and Mitel 5000 Gateways systems, proceed as follows:

- Go to the MD5 password definition menu:

This menu (124) is accessible via Menu **Subscribers>Subscriptions>Terminal authentication** and MDP User Portal.

- Select the operation type: **SIP authentication.**
- Enter the start directory.
- Enter the end directory.
- Select the creation mode:
    - Manual creation.
    - Automatic generation.

For manual creation, enter the MD5 password for the selected events (alphanumeric code comprising between 8 and 16 characters).

- Click the **Confirmation** button to confirm the MD5 password creation.

The Export operation is used to generate and save a file in .csv format containing the subscriptions and their MD5 password.

It is possible to know whether a subscription has an already defined MD5 password:

This menu (1231) is accessible by Subscribers>Subscriptions>Features: **Terminal authentication** parameter on the **Characteristics** tab.

8.4.3 CONFIGURING THE MD5 PASSWORD MANUALLY IN MITEL 6000 SIP PHONES

This configuration method should only be used in the following cases:

- If the terminal service is not started in Web Admin (single-site configuration)
- If TMA is not configured in MiVoice 5000 Manager (multi-site configuration)

The parameters to define on Mitel 6000 SIP phones are:

- **sip line1 password**=> Specifies the MD5 password used by Mitel 6000 SIP Phones
- **sip line1 auth name**=> Specifies the authentication name used by Mitel 6000 SIP Phones

This parameter can be configured using any of the following three methods:

- Via the specific configuration file **<MAC>.cfg**. In this case, the lines **sip line1 password and sip line1 auth name** should not be in comment, and the line **sip line1 password** contains the MD5 password.
- In manual configuration via the terminal configuration menu (Menu **Options**>**Administrator** >**SIP Settings**>**Password** and **Authentication Name**)
- In manual configuration mode via the terminal configuration web interface (Menu **Advanced Settings>line1>Basic SIP Authentication Settings>Password** and **Authentication Name**).
- In multi-line configuration the parameter to configure is called **sip lineN password** where **N**= the line number from 1 to 9.

ATTENTION : Manual deployment through free seating of a Mitel 6000 SIP Phone with an MD5 password defined in its subscription requires TLS configuration. In this case, the password is transmitted to the terminal via NOTIFY messages

ATTENTION : In a multi-line configuration, the MD5 password is only controlled on the main number of the multi-line subscription.

8.5 CONFIGURING MITEL 6000 SIP PHONES IN AN 802.1X ENVIRONMENT

8.5.1 OPERATING PRINCIPLE

The purpose of standard 802.1X is to authenticate to the network access while logging on physically to the network. This authentication takes place before any self-configuration mechanism (such as DHCP). In most cases, the service authorised in case of success is the Ethernet service.

Therefore, the aim of this standard is only to validate a right to physically access the network, regardless of the transmission tool used and based on existing authentication mechanisms.

Three main items are involved in this mechanism:

- The system to authenticate (requester or client)
- The LAN access point (authenticator, switch, WiFi base station, etc.)
- The authentication server

An example of 802.1X architecture is given below:

As long as it is not authenticated, the client cannot access the network; only the exchanges relating to the authentication process are transmitted to the authentication server through the access point. Once authenticated, the access point leaves the client-related traffic to pass through.

The 802.1X protocol defines the use of EAP (Extensible Authentication Protocol, RFC3748), a mechanism which describes the authentication method.

Mitel 6000 SIP Phones support 802.1X authentication so as to:

- Authenticate them to a secure LAN according to the 802.1X protocol
- Allow transparent transmission of the authentication request from a PC connected to the switch incorporated into the terminal*

ATTENTION : * This configuration works only on certain network devices (switches).

8.5.2 CONFIGURING 802.1X AUTHENTICATION PARAMETERS ON TERMINALS MITEL 6000 SIP PHONES

Mitel 6000 SIP Phones authenticate to the network using the EAP-MD5 protocol.

Authentication thus takes place based on two parameters: login and password.

The parameters to define on Mitel 6000 SIP phones are:

- **eap type:** 1 => Specifies the protocol to use (1=EAP-MD5).
- **Identity:** xUsEr3 => Specifies the 802.1X login.
- **md5 password:** xPaSsWoRd3 => Specifies the 802.1X password.

These parameters can be configured using any of the following three methods:

- Via the specific configuration file **<MAC>.cfg**. In this case, the three lines below should not be in comment and should not contain the type of protocol used, the login and 802.1X password*.

ATTENTION : * If the 802.1X authentication parameters are negotiated via the specific configuration files, it is mandatory to make the first update on a network that does not implement 802.1x or on which it is deactivated.

- In manual configuration via the terminal configuration menu

  Menu **Options**>**Administrator Menu**>**Network Settings**>**Ethernet & VLAN**>**802.1X Settings**>**802.1X Mode**: **EAP-MD5.**

  Menu **Options**>**Administrator Menu**>**Network Settings**>**Ethernet & VLAN**>**802.1X Settings**>**EAP-MD5 Settings>Identity>User name**: enter the login.

  Menu **Options**>**Administrator Menu**>**Network Settings**>**Ethernet & VLAN**>**802.1X Settings**>**EAP-MD5 Settings>MD5 Password>Password**: enter the login.

- In manual configuration via the terminal's web configuration interface:

  Menu **Advanced Settings>802.1X Support>EAP Type>EAP-MD5.**

  Menu **Advanced Settings>802.1X Support>identity**: enter the login.

  Menu **Advanced Settings>802.1X Support>MD5 Password**: enter the login.

See the Section for the priority assigned to the parameter in case these parameters are defined using several methods.

8.5.3 MITEL 6000 SIP PHONE AUTHENTICATION PROCEDURES

The normal authentication procedures are:

- The switch port is closed.
- Mitel 6000 SIP Phone is physically connected to the switch port.
- The switch sends an authentication request to Mitel 6000 SIP Phone then to the RADIUS server.
- The switch port is opened.
- Mitel 6000 SIP Phone connects to the LAN (ARP, DHCP, etc.).

8.5.4 SWITCH BEHAVIOUR

- The switch port remains closed in case of error or non-response during authentication.
- A new authentication is started by the switch in case of error or non-response to the previous authentication.
- The switch detects the terminal's connection or disconnection to start the terminal authentication.
- If the switch port is closed, new authentication attempts are made after the terminal is disconnected then reconnected.

8.5.5 BEHAVIOUR OF MITEL 6000 SIP PHONES

The authenticator (switch) generally initiates the dialogue once the port becomes active and sends an EAP-request frame. If the authenticator fails to initiate the dialogue, Mitel 6000 SIP Phones can initiate it by sending an EAP-start frame.

Mitel 6000 SIP Phones respond to the re-authentication frames (every hour). The re-authentication mechanism can be activated during communication.

These exchanges are illustrated in the diagram below:

8.6 CONFIGURING MITEL 6000 SIP PHONE FOR THE SIGNAL AND VOICE ENCRYPTION FUNCTION

See the call encryption operating manual (AMT/PTD/PBX/0103*).

8.7 CONFIGURING MITEL 6800 AND 6900 IP PHONES FOR ACCESS TO THE LDAP DIRECTORY AND PERSONAL EXCHANGE CONTACTS

8.7.1 OPERATING PRINCIPLE

This function allows Mitel 6800 and 6900 IP Phone access via the **Pers. Ann.** (system key: personal directory) to the LDAP directory of Mitel 5000 Gateways or MiVoice 5000 Server or MiVoice 5000 Manager and to the personal contacts of the company's Exchange server.

For the 6867 and 6869 SIP Phones, this function is directly accessible from the detachable K680i magnetic keyboard.

To use this function, it is advisable to deactivate the system key **Directory** (system key: call by name).

8.7.2 OPERATION SEQUENCES

The sequence of operations used to configure this function is as follows:

- Preparing the configuration parameters (either by template file or by TMA)
- Taking the new configuration into account:
  - Restarting the terminal via TMA
  - Configuring in the terminal the login/password of the Outlook account (possibly testing the access to LDAP and Exchange servers from the terminal). This point must be carried out by the end user.
  - System key **Directory** to be disabled
  - System key **Pers. Ann.** to be renamed to Directory.

8.7.3 PROGRAMMING, VIA TMA, THE ACCESS TO THE LDAP DIRECTORY AND PERSONAL EXCHANGE CONTACTS FOR ALL MITEL 6800 AND 6900 IP PHONES

This operating mode allows you to automatically configure this function via TMA for all Mitel 6800 and 6900 IP Phones in the installation. All Mitel 6800 and 6900 IP phone models in the installation are affected.

If configuration file encryption is configured, the configuration files associated with this function are also encrypted by TMA.

The procedure for configuring this function via TMA is as follows:

- Via TMA, modify the distribution of the parameters to take into account the optional parameters present in the **Directory** tab. Refer to Section 6.15.5 to assign in the global range the configuration parameters used for this function.
- Via TMA, launch a manual global data update to update all Mitel 6800 and 6900 IP Phones with these new configuration parameters. Refer to Section 6.15.2 for the launching of this action.

At least the following parameters must be entered:

- **ldap server**: enter the IP address of the LDAP server (Mitel 5000 Gateways or MiVoice 5000 Server or MiVoice 5000 Manager).
- **ldap base dn** : leave either ou=local (case of a configuration without MiVoice 5000 Manager) or change the name (case of a configuration with MiVoice 5000 Manager) or=name of the multi-site configuration.

- **exchange server** : enter the IP address of the Exchange server or the name of the Exchange server (resolved by the DNS server).

Configure in the terminal the login/password of the Outlook account:

- Options key, then Identifiers menu.
- With the arrow >, go to the Microsoft Exchange menu and enter the Username / Password settings.
- To test access to LDAP and Microsoft Exchange servers, go via the arrow > to the Test connection menu. Tick LDAP and Microsoft Exchange and then press test. Check that the ticks are green. Restart the terminal to immediately take these changes into account (or wait for the automatic synchronisation mechanism at 00:30).

System key **Directory** to be disabled:

From the Mitel 5000 Gateways or MiVoice 5000 Server Web admin, Menu **Telephony Service>Subscribers>Terminals and Applications>6xxxi Keys.**

For the terminal models concerned, untick the system key **Directory** (system key: Call by name).

System key **Pers. Ann.** to be renamed to Directory:

From the Mitel 5000 Gateways or MiVoice 5000 Server Web admin, Menu **Telephony Service>Subscribers>Terminals and Applications>6xxxi Keys.**

For the terminal models concerned, untick the system key **Directory** (system key **Pers**. **Ann.** (system key: personal directory) and via the label field enter the new label **Directory.**

8.7.4 MANUALLY PROGRAMMING THE ACCESS TO THE LDAP DIRECTORY AND PERSONAL EXCHANGE CONTACTS FOR ONE OR MORE MITEL 6800 AND 6900 IP PHONE MODELS

This operating mode allows you to manually configure this function for one or more Mitel 6800 and 6900 IP Phone models in the installation. In this case, only some Mitel 6800 and 6900 IP phone models in the installation are configured to use this function.

The procedure for configuring this function on a specific Mitel 6800 and 6900 IP phone model is as follows:

- Retrieve from the deployment area of the 6800 and 6900 IP Phones or from the Mitel France Extranet (software part), the canonical configuration files named **68xxi_LDAP_outlook.cfg** (depending on the terminal model for which this function must be opened, xx=63 or 65 or 67 or 69 or 73).

Note : The canonical configuration files (model files) are available on the Mitel France Extranet.

Customise this (these) canonical configuration file(s).

Via the **deployment** function of TMA, place this/these previously customised configuration file(s) in the appropriate FTP area.

Restart the Mitel 6800 and 6900 IP phones to take this/these configuration file(s) into account.

The example below describes the implementation of this function for the **Mitel 6867 SIP Phone** model:

- Retrieve from the deployment area of the 6800 and 6900 IP Phones, the canonical configuration file named **6867i_LDAP_outlook.cfg:**

- Connect to the embedded download server via the **connexio/connexio** account and transfer the file **6867i_LDAP_outlook.cfg** to a workspace.

From this workspace, customise the canonical configuration file **6867i_LDAP_outlook.cfg** (section A of the file)**:**

- **ldap server**: enter the IP address of the LDAP server (Mitel 5000 Gateways or MiVoice 5000 Server or MiVoice 5000 Manager).
- **ldap base dn** : leave either ou=local (case of a configuration without MiVoice 5000 Manager) or change the name (case of a configuration with MiVoice 5000 Manager) or=name of the multi-site configuration.
- **exchange server** : enter the IP address of the Exchange server or the name of the Exchange server (resolved by the DNS server).

Section B of this file (optional data) contains the mapping between the attributes used by the terminal and the attributes used in the LDAP database of Mitel 5000 Gateways or MiVoice 5000 Server or MiVoice 5000 Manager. These are the most commonly used optional attributes. By default, they are all sin comment (#). In case you want to use the mobile number, for example, you will have to delete the # on the ldap mobile phone attribute list line: attr1 (attr1: 1st customisable field in the LDAP database among the 10 possible ones).

Section C of this file should not be modified except in specific cases.

By default, this file contains the following information:

#----------

Fichier template pour 6867i / Template file for 6867i

#

This template file contains the settings that allow 68xxi extensions to connect directly to the MV5000 LDAP directory and to personal Exchange contacts.

#

Part A (customer data) is to be adapted specifically to the client configuration.

#

Rename this file to 6867i.cfg, and use TMA to upload it to the download server.

##----------

A- Client data to be adapted during installation

#----------

######### MV5000 LDAP Directory #########

ldap enabled: 1

Enable access to the Ldap Directory

ldap name: Directory Company

Ldap Directory name displays on the phone.

ldap server: cn=i2052,ou=Users,dc=DOMAIN,dc=com:i2052@**<IP address-MV5000**>:389

Specifies the MV5000 IP address

ex: ldap server: cn=i2052,ou=Users,dc=DOMAIN,dc=com:i2052@192.168.100.1:389

ldap base dn: **ou=local,**o=AASTRA,dc=DOMAIN,dc=com

In case the LDAP is managed by a MV5000 Manager, modify the sub-folder "local" with the multisite name

######### Microsoft Exchange contacts #########

exchange contacts enabled: 1

Enable access to the Contact Exchange

exchange contacts name: Exchange Contacts

Exchange Directory name displays on the phone

exchange server: **<Exchange Server>**

Specifies the Microsoft Exchange server hostname or IP address

ex: exchange server: mail.company.com

#----------

B- Optional data to be adapted if necessary

#---

######### MV5000 LDAP Directory #########

#ldap job title attribute list: function

#ldap company attribute list: hierarchySV

#ldap mobile phone attribute list : attr1

#ldap other phone attribute list: secretary

#ldap business street attribute list: localisationDesc

#ldap business city attribute list:

#ldap business state attribute list:

#ldap business postal code attribute list:

#ldap business country attribute list:

#ldap business phone 2 attribute list : didNumber

#ldap business fax attribute list:

#ldap home street attribute list:

#ldap home city attribute list:

#ldap home state attribute list:

#ldap home postal code attribute list:

#ldap home country attribute list:

#ldap home phone 1 attribute list:

#ldap home phone 2 attribute list:

#ldap email 1 attribute list: mail

#ldap email 2 attribute list:

#ldap email 3 attribute list:

C- Generic data. Do not modify (except in specific cases)

#---

############### Direct access to the directory via the K680i keyboard #############

live keyboard: 1

keyboard script:

######### MV5000 LDAP Directory #########

ldap user name: cn=i2052,ou=Users,dc=DOMAIN,dc=com

ldap search filter: (&(displayName=%)(|(&(telephoneNumber=*)(objectclass=peoplerecord))(&(!(private=LR))(phoneNumber=*)(objectclass=contactrecord))))

ldap first name attribute list: displayGn

ldap last name attribute list: displayName

ldap business phone 1 attribute list: telephoneNumber,phoneNumber

ldap search scope: subtree

ldap resync time: 00:30

ldap resync max delay: 1380

directory digits match: 9

directory search dynamic threshold: 100

######### Microsoft Exchange contacts #########

exchange use ssl: 1

exchange path: ews/exchange.asmx

exchange contacts resync time: 00:30

exchange contacts resync max delay: 1380

#########

Rename the file **6867i_LDAP_outlook.cfg** previously modified to **6867i.cfg**.

Via the TMA **Deployment** function, place the file **6867i.cfg** in the appropriate FTP area (see Section 6.21.1).

Restart the Mitel 6800 or 6900 IP phones to take the configuration file **6867i.cfg** into account. Via TMA, launch a manual global data update to update the Mitel 6800 and 6867 IP Phones with this new configuration file. Refer to Section 6.15.2 for the launching of this action.

Configure in the terminal the login/password of the Outlook account:

Options key, then **Identifiers** menu.

With the arrow >, go to the **Microsoft Exchange**menu and enter the **Username / Password** settings.

To test access to LDAP and Microsoft Exchange servers, go via the arrow > to the **Test connection** menu. Tick **LDAP** and **Microsoft Exchange** and then press **test**. Check that the ticks are green. Restart the terminal to immediately take these changes into account (or wait for the automatic synchronisation mechanism at 00:30).

System key **Directory** to be disabled:

- From the Mitel 5000 Gateways or MiVoice 5000 Server Web admin, Menu Telephony Service>Subscribers>Terminals and Applications>6xxxi Keys.
- For the terminal models concerned, untick the system key Directory (system key: call by name).

- System key **Pers. Ann.** to be renamed to Directory:
- From the Mitel 5000 Gateways or MiVoice 5000 Server Web admin, Menu **Telephony Service>Subscribers>Terminals and Applications>6xxxi Keys.**

- For the terminal models concerned, untick the system key **Directory** (system key **Pers**. **Ann.** (system key: personal directory) and via the label field enter the new label **Directory.**

8.8 RESTORING THE FACTORY CONFIGURATION OF MITEL 6000 SIP PHONES

8.8.1 FROM THE TERMINAL

- Press the ‘Options’ key.
- In the parameter option list, select: ’Administrator Menu’ then press ’Select’.
- Enter the administrator password (22222) then press ’Enter’ to confirm.
- Select ‘Factory default’ then press ‘Select’.
- Press ‘Default’ then ‘Restart’ to restart the terminal.

8.8.2 FROM THE WEB INTERFACE

Procedure:

- Connect as Administrator.
- In Menu **Operation>Reset**, click **Remove** to delete the local configuration parameters.
- Then click **Restore** to reset the terminal with the default factory settings.
- The terminal must be restarted for the settings to become effective: click **Restart**.

8.9 NTP SERVER

Time is set on the terminals via an NTP server. The NTP server IP address must be configured in the general parameters (file **aastra.cfg**) or specific parameters (file **@MAC.cfg**) of the SIP terminals.

The NTP server address can also be negotiated with the DHCP server via option 42.

The NTP server, available by default on Mitel 5000 Gateways systems, may be used.

You will indicate in Menu **System>Info>Date and time** the address of an external NTP server. This configuration enables you to have the same reference time for the Mitel 5000 Gateways system as well as for Mitel 6000 SIP Phones and MiVoice 5300 IP Phones.

Example of NTP server: Absolute Time Server 2.2:

The server proposes by default UDP and TCP ports 37 as well as SNTP port 123. These fields can be redefined by the user. The SIP terminal uses SNTP port 123.

8.10 CONFIGURATION REQUIRED IN THE SYSTEM

8.10.1 DECLARING MITEL 6000 SIP PHONES IN THE SYSTEM

The use of Mitel 6000 SIP Phones is subject to a PROPRIETARY AUDIO license key code. The type of subscription to declare for Mitel 6000 SIP Phones is “Local Subscriber”.

Procedure:

- Go to the licence selection menu:

this menu (213) is accessible via **System>Info>Licences**.

- Enter the key code corresponding to the number of Mitel 6000 SIP Phones deployed on the client’s LAN.
- Create local subscribers:

this menu (121) is accessible via **Subscribers> Subscription>Creation**.

8.10.2 CONFIGURING THE ENCODING LAWS ASSOCIATED WITH MITEL 6000 SIP PHONES

Go to the encoding law selection menu:

This menu (441) is accessible via Networks and links>Quality of service>Voice over IP coding law.

Select a call type: INTERNAL.

Select a terminal type: SIP

Note : The SIP terminal type corresponds to Mitel 6000 SIP Phone and other commercially available functional SIP terminals.

Confirm by clicking "**Select item**". In the following menu, indicate the required encoding laws depending on the available bandwidth and the required voice quality.

Then check the application of the encoding laws:

Go to the encoding law display menu:

This menu (442) is accessible via **Networks and links>Quality of service>Display of the coding laws**.

8.11 CONFIGURING THE ETHERNET SWITCH

In accordance with the general recommendations for the MiVoice 5000 solution, a sub-division into VLAN must be used:

- A VLAN comprising PT2/IPS cards and the MiVoice 5000 Servers.
- One or more VLANs containing Mitel 6000 SIP Phones
- One VLAN containing telephony servers (messaging system, administration, etc.)
- One or more Data VLANs.

Standalone terminals:

TERMINAL CONFIGURATION (WEB INTERFACE/ AASTRA.CFG FORMAT)	CONFIGURING THE ETHERNET SWITCH
VLAN Enabled (no) / tagging enabled=0	The Ethernet switch port is in a "terminals" VLAN without 802.1Q marking.
VLAN Enabled (yes) / tagging enabled=1 Port 0 VLAN ID 20 / VLAN id: 20	The terminal and Ethernet switch mark the frames in 802.1Q in VLAN 20

Terminals with a PC:

TERMINAL CONFIGURATION (WEB INTERFACE/ AASTRA.CFG FORMAT)	CONFIGURING THE ETHERNET SWITCH
VLAN Enabled (yes) / tagging enabled=1 Port 0 VLAN ID 20 / VLAN id: 20 Port 1 VLAN ID 30 / VLAN id port 1: 30	The terminal and Ethernet switch mark the frames in 802.1Q in VLAN 20 The frames to the PC are marked in VLAN 30; it is the Mitel 6000 SIP Phone that manages the marking to the PC. Thanks to the use of VLAN 4095 on port 1, all unmarked frames can be sent to the PC port. This configuration is recommended because the DATA flow marking may not be compatible with certain routers.

8.12 QOS ON THE IP NETWORK

Mitel 6000 SIP Phones can mark ToIP frames according to their type (signalling, RTP, RTCP) on Level 2 (802.1Q) and on Level 3 (DiffServ).

They can also assign a level 2 priority to traffic from the connected PC.

Therefore, level 2 devices do not have to modify the marking of traffic from the Mitel 6000 SIP Phone, unless there is an inbound-traffic-analysis and traffic-remarking policy.

On level 3, you only have to activate DiffServ in the devices to take account of the ToIP frame marking.

The standard QoS recommendations are:

- Priority level 2 ToIP (signalling, RTP/RTCP)=6
- Priority level 2 Data=0
- Priority level 3 ToIP (RTP/RTCP flow)=B8h
- Priority level 3 ToIP (signalling flow)=A0h
- Priority level 3 Data=00h

8.13 TROUBLESHOOTING SOLUTIONS

8.13.1 WHY DOES MY MITEL 6000 SIP PHONE DISPLAY "APPLICATION MISSING"?

If you had some network problems while Mitel 6000 SIP Phone was downloading the firmware from the download server, it is possible that the telephone will no longer be able to recover the firmware. If Mitel 6000 SIP Phone is no longer able to communicate with the download server while trying to download the firmware, and if it cannot locate the firmware locally, the message "Application missing" is displayed.

Mitel 6000 SIP Phone then also displays the following text: "Recovery web-client at: <IP Address>".

The IP address displayed is the telephone IP address. If the telephone cannot receive an IP address from the DHCP server, or if it has lost its static IP address, it assigns itself the default IP address: 192.168.0.50.

To recover the firmware of your telephone under this circumstance, proceed as follows:

- Open the web browser on a PC located on the same network as the terminal.
- In the URL, type: "http:// <IP address>" (where IP address is the IP address displayed on the telephone). The browser opens the Mitel IP terminal firmware recovery page.
- Recover and copy the firmware corresponding to the terminal in the download server storage area, if necessary.
- Enter the download server IP address and name of the firmware corresponding to the terminal model.
- Click **Download firmware** and wait for the end of the download.

At the end of the terminal download, the default passwords are restored:

Admin: 22222, for Administrator access

User: ‘no password’, for user access.

ATTENTION : During the ‘recovery’ procedure and as long as it has not been reloaded by its configuration files, the terminal does not mark the frames in 802.1Q (VLAN number). It may be necessary, for instance if the terminal is connected to a PC and uses 802.1Q marking, to temporarily move it to an IP network port in ‘access’ mode.

ATTENTION : In recovery mode, the terminal no longer has a default router address: the PC and download server must be on the same IP network as the terminal.

8.13.2 WHY DOES MY MITEL 6000 SIP PHONE DISPLAY "NO SERVICE"?

The telephone displays "No Service", among others, if the SIP parameters have not be correctly defined. If the IP address of the parameter “Server Registrar” is not entered correctly, the terminal will not be able to register with the MiVoice 5000 Server or Mitel 5000 Gateways platform’s SIP access point and will display “No Service”.

The following points must be checked:

- Check from the terminal’s web user interface, in Menu "Advanced parameters >General SIP", that the parameter “Server Registrar” is correct.
- Check in the configuration files that the parameter "sip registrar ip" is correct.
- Check that the terminal's subscription has been created: Menu **Subscribers>Subscriptions>Characteristics>General characteristics**.
- Check that the SIP service has started correctly: Menu **System>Configuration>Services**.

8.13.3 WHY DOES MY MITEL 6000 SIP PHONE NOT RECEIVE THE DOWNLOAD SERVER IP FROM THE DHCP SERVER?

To assign Mitel 6000 SIP Phone the download server IP address to use, the DHCP server must be configured to negotiate with Mitel 6000 SIP Phone:

- Either standard option 66
- Or option 43 (vendor specific)

ATTENTION : If both options are traded simultaneously, Mitel 6000 SIP Phone will give priority to option 43 over option 66. Option 43 is managed in release 2.1.2 and later.

Check that these two option are configured on the DHCP server, specifying:

- The protocol to use
- The password associated with the download server storage directory.
- The download server IP address.

For a network architecture with several VLAN and/or several subnets, check that the router configuration allows the transmission of the broadcast frames sent by the terminal to the DHCP server using the DHCP RELAY information.