TA7102i, Software Configuration Guide

Dgw v2.0 Application TA7102i, Software Configuration Guide

Document ID: 154/1531 ANF 901 Uen A 2014-01-30

Third-Party Software Copyright Information

The Dgw v2.0 Application firmware aggregates some third-party software modules (open source and commercial) that are distributed to you in accordance with their respective licenses. Refer to the *Third Party Software Copyright Information* addendum, which lists the third-party software modules along with any copyright and license information.

PREFACE

P

About this Manual

Document Objectives

The Dgw v2.0 application *Software Configuration Guide* provides technical information on how to configure and operate the application for your Aastra unit.

Use the Dgw v2.0 application *Software Configuration Guide* in conjunction with the appropriate publications listed in "Related Documentation" on page iii.

Any reference to gateway unit 4102S does relate to terminal adapter TA7102i.

Intended Audience

This Software Configuration Guide is intended for the following users:

- System administrators who are responsible for installing and configuring networking equipment and who are familiar with the Aastra unit.
- System administrators with a basic networking background and experience, but who might not be familiar with the Aastra unit.
- Operators.
- Installers.
- Maintenance technicians.

Related Documentation

In addition to this manual, the Aastra unit document set includes the following:

- Model-Specific *Hardware Installation Guide*

  Describes how to install the hardware of your specific Aastra unit.

  This booklet allows you to quickly setup and work with the Aastra unit.

  Lists all the parameters, tables, and commands available in the Dgw v2.0 application.

  Lists and describes all syslog messages and notification messages that the Dgw v2.0 application may send.
- *Third Party Software Copyright Information (please contact your Aastra representative for detailed information if needed.*

  This document lists the third-party software modules used in the Aastra unit along with any copyright and license information.

Be sure to read any readme files, technical bulletins, or additional release notes for important information.

Document Structure

The Dgw v2.0 application *Software Configuration Guide* contains the following information.

Table 1: Software Configuration Guide Chapter/Appendices

Title	Summary
“Chapter 1 - System Overview” on page 1	Provides an overview of the Dgw v2.0 application as well as the units that support it.
“Chapter 2 - Command Line Interface (CLI)” on page 11	Describes how to access the CLI environment in order to perform configuration tasks.
“Chapter 3 - Web Interface Configuration” on page 33	Describes how to access the embedded web server of the Aastra unit.
System Parameters	
“Chapter 4 - Services” on page 43	Describes how to view and start/stop system and network parameters.
“Chapter 5 - Hardware Parameters” on page 49	Describes the hardware installed on your Aastra unit.
“Chapter 6 - Endpoints Configuration” on page 53	Describes how to set the administrative state of the Aastra unit endpoints.
“Chapter 7 - Syslog Configuration” on page 57	Describes how the Aastra unit handles syslog messages and notification messages.
“Chapter 8 - Events Configuration” on page 63	Describes how to associate a NOTIFICATION message and how to send it (via syslog or via a SIP NOTIFY packet).
Network Parameters	
“Chapter 10 - IPv4 vs. IPv6” on page 71	This chapter describes the differences between IPv4 and IPv6 addressing.
“Chapter 11 - Host Parameters” on page 75	Describes how to set the host information used by the Aastra unit, as well as the default gateway, DNS servers and SNTP servers configuration source.
“Chapter 12 - Interface Parameters” on page 85	Describes how to set the interfaces of the Aastra unit.
“Chapter 13 - VLAN Parameters” on page 99	Describes how to create and manage dynamic VLANs.
“Chapter 14 - Local QoS (Quality of Service) Configuration” on page 101	Describes how to configure packets tagging sent from the Aastra unit.
“Chapter 15 - Local Firewall Configuration” on page 107	Describes how to configure the local firewall feature.
“Chapter 16 - IP Routing Configuration” on page 113	Describes how to configure the unit's IP routing parameters.
“Chapter 17 - Network Firewall Configuration” on page 121	Describes how to configure the network firewall parameters.
“Chapter 18 - NAT Configuration” on page 127	Describes the configuration parameters to define the Aastra unit´s NAT.

Table 1: Software Configuration Guide Chapter/Appendices (Continued)

Table 1: Software Configuration Guide Chapter/Appendices (Continued)

Document Conventions

The following information provides an explanation of the symbols that appear on the Aastra unit and in the documentation for the product.

Warning Definition

Warning: Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

Where to find Translated Warning Definition

For safety and warning information, refer to Appendix A - “Standards Compliance and Safety Information” in the Aastra unit *Hardware Installation Guide*. This Appendix describes the international agency compliance and safety information for the Aastra unit. It also includes a translation of the safety warning listed in the previous section.

Other Conventions

The following are other conventions you will encounter in this manual.

Caution: Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury and/or damage to the equipment or property.

Note: Indicates important information about the current topic.

Standards Supported	Indicates which RFC, Draft or other standard document is supported for a specific feature.

SCN vs. PSTN

In Aastra and other vendor’s documentation, the terms SCN and PSTN are used. A SCN (Switched Circuit Network) is a general term to designate a communication network in which any user may be connected to any other user through the use of message, circuit, or packet switching and control devices. The Public Switched Telephone Network (PSTN) or a Private Branch eXchange (PBX) are examples of SCNs.

Standards Supported

When available, this document lists the standards onto which features are based. These standards may be RFCs (Request for Comments), Internet-Drafts, or other standard documents.

The Dgw v2.0 application’s implementations are ***based*** on the standards, so it’s possible that some behaviour differs from the official standards.

For more information on and a list of RFCs and Internet-Drafts, refer to the IETF web site at http://www.ietf.org.

CHAPTER 1

System Overview

This chapter provides an overview of the Aastra devices supported by the Dgw v2.0 application:

- Introduction to the Aastra devices and the models available.
- Description of the various ways to manage the Aastra unit.
- How to use the DEFAULT/RESET button (partial reset and factory reset procedures).
- How to configure user access to the Aastra unit.

Introduction

The Aastra unit integrates features such as TLS, SRTP, and HTTPS designed to bring enhanced security for network management, SIP signalling and media transmission aspects.

The following describes the devices that the application supports.

TA7102i

The Aastra TA7102i is a standalone Internet telephony access device that connects to virtually any business telephone system supporting standard analog lines.

Key Features

The following are the key features offered by the various models available.

Table 2: Aastra Units Key Features

Feature	
IP connectivity for analog phones and faxes	✓
Number of simultaneous calls	up to 24
FXS interface ports	✓
HTTP, SNMP, FTP and TFTP for configuration and management	✓
True Plug-and-Play	✓
Automatic configuration script download	✓
Call Routing service	✓
Secure SIP signalling	✓
Secure Media transmission	✓
SNMPv3 and web management	✓
DHCP Client	✓
PPPoE Client	✓

Table 2: Aastra Units Key Features (Continued)

Feature	
T.38 support	✓
Command Line Interface (CLI)	✓
SSL/TLS Encryption	✓
60 VRMS ringing voltage, 2 kilometres loop distance .	✓

DSP Limitation

The Aastra unit models currently suffer from local limitation of their DSPs. When using a codec other than G.711, enabling Secure RTP (SRTP) and/or using conferences has an impact on the Aastra unit's overall performance as SRTP and conferences require CPU power. This means there is a limitation on the lines that can be used simultaneously, depending on the codecs enabled and SRTP. This could mean that a user picking up a telephone on these models may not have a dial tone due to lack of resources in order to not affect the quality of ongoing calls.

The DSPs offer channels as resources to the Aastra unit. The Aastra unit is limited to two conferences per DSP. See "Conference" on page 305 for more details on Conference limitations.

Howerver, as recomendation is to use the conference service in the call server this would normally not cause any problem. Please note that:

- One FXS line requires one channel.
- There is a maximum of 2 conferences per DSP
- Each conference requires one additional channel

In the following tables, compressed RTP refers to codecs other than G.711. Numbers in **Bold** indicate a possible under-capacity.

TA7102i

Table 3 describes the TA7102 processing capacity.

Table 3: TA7102i Offered Channels vs. Processing Capacity

Model	Offered Chanels		Processing Capacity			
	Phys. Channels	3-way Conf. Channels	G.711 RTP Channels	Compr. RTP Channels	G.711 SRTP Channels	Compr. SRTP Channels
TA7102i	2	2	4	4	4	4

Management Choices

The Aastra unit offers various management options to configure the unit.

Figure 1: Management Interfaces

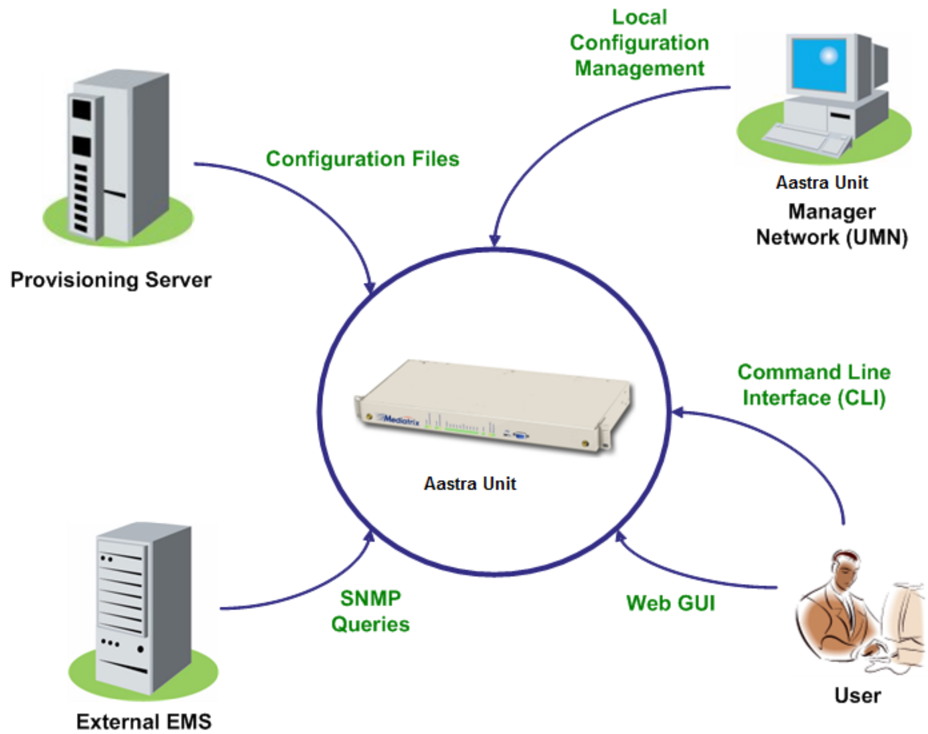


Table 4: Management Options

Management Choice	Description	Features
Web GUI	The Aastra unit web interface offers the following options: • Password-protected access via basic HTTP authentication, as described in RFC 2617 • User-friendly GUI	The Aastra unit web interface allows you to configure the following information: • Network attributes • SIP parameters • VoIP settings • Management settings such as configuration scripts, restore / backup, etc.
SNMPv1/2/3	The Aastra unit SNMP feature offers the following options: • Password-protected access • Remote management • Simultaneous management Refer to "Chapter 44 - SNMP Configuration" on page 437 for more details.	The Aastra unit SNMP feature allows you to configure all the MIB services.

Table 4: Management Options (Continued)

Management Choice	Description	Features
Command Line Interface (CLI)	The Aastra unit uses a proprietary CLI to configure all the unit's parameters.	The Aastra unit CLI feature allows you to configure all the MIB services.
Unit Manager Network	The Unit Manager Network (UMN) is a PC-Windows based element management system designed to facilitate the deployment, configuration and provisioning of Aastra access devices gateways. The UMN enables the simple and remote configuration and deployment of numerous Aastra units.	The UMN offers the following: • Auto-discovery • Group provisioning • SNMP access and remote management.

RESET/DEFAULT Button

The *RESET/DEFAULT* button allows you to:

- Cancel an action that was started.
- Revert to known factory settings if the Aastra unit refuses to work properly for any reason or the connection to the network is lost.
- Reconfigure a unit.

At Run-Time

You can use the *RESET/DEFAULT* button at run-time – you can press the button while the Aastra unit is running without powering the unit off. Table 5 describes the actions you can perform in this case.

Table 5: RESET/DEFAULT Button Interaction

RESET/ DEFAULT Button Pressed for:	Action	Comments	LEDs Pattern
2 to 6 seconds	Restarts the Aastra unit	No changes are made to the Aastra unit settings.	*Power* LED: • blinking, 1Hz, 50% duty All other LEDs: • OFF
7 to 11 seconds	Sets the Aastra unit in Partial Reset Mode	Sets some of the Aastra unit configuration to pre-determined values.	All LEDs • blinking, 1Hz, 50% duty
12 to 16 seconds	Restarts the Aastra unit in Factory Reset	Deletes the persistent configuration values, creates a new configuration file with the default factory values, and then restarts the unit.	All LEDs • steady ON
17 seconds and more	No action is taken	The RESET/DEFAULT button pressed event is ignored.	N/A

At Start-Time

You can use the *RESET/DEFAULT* button at start-time – you power the unit off, and then depress the button until the LEDs stop blinking and remain ON. This applies the “Factory Reset” procedure (see “Factory Reset” on page 7). This feature reverts the Aastra unit back to its default factory settings.

Partial Reset

The Partial reset provides a way to contact the Aastra unit in a known and static state while keeping most of the configuration unchanged.

Following a partial reset, the Aastra unit management interface is set to the *Rescue* interface. The default IPv4 address for this interface is 192.168.0.1/24 and has its corresponding link-local IPv6 available and printed on the sticker under the Aastra unit (see "Chapter 10 - IPv4 vs. IPv6" on page 71 for more details). Any existing network interface that conflicts with the *Rescue* interface address is disabled.

You can contact the Aastra unit this address to access its configuration parameters. It is not advised to access the unit on a regular basis through the *Rescue* network interface. You should reconfigure the unit's network interfaces as soon as possible in order to access it through another interface.

In a partial reset, the following services and parameters are also affected:

- AAA service: User(s) from profile are restored with their factory password.
- SNMP service: Resets the *enableSnmpV1*, *enableSnmpV2*, *enableSnmpV3* and *snmpPort* values to their default values.
- WEB service: Resets the *serverPort* to its default value.
- CLI service: The CLI variables revert back to their default value.
- NAT service: The configuration is rolled back if it was being modified. A new rule is then automatically applied in the source and in the destination NAT tables to prevent incorrect rules from blocking access to the unit. If those rules are not the first priority, they are raised. If there are no rules in the tables, the new rules are not added since there are no rules to override.
- LFW service: When a partial reset is triggered and the firewall is enabled, the configuration is rolled back if it was being modified. A new rule is then automatically applied in the firewall to allow access to the 'Rescue' interface. However, if the firewall is disabled, the configuration is rolled back but no rule is added.
- HOC service: The Management Interface reverts back to its default value.
- BNI service: The Rescue interface is configured and enabled with:
  - its hidden IPv4 link configuration values
  - its hidden IPv4 address configuration
  - an IPv6 link-local address on all network links

  Hidden values are set by the unit's profile.

  Just before the Rescue is configured, all IPv4 network interfaces that could possibly conflict with the Rescue interface are disabled.

  If the BNI Service is stopped when the partial reset occurs, it is started and the above configuration is applied.

To trigger the Partial Reset:

1. Insert a small, unbent paper clip into the *RESET/DEFAULT* hole located at the rear of the Aastra unit. While pressing the *RESET/DEFAULT* button, restart the unit.

   Do not depress before all the LEDs start blinking (between 7-11 seconds).
2. Release the paper clip.

   This procedure can also be performed at run-time.

Disabling the Partial Reset

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

You can disable the partial reset procedure, even if users depress the *Reset/Default* button. The following parameters are supported:

Table 6: Partial Reset Parameters

Parameter	Description
All	All the actions are allowed: reset, partial reset and factory reset.
DisablePartialReset	All actions are allowed ***except*** the partial reset.

- The reset action restarts the unit.
- The partial reset action provides a way to contact the unit in a known and static state while keeping most of the configuration unchanged.
- The factory reset action reverts the unit back to its default factory settings.

▶ **To change the partial reset behaviour:**

1. In the *hardwareMIB*, set the `ResetButtonManagement` variable to the proper behaviour.

   You can also use the following line in the CLI or a configuration script:

   `hardwareMIB.ResetButtonManagement="Value"`

   where:

   - *Value* may be as follows:

Table 7: Partial Reset Values

Value	Meaning
100	All
200	DisablePartialReset

Factory Reset

The Factory reset reverts the Aastra unit back to its default factory settings. It deletes the persistent MIB values of the unit, including:

- The firmware pack download configuration files.
- The SNMP configuration, including the SNMPv3 passwords and users.
- The PPPoE configuration, including the PPP user names and passwords.

The Factory reset creates a new configuration file with the default factory values. It should be performed with the Aastra unit connected to a network with access to a DHCP server. If the unit cannot find a DHCP server, it sends requests indefinitely.

The following procedure requires that you have physical access to the Aastra unit. However, you can also trigger a factory reset remotely:

- via the web interface of the Aastra unit. See “Firmware Packs Configuration” on page 425 for more details.
- via the Command Line Interface of the Aastra unit by using the `fpu.defaultsetting` command.

▶ **To trigger the Factory Reset:**

1. Power the Aastra unit off.
2. Insert a small, unbent paper clip into the *RESET/DEFAULT* hole located at the rear of the Aastra unit. While pressing the *RESET/DEFAULT* button, restart the unit.

   Do not depress before the LEDs stop blinking and are steadily ON. This could take up to 30 seconds.
3. Release the paper clip.

   The Aastra unit restarts.

This procedure resets all variables in the MIB modules to their default value.

When the Aastra unit has finished its provisioning sequence, it is ready to be used with a DHCP-provided IP address and MIB parameters.

This procedure can also be performed at run-time.

> **Note:** The Factory reset alters any persistent configuration data of the Aastra unit.

User Access

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

The following describes how to configure user access to the Aastra unit. The access information is available for the SNMP and Web interface management methods.

> **Note:** Currently, the user name cannot be modified. To access the unit via SNMPv1, you must use the user name as being the "community name" and there must be no password for this user name.

To configure the Aastra unit user access:

1. In the *aaaMIB*, set the password associated with the user name in the `usersPassword` variable.

   You can also use the following line in the CLI or a configuration script:

   `aaa.users.Password[UserName="User_Name"]="Value"`

   Only the "admin" and "public" user names are available for the moment.

2. Set the user name that is used for scheduled tasks in the `batchUser` variable.

   You can also use the following line in the CLI or a configuration script:

   `aaa.batchUser="Value"`

   For instance, if you are using an automatic configuration update everyday at midnight, the relevant service will use the "batchUser" user to execute the request.

Secure Password Policies

It is possible to validate a password against some password policies to be considered as valid. These policies may only be activated via customized profiles created by Aastra. The available policies are:

Table 8: Secure Password Policies

Policy	Description
Minimum Length of User Password	The minimum length the user password must have to be considered as valid.
Upper and Lower Case Required on User Password	Indicates if the user password is required to contain an upper and a lower case characters to be considered as valid. Here is an example of a valid password : 'Password' and examples of invalid passwords : '1234', 'password', '1password', 1PASSWORD.
Numeral character Required on User Password	Indicates if the user password is required to contain a numeral character to be considered as valid. Here is an example of a valid password : '1password2' and examples of invalid passwords : 'password', 'Password'.

Table 8: Secure Password Policies (Continued)

Policy	Description
Special character Required on User Password	Indicates if the user password is required to contain a special character to be considered as valid. Here is an example of a valid passwords : 'pass$word', 'pass_word#' and examples of invalid passwords : 'password', 'Password', '1234', '1Password'.

For more information on how to get a customized user profile, please refer to your Aastra representative.

Partial Reset

AAA service: User(s) from profile are restored with their factory password.

Where to Go From Here

The current manual offers reference information on the features that the Aastra unit supports.

- If you plan on using the web interface configuration.
- If you plan on using the CLI configuration.
- If you plan on using the SNMP configuration, go to “Chapter 44 - SNMP Configuration” on page 437

“Appendix B - Scripting Language” on page 477 also offers a few configuration samples that can be pasted or typed into the CLI or downloaded into the Aastra unit via the Configuration Script feature.

CHAPTER
2
Command Line Interface (CLI)

This chapter describes how to access the CLI environment in order to perform configuration tasks.

Introduction

You can configure the Aastra unit parameters through a proprietary Command Line Interface (CLI) environment. It allows you to configure the unit parameters by Aastra, Telnet or SSH.

The CLI uses the Aastra proprietary scripting language as described in "Appendix B - Scripting Language" on page 477.

Configuring the CLI

You must configure the CLI access. This can be done via the MIB variables. Once you have access to the CLI, you can also use it to configure the access.

▶ **To configure the CLI access:**

1. In the *cliMIB*, set the inactivity expiration delay for exiting the CLI session in the `inactivityTimeOut` variable.

   If there is no activity during the delay defined, the CLI session is closed. This value is expressed in minutes.

2. Enable remote Telnet access if applicable by setting the `EnableTelnet` variable to **Enable**.

   By default, Telnet is not enabled.

3. Set the port on which the Telnet service should listen for incoming Telnet requests in the `IpPort`. variable.

4. Enable remote SSH access if applicable by setting the `EnableSsh` variable to **Enable**.

5. Set the port on which the SSH service should listen for incoming SSH requests in the `IpPort`. variable.

The configuration is loaded when it is started. It configures and starts Telnet and SSH according to the options offered through the configuration variables. The configuration can be updated by the CLI service while running.

Partial Reset

When a partial reset is triggered, the CLI variables revert back to their default value.

Accessing the CLI

You can access the CLI a Telnet or SSH session.

Only one session at a time is allowed. These sections describe how to access the CLI:

- "Accessing the CLI via a Telnet Session" on page 12
  - "Opening a Telnet Session with the Unit Manager Network" on page 12
- "Accessing the CLI via a SSH Session" on page 13

Which method you choose depends primarily on your preference and level of experience with one or all of the options provided. None precludes using other configuration methods. Note that after performing a factory reset or a firmware update, accessing the CLI may take up to one minute, even if the web and SNMP interfaces are already accessible.

Note: When performing a partial reset, the root password is removed. See "Partial Reset" on page 6 for more details.

Accessing the CLI via a Telnet Session

Standards Supported	• RFC 854: Telnet Protocol Specification

Connecting via Telnet requires a computer with a Telnet remote client running on a PC that acts as a Telnet host. The Telnet host accesses the Aastra unit via its LAN or WAN network interface.

▶ **To access the CLI from a remote host using Telnet:**

1. Set up the Aastra unit as described in the *Hardware Installation Guide*.

2. Power on your Aastra unit. Wait 60 seconds before proceeding to the next step.

3. Open a Telnet session to the Aastra unit by using one of the following IP addresses:

- obtained dynamically from the DHCP server
- you have configured statically
- after performing a partial reset (192.168.0.1)
- the link-local IPv6 available and printed on the sticker under the Aastra unit (see "Chapter 10 - IPv4 vs. IPv6" on page 71 for more details)

If you are using a Telnet port other than 23, (as configured in "Configuring the CLI" on page 11) you must also specify it.

4. When prompted for a login, type the following:

`public`

Do not type a password, just press <Enter>. After you successfully connect to the Aastra unit by using Telnet, you can start using the CLI to configure the unit.

Opening a Telnet Session with the Unit Manager Network

You can use the Aastra Unit Manager Network (UMN) product to launch a Telnet client session to configure the parameters of the Aastra unit. You can define which Telnet client to use in the UMN.

The Telnet session is opened from the PC where the client application is installed. It thus establishes a direct connection to the unit. This could cause some problems if the client PC cannot directly access the unit because of firewall restrictions, etc.

▶ **To open a Telnet session via UMN:**

1. In the UMN, autodetect the Aastra unit at one of the IP addresses listed in "Accessing the CLI via a Telnet Session" on page 12.

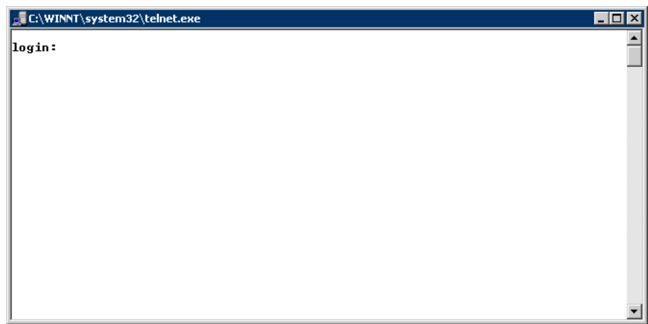
   Refer to the *Unit Manager Network Administration Manual* for more details on how to perform this task.

2. Right-click the unit for which to open a Telnet session.

3. Select the *Open Telnet Session* option in the context sensitive menu that opens.

   The following window opens:

Figure 2: Telnet Session Login



This window may differ if you are not using the default Windows Telnet client.

Accessing the CLI via a SSH Session

Standards Supported	• RFC 4251: The Secure Shell (SSH) Protocol Architecture

Connecting via a Secure Socket Shell (SSH) session requires a computer with a SSH or OpenSSH compatible remote shell client running on a PC that acts as a SSH host. All communication between a client and server is encrypted before being sent over the network, thus packet sniffers are unable to extract user names, passwords, and other potentially sensitive data.

▶ **To access the CLI from a remote host using SSH:**

1. Set up the Aastra unit as described in the *Hardware Installation Guide*.

2. Power on your Aastra unit. Wait 60 seconds before proceeding to the next step.

3. Open a SSH session to the Aastra unit by using one of the following IP addresses:

   - obtained dynamically from the DHCP server
   - you have configured statically
   - after performing a partial reset (192.168.0.1)

   If you are using a SSH port other than 22, (as configured in "Configuring the CLI" on page 11) you must also specify it.

4. When prompted for a login, type the following:

   `public`

   Do not type a password, just press <Enter>. If you are accessing the unit through the CLI for the first time or after a factory reset, you may be presented with a warning message regarding the unit's identification. You can accept the message and continue.

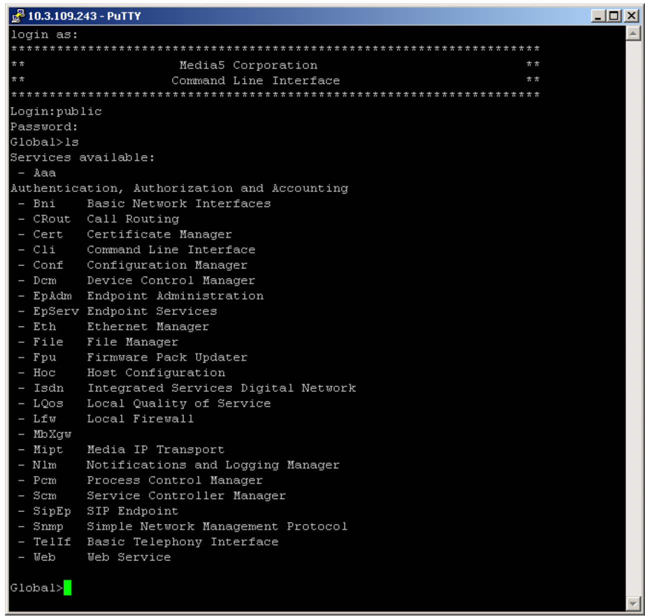
   After you successfully connect to the Aastra unit by using Telnet, you can start using the CLI to configure the Aastra unit.

Working in the CLI

The command interpreter interface of the CLI is a program called by the Telnet or SSH client.

It allows you to browse the parameters of the unit. It also allows you to write the command lines and the CLI interprets and executes it. The following figure illustrates the CLI in the global context after preforming a `ls` command:

Figure 3: CLI Global Context



Contexts

The CLI has various contexts. A context is defined as a service name indicated by its textual key (for instance, the *Conf* service). Upon entering the CLI, you are located in the *Global* context. This is indicated by the following prompt:

```
Global>
```

You can change context by using the `cd` (change directory) command with the following syntax:

```
cd Service_Name
```

This allows you to enter into a service context. You can thus execute commands without writing the service name. For instance:

```
Global>cd Conf
```

The prompt then changes to:

```
Conf>
```

You can use the following to get back to the global context:

```
Conf>cd
```

You can also access another service context from the Conf context:

```
Conf>cd Bni
```

Executing a command is different depending on if you are in the global context or a service context. See “commands” on page 20 for examples.

Exiting from the CLI

To exit the CLI, type the `exit` command from the global context or any of the service contexts.

Command Completion

The CLI command completion function works on everything in the CLI including aliases, macros, commands, names, etc. It is case insensitive, which means that typing `interface` is the same as typing `Interface`. However, names that are unique are case sensitive, such as interface names.

To display all possible commands or statements, enter at least one character and press the *Tab* key to complete the command line. If more than one possibility exists, they are listed and you can select the one you want.

Let's say for instance that you type the following command in the Bni context:

```
Bni>Net[+ Tab key]
```

The CLI displays the following choices:

```
NetworkInterfaces        NetworkInterfacesStatus
Bni>NetworkInterfaces
```

Macros

Macros are internal hardcoded commands that are frequently used. The CLI currently supports the following macros:

Table 9: Macros

Macro	Description
Reboot	Reboots the unit.
Restart	Restarts the services when in a service context or restarts the unit in the global context. For instance: `Global>Mipt.Restart`

You can see the list of available macros by typing the following command from anywhere in the CLI:

```
Conf.Macros
```

This will return a table similar to the following:

```
 ______________________________
| Name      | Description       |
|___________|___________________|
| Reboot    | Reboot unit       |
| Restart   | Restart service   |
|___________|___________________|
```

History

You can recall the history commands and navigate through the history using the up and down arrows.

Services Restart

Whenever you perform changes in the configuration, this usually means that you must restart a service for the changes to take effect. When this is the case, the following message appears in the CLI:

```
Need Restart
```

Use the `Restart` macro as described in "Macros" on page 15.

Syslog Messages

You can access the notifications, diagnostic traces and SIP signalling logs of the Aastra unit. Use the `logs on` command to display Syslog traces as soon as they are sent. Use the `logs off` command to stop displaying the logs.

Configuring the Aastra unit with the CLI

Once you are in the CLI, you can configure all the parameters of the Aastra unit with the various keywords available. These keywords are described in "List of Commands / Keywords" on page 18. You must however have a good understanding of the parameters structure

A good way of working with the CLI is to create the complete configuration in a text file, then copy and paste chunks of the configuration in the CLI. This avoids to type all the commands in the CLI itself. However, be aware that you must not copy configuration when a service needs to be restarted. You must first restart the service before continuing.

Let's say for instance you are in the *Global* context and you want to see the inactivity timeout value of the CLI. Type the following:

```
Global>get Cli.InactivityTimeOut
```

The CLI displays the current value. If you want to change this value to 10 minutes, type the following:

```
Global>set Cli.InactivityTimeOut=10
```

Refer to "Appendix B - Scripting Language" on page 477 for samples of configurations you can use in the CLI. The samples include the configuration required to perform a basic call between an ISDN telephone and an analog telephone. These samples may also be used in configuration scripts that you can download into the Aastra unit.

Current Unit Status

The current unit status is displayed every time a user is authenticated by the CLI. You can also display the same information during a session by executing the `sysinfo` command. The information displayed is:

- System Description
- Serial Number
- Firmware Version
- Host Name
- Mac Address
- System Uptime
- System Time
- Snmp Port
- Installed Hardware Information (Name, description, location).

Welcome Message

You can define a message that is displayed when connecting to the CLI by typing the following:

```
Global>set Cli.WelcomeMessage=Value
```

Where `Value` is the actual message you want displayed. The following escape characters are supported:

- \n for new line
- \t for tab
- \\ for the \ character.

Other characters are left unchanged.

Help

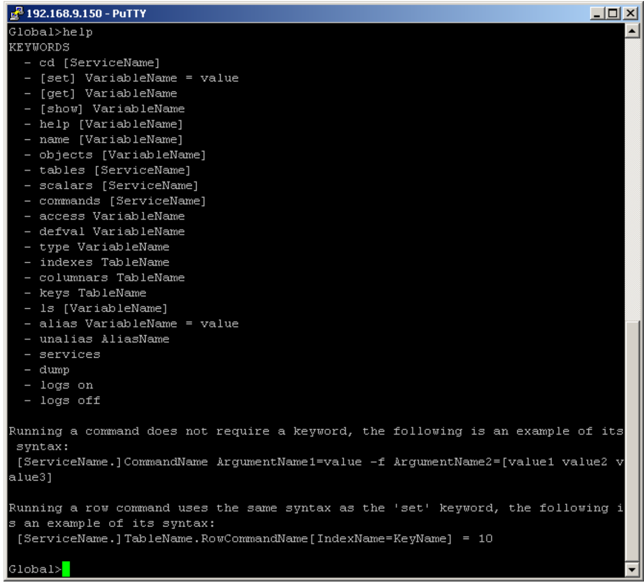
The CLI allows you to get help on the various keywords supported. You can have access to general or contextual help.

You can access the general help by typing the `help` keyword:

```
Global>help
```

In that case, the CLI displays the list of all keywords available.

Figure 4: CLI Global Help

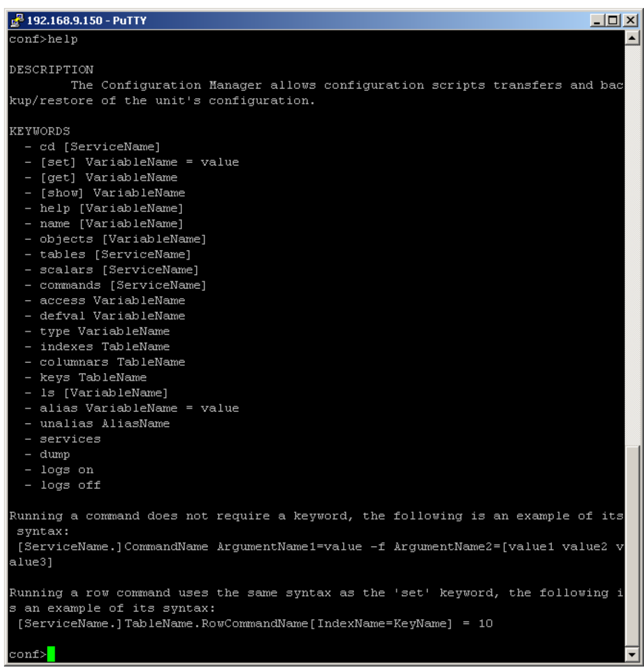


You can also access a more specific general help by typing the `help` keyword in a context.

`Conf>`**`help`**

In that case, the CLI displays the list of all keywords available as well as a description of the context.

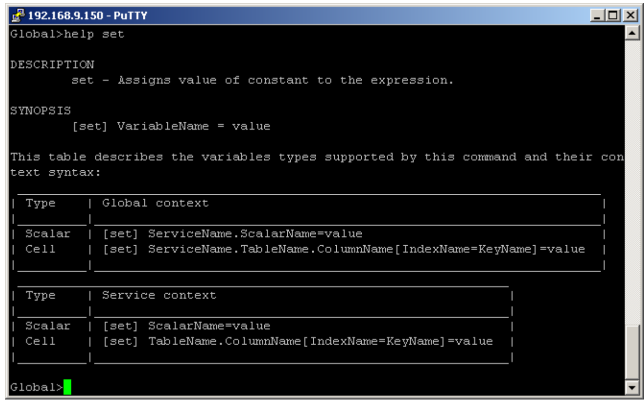
Figure 5: CLI Global Help Variation



You can access the contextual help by typing the `help` keyword followed by the keyword.

`Global>`**`help set`**

Figure 6: CLI Contextual Help

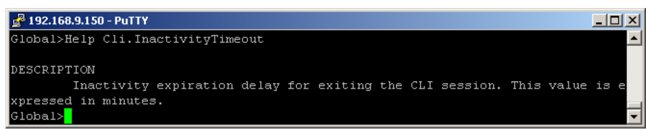


See “List of Commands / Keywords” on page 18 for a list of keywords available.

Finally, you can access a more specific contextual help by typing the `help` keyword followed by the name of the expression (scalar, table, command, column, service).

`Global>`**`help Cli.InactivityTimeOut`**

Figure 7: CLI Expression Help



List of Commands / Keywords

The following sections describe the commands and keywords and their syntax depending on the context in which you are located. Each syntax also has an example in *blue*.

access

Retrieves the `access` type of the expression. The expression may be a variable (scalar), a table cell, or a table column.

Applies To			
Services	Tables	Columns	Variables
		✓	✓

Variables – Global Context

Use this syntax when in the global context.

```
access Service_Name.Scalar_Name
```
access Cli.InactivityTimeOut

Variables – Service Contexts

Use this syntax when in a service context.

```
access Scalar_Name
```
access InactivityTimeOut

Table Cell or Column Properties – Global Context

Use this syntax when in the global context. The `Index` parameter is the first column of the table.

```
access Service_Name.Table_Name[Index=key].Column_Name
```
access Hoc.DnsServersInfo[Priority=2].IpAddress

```
access Service_Name.Table_Name.Column_Name
```

access Hoc.DnsServersInfo.IpAddress

Table Cell or Column Properties – Service Contexts

Use this syntax when in a service context. The `Index` parameter is the first column of the table.

```
access Table_Name[Index=key].Column_Name
access DnsServersInfo[Priority=2].IpAddress

access Table_Name.Column_Name
access DnsServersInfo.IpAddress
```

alias / unalias

The alias function allows you to create a keyboard shortcut, an abbreviation, a mean of avoiding typing a long command sequence. You can assign an alias to services, scalars, tables, and commands. You cannot currently assign an alias to columns.

Once an alias has been added, you can use it in place of the entity name when typing commands. You can delete an alias with the `unalias` command.

Applies To			
Services	Tables	Columns	Variables
✓	✓	✓	✓

Note: When naming an alias, you cannot use an existing macro name, service name, nor MIB object name from the same context.

You can see the list of available aliases by typing the following command from anywhere in the CLI:

```
Conf.Alias
```

This will return a table similar to the following:

Name	Entity	Type	Context
TimeOut	InactivityTimeOut	200	Cli

Variables – Global Context

Use this syntax when in the global context.

```
alias Service_Name.Scalar_Name=aliasName
alias Cli.InactivityTimeOut=timeout
unalias aliasName
unalias timeout
```

Variables – Service Contexts

Use this syntax when in a service context.

```
alias Scalar_Name = aliasName
alias InactivityTimeOut=timeout
unalias aliasName
unalias timeout
```

Tables or Columns – Global Context

Use this syntax when in the global context.

```
alias Service_Name.Table_Name=aliasName
alias Hoc.DnsServersInfo.IpAddress
alias Service_Name.Table_Name.Column_Name=aliasName
alias Hoc.DnsServersInfo.IpAddress = IPAddress

unalias aliasName
unalias IPAddress
```

Tables or Columns – Service Contexts

Use this syntax when in a service context.

```
alias Table_Name = aliasName
alias DnsServersInfo.IpAddress
alias Table_Name.Column_Name=aliasName
alias DnsServersInfo.IpAddress=IPAddress

unalias aliasName
unalias IPAddress
```

cd

Changes context (global or service context).

Applies To			
Services	Tables	Columns	Variables
✓			

Enter into a Context – Global Context

Use this syntax when in the global context.

```
cd Service_Name
cd Hoc
```

Enter into a Context – Service Contexts

Use this syntax when in a service context.

```
cd Service_Name
cd Hoc
```

Get Back to the Global Context from a Service Context

Use this syntax when in a service context.

```
cd
```

columnars

Retrieves the columns associated with a table.

Applies To			
Services	Tables	Columns	Variables
	✓		

Table Consultation – Global Context

Use this syntax when in the global context.

```
columnars Service_Name.Table_Name
columnars Hoc.DnsServersInfo
```

Table Consultation – Service Contexts

Use this syntax when in a service context.

```
columnars Table_Name
columnars DnsServersInfo
```

commands

Retrieves the commands associated with a service or a table.

Applies To			
Services	Tables	Columns	Variables
✓	✓		

Service Consultation – Global Context

Use this syntax when in the global context.

```
commands Service_Name
commands Bni
```

Service Consultation – Service Contexts

Use this syntax when in a service context.

```
commands
```

Table Consultation – Global Context

Use this syntax when in the global context.

```
commands Service_Name.Table_Name
commands Hoc.DnsServersInfo
```

Table Consultation – Service Contexts

Use this syntax when in a service context.

```
commands Table_Name
commands DnsServersInfo
```

defval

Retrieves the default value of the expression. The expression may be a variable (scalar), a table column, or a table cell).

Applies To			
Services	Tables	Columns	Variables
		✓	✓

Variables – Global Context

Use this syntax when in the global context.

```
defval Service_Name.Scalar_Name
defval Cli.InactivityTimeOut
```

Variables – Service Contexts

Use this syntax when in a service context.

```
defval Scalar_Name
defval InactivityTimeOut
```

Cell or Column Properties – Global Context

Use this syntax when in the global context. The `Index` parameter is the first column of the table.

```
defval Service_Name.Table_Name[Index=key].Column_Name
defval Hoc.DnsServersInfo[Priority=2].IpAddress

defval Service_Name.Table_Name.Column_Name
defval Hoc.DnsServersInfo.IpAddress
```

Cell or Column Properties – Service Contexts

Use this syntax when in a service context. The `Index` parameter is the first column of the table.

```
defval Table_Name[Index=key].Column_Name
defval DnsServersInfo[Priority=2].IpAddress

defval Table_Name.Column_Name
defval DnsServersInfo.IpAddress
```

dump

Displays the unit's whole configuration on screen.

```
dump
```

Applies To			
Services	Tables	Columns	Variables
✓	✓	✓	✓

get

Retrieves the value of the expression. The expression may be a variable (scalar), a table, a table row, a table column, or a table cell). Note that entering the `get` command is optional.

Applies To			
Services	Tables	Columns	Variables
	✓	✓	✓

Variable Consultation – Global Context

Use this syntax when in the global context.

```
Service_Name.Scalar_Name
Cli.InactivityTimeOut
get Service_Name.Scalar_Name
get Cli.InactivityTimeOut
```

Variable Consultation – Service Contexts

Use this syntax when in a service context.

```
Scalar_Name
InactivityTimeout
get Scalar_Name
get InactivityTimeOut
```

Table Consultation – Global Context

Use this syntax when in the global context.

```
Service_Name.Table_Name
Hoc.DnsServersInfo
get Service_Name.Table_Name
get Hoc.DnsServersInfo
```

Table Consultation – Service Contexts

Use this syntax when in a service context.

```
Table_Name
DnsServersInfo
get Table_Name
get DnsServersInfo
```

Column Consultation – Global Context

Use this syntax when in the global context.

```
Service_Name.Table_Name.Column_Name
Hoc.DnsServersInfo.Priority
get Service_Name.Table_Name.Column_Name
get Hoc.DnsServersInfo.Priority
```

Column Consultation – Service Contexts

Use this syntax when in a service context.

```
Table_Name.Column_Name
DnsServersInfo.Priority
get Table_Name.Column_Name
get DnsServersInfo.Priority
```

Row Consultation – Global Context

Use this syntax when in the global context. The `Index` parameter is the first column of the table.

```
Service_Name.Table_Name[Index=key]
Hoc.DnsServersInfo[Priority=2]
get Service_Name.Table_Name[Index=key]
get Hoc.DnsServersInfo[Priority=2]
```

Row Consultation – Service Contexts

Use this syntax when in a service context. The `Index` parameter is the first column of the table.

```
Table_Name[Index=key]
DnsServersInfo[Priority=2]
get Table_Name[Index=key]
get DnsServersInfo[Priority=2]
```

Cell Consultation – Global Context

Use this syntax when in the global context. The `Index` parameter is the first column of the table.

```
Service_Name.Table_Name[Index=key].Column_Name
Hoc.DnsServersInfo[Priority=2].IpAddress
get Service_Name.Table_Name[Index=key].Column_Name
get Hoc.DnsServersInfo[Priority=2].IpAddress
```

Cell Consultation – Service Contexts

Use this syntax when in a service context. The `Index` parameter is the first column of the table.

```
Table_Name[Index=key].Column_Name
DnsServersInfo[Priority=2].IpAddress
get Table_Name[Index=key].Column_Name
get DnsServersInfo[Priority=2].IpAddress
```

help

Retrieves the documentation related to the expression. This keyword is case sentitive.

You can have access to general or contextual help. You can access the general help by typing the `help` keyword. You can access the contextual help by typing the `help` keyword followed by the name of the expression.

Applies To			
Services	Tables	Columns	Variables
✓	✓	✓	✓

Service Consultation – Global Context

Use this syntax when in the global context.

```
help Service_Name
help Bni
```

Service Consultation – Service Contexts

Use this syntax when in a service context.

```
help
```

Table Consultation – Global Context

Use this syntax when in the global context.

```
help Service_Name.Table_Name
help Hoc.DnsServersInfo

help Service_Name.Table_Name.Column_Name
help Hoc.DnsServersInfo.IpAddress
```

Table Consultation – Service Contexts

Use this syntax when in a service context.

```
help Table_Name
help DnsServersInfo

help Table_Name.Column_Name
```

```
help DnsServersInfo.IpAddress
```

Commands – Global Context

Use this syntax when in the global context.

```
help Service_Name.Command
help Scm.LockConfig
```

Commands – Service Contexts

Use this syntax when in a service context.

```
help Command
help LockConfig
```

indexes

Retrieves the indexes associated with the expression of a table. The expression may be the table itself or one of its columns.

Applies To			
Services	Tables	Columns	Variables
	✓	✓	

Table Consultation – Global Context

Use this syntax when in the global context.

```
indexes Service_Name.Table_Name
indexes Hoc.DnsServersInfo
```

Table Consultation – Service Contexts

Use this syntax when in a service context.

```
indexes Table_Name
indexes DnsServersInfo
```

Column Consultation – Global Context

Use this syntax when in the global context.

```
indexes Service_Name.Table_Name.Column_Name
indexes Hoc.DnsServersInfo.IpAddress
```

Column Consultation – Service Contexts

Use this syntax when in a service context.

```
indexes Table_Name.Column_Name
indexes DnsServersInfo.IpAddress
```

keys

Retrieves the keys associated with the expression of a table. The expression may be the table itself or one of its columns.

Applies To			
Services	Tables	Columns	Variables
	✓	✓	

Table Consultation – Global Context

Use this syntax when in the global context.

```
keys Service_Name.Table_Name
keys Hoc.DnsServersInfo
```

Table Consultation – Service Contexts

Use this syntax when in a service context.

```
keys Table_Name
keys DnsServersInfo
```

Column Consultation – Global Context

Use this syntax when in the global context.

```
keys Service_Name.Table_Name.Column_Name
```

keys Hoc.DnsServersInfo.IpAddress

Column Consultation – Service Contexts

Use this syntax when in a service context.

```
keys Table_Name.Column_Name
```

keys DnsServersInfo.IpAddress

logs off

Stops to display of Syslog traces.

```
logs off
```

Applies To			
Services	Tables	Columns	Variables
✓	✓	✓	✓

logs on

Displays Syslog traces as soon as they are sent.

The traces displayed are the notifications coming from the services, the diagnostic traces and the Signaling Logs.

```
logs on
```

Applies To			
Services	Tables	Columns	Variables
✓	✓	✓	✓

ls

Retrieves the list of services available in a global context and the objects of the service on a service context.

Applies To			
Services	Tables	Columns	Variables
✓	✓		

Service Consultation – Global Context

Use this syntax when in the global context.

```
ls Service_Name
```

ls Bni

Service Consultation – Service Contexts

Use this syntax when in a service context.

```
ls
```

Table Consultation – Global Context

Use this syntax when in the global context.

```
ls Service_Name.Table_Name
```

ls Hoc.DnsServersInfo

Table Consultation – Service Contexts

Use this syntax when in a service context.

```
ls Table_Name
```

ls DnsServersInfo

name

Retrieves the name of the expression. This keyword is case sensitive. You must type the exact name after the `name` key.

Applies To			
Services	Tables	Columns	Variables
✓	✓	✓	✓

Variables Configuration – Global Context

Use this syntax when in the global context.

```
name Service_Name.Scalar_Name
name Cli.InactivityTimeOut
```

Variables Configuration – Service Contexts

Use this syntax when in a service context.

```
name Scalar_Name
name InactivityTimeOut
```

Table Configuration – Global Context

Use this syntax when in the global context.

```
name Service_Name.Table_Name
name Hoc.DnsServersInfo

name Service_Name.Table_Name.Column_Name
name Hoc.DnsServersInfo.IpAddress
```

Table Configuration – Service Contexts

Use this syntax when in a service context.

```
name Table_Name
name DnsServersInfo

name Table_Name.Column_Name
name DnsServersInfo.IpAddress
```

Command Execution – Global Context

Use this syntax when in the global context.

```
name Service_Name.Command
name Scm.LockConfig
```

Command Execution – Service Contexts

Use this syntax when in a service context.

```
name Command
name LockConfig
```

objects

Retrieves the objects associated with the expression of a service.

Applies To			
Services	Tables	Columns	Variables
✓	✓		

Service Consultation – Global Context

Use this syntax when in the global context.

```
objects Service_Name
objects Bni
```

Service Consultation – Service Contexts

Use this syntax when in a service context.

```
objects
```

Table consultation – Global Context

Use this syntax when in the global context.

```
objects Service_Name.Table_Name
objects Hoc.DnsServersInfo
```

Table consultation – Service Contexts

Use this syntax when in a service context.

```
objects Table_Name
objects DnsServersInfo
```

PCapture

Starts a network capture. Typing ctrl+c stops immediately a running capture command and displays statistics. Supported parameters can be found by typing "help pcapture".

The Telnet and SSH ports are automatically filtered out. The host addresses are not converted to names to avoid DNS lookups. The protocol and port numbers are not converted to names either.

Use this syntax.

```
pcapture [options] [expression]
pcapture -raw -c 50 port 161
```

Options:

- -c 'count': Exit after receiving 'count' packets.
- -raw: Raw packets are output (unreadable output, must be redirected to file or Wireshark)
- -D: Print the list of network interfaces available on the system and on which pcapture can capture packets.
- -e: Print the link-level header on each dump line.
- -i 'if': Listen on interface 'if'. Can be any of the interfaces returned by option -D or can be set to 'any'. 'any' will listen on all interfaces but not in promiscuous mode.
- -p: Don't put the interface into promiscuous mode.
- -S: Print absolute, rather than relative, TCP sequence numbers.
- -T 'expression': Force packets selected by 'expression' to be interpreted of the specified type. Supported types are rtp, rtcp, snmp, tftp.

Expression:

- Selects which packets will be dumped. If no expression is given, all packets on the net will be dumped. Otherwise, only packets for which expression is 'true' will be dumped. For the expression syntax, see pcap-filter(7).

It is possible to route the capture to Wireshark to have a remote live capture. From the remote PC (Windows or Linux), type the following command:

```
plink.exe -pw "" public@10.4.127.128 "pcapture -raw port 161" | wireshark -k -i -
```

This example connects by using plink (from putty) in SSH to the unit 10.4.127.128 by using the username "public" and an empty password. It would capture the SNMP packets.

For more information in the `pcapture` command, please refer to the following page: http://www.tcpdump.org/pcap3_man.html.

ping (IPv4)

Executes a ping command using IPv4 with the arguments and the target host provided by the user.

Use this syntax when using the *ping* command:

```
ping [-c COUNT -s SIZE -q] host_name
ping -c 3 -s 300 -q 192.168.0.25
```

The supported ping arguments are:

- -c COUNT: Stops the ping after it has sent COUNT packets.
- -s SIZE: Sends SIZE data bytes in packets (default = 56).
- -q: Shows information only at the start and when finished.

Typing Ctrl+c immediately stops a running *ping* command and displays statistics.

ping (IPv6)

Executes a ping command using IPv6 with the arguments and the target host provided by the user.

Use this syntax when using the *ping* command:

```
ping [-c COUNT -s SIZE -q] host_name
ping -c 3 -s 300 -q 192.168.0.25
```

The supported ping arguments are:

- -c COUNT: Stops the ping after it has sent COUNT packets.
- -s SIZE: Sends SIZE data bytes in packets (default = 56).
- -q: Shows information only at the start and when finished.

Typing Ctrl+c immediately stops a running *ping* command and displays statistics.

scalars

Retrieves the scalars associated with the expression of a service.

Applies To			
Services	Tables	Columns	Variables
✓			

Service Consultation – Global Context

Use this syntax when in the global context.

```
scalars Service_Name
scalars Bni
```

Service Consultation – Service Contexts

Use this syntax when in a service context.

```
scalars
```

set

Assigns a constant value to the expression. The expression may be a variable (scalar) or a table cell.

Applies To			
Services	Tables	Columns	Variables
		✓	✓

Variables Configuration – Global Context

Use this syntax when in the global context.

```
Service_Name.Scalar_Name = constant
Cli.InactivityTimeOut = 25
set Service_Name.Scalar_Name = constant
set Cli.InactivityTimeOut = 25
```

Variables Configuration – Service Contexts

Use this syntax when in a service context.

```
Scalar_Name = constant
InactivityTimeOut = 25
set Scalar_Name = constant
set InactivityTimeOut = 25
```

Cell Configuration – Global Context

Use this syntax when in the global context. The `Index` parameter is the first column of the table.

```
Service_Name.Table_Name[Index=key].Column_Name=Value
Hoc.DnsServersInfo[Priority=2].IpAddress="192.168.0.10"
set Service_Name.Table_Name[Index=key].Column_Name=Value
set Hoc.DnsServersInfo[Priority=2].IpAddress="192.168.0.10"
```

Cell configuration – Service Contexts

Use this syntax when in a service context. The `Index` parameter is the first column of the table.

```
Table_Name[Index=key].Column_Name=Value
DnsServersInfo[Priority=2].IpAddress="192.168.0.10"
set Table_Name[Index=key].Column_Name=Value
set DnsServersInfo[Priority=2].IpAddress="192.168.0.10"
```

show

Retrieves the value of the expression.

Applies To			
Services	Tables	Columns	Variables
	✓	✓	✓

Variable Consultation – Global Context

Use this syntax when in the global context.

```
show Service_Name.Scalar_Name
show Cli.InactivityTimeOut
```

Variable Consultation – Service Contexts

Use this syntax when in a service context.

```
show Scalar_Name
show InactivityTimeOut
```

Table Consultation – Global Context

Use this syntax when in the global context.

```
show Service_Name.Table_Name
show Hoc.DnsServersInfo
```

Table Consultation – Service Contexts

Use this syntax when in a service context.

```
show Table_Name
show DnsServersInfo
```

Column Consultation – Global Context

Use this syntax when in the global context.

```
show Service_Name.Table_Name.Column_Name
show Hoc.DnsServersInfo.IpAddress
```

Column Consultation – Service Contexts

Use this syntax when in a service context.

```
show Table_Name.Column_Name
show DnsServersInfo.IpAddress
```

Row Consultation – Global Context

Use this syntax when in the global context. The `Index` parameter is the first column of the table.

```
show Service_Name.Table_Name[Index=key]
show Hoc.DnsServersInfo[Priority=2]
```

Row Consultation – Service Contexts

Use this syntax when in a service context. The `Index` parameter is the first column of the table.

```
show Table_Name[Index=key]
```

show DnsServersInfo[Priority=2]

Cell Consultation – Global Context

Use this syntax when in the global context. The `Index` parameter is the first column of the table.

```
show Service_Name.Table_Name[Index=key].Column_Name
```

show Hoc.DnsServersInfo[Priority=2].IpAddress

Cell Consultation – Service Contexts

Use this syntax when in a service context. The `Index` parameter is the first column of the table.

```
show Table_Name[Index=key].Column_Name
```

show DnsServersInfo[Priority=2].IpAddress

sysinfo

Displays the current unit status. The information displayed is:

- System Description
- Serial Number
- Firmware Version
- Host Name
- Mac Address
- System Uptime
- System Time
- Snmp Port
- Installed Hardware Information (Name, description, location).

tables

Retrieves the tables associated with the a service.

Applies To			
Services	Tables	Columns	Variables
✓			

Service Consultation – Global Context

Use this syntax when in the global context.

```
tables Service_Name
```

tables Bni

Service Consultation – Service Contexts

Use this syntax when in a service context.

```
tables
```

type

Retrieves the type of the data of the expression. The expression may be a variable (scalar), a table column, or a table cell.

Applies To			
Services	Tables	Columns	Variables
		✓	✓

Variables Configuration – Global Context

Use this syntax when in the global context.

```
type Service_Name.Scalar_Name
```

type Cli.InactivityTimeOut

Variables Configuration – Service Contexts

Use this syntax when in a service context.

```
type Scalar_Name
type InactivityTimeOut
```

Cell or Column Properties – Global Context

Use this syntax when in the global context. The `Index` parameter is the first column of the table.

```
type Service_Name.Table_Name[Index=key].Column_Name
type Hoc.DnsServersInfo[Priority=2].IpAddress
```

```
type Service_Name.Table_Name.Column_Name
type Hoc.DnsServersInfo.IpAddress
```

Cell or Column Properties – Service Contexts

Use this syntax when in a service context. The `Index` parameter is the first column of the table.

```
type Table_Name[Index=key].Column_Name
type DnsServersInfo[Priority=2].IpAddress
```

```
type Table_Name.Column_Name
type DnsServersInfo.IpAddress
```

Command Execution

This section describes the syntax to use to execute a MIB command.

Global Context

```
Service_Name.Command arg1=value1 -b arg2=[value2 value3 value4]
SipEp.InsertGateway Name=test
```

Service Context

```
Command arg1=value1 -b arg2=[value2 value3 value4]
InsertGateway Name=test
```

CHAPTER
3

Web Interface Configuration

The Aastra unit contains an embedded web server to set parameters by using the HTTP or HTTPS protocol.

Standards Supported	• RFC 1945: Hypertext Transfer Protocol - HTTP/1.0 • RFC 2616: Hypertext Transfer protocol - HTTP/1.1.

This chapter describes the following:

- Introduction to the Aastra unit web pages.
- Short description of the Aastra unit SNMP configuration.
- How to access the web interface and description of the various menus available.
- How to submit changes.

Introduction

The web interface may be used to:

- View the status of the Aastra unit.
- Set the uplink parameters of the Aastra unit.
- Perform a firmware update, configuration scripts download, or configuration backup/restore.
- Set numerous parameters of the Aastra unit.

All of the parameters in the web interface may also be configured via SNMP. See“Chapter 44 - SNMP Configuration” on page 437 for more details.

▶ **To configure the web-based configuration service:**

1. In the *webMIB*, locate the *serverGroup* folder.

2. Define the HTTP mode(s) to which the Web server should listen in the `httpMode` variable.

You can also use the following line in the CLI or a configuration script:

```
web.httpMode="Value"
```

where *Value* may be as follows:

Table 10: HTTP Modes

Value	Mode	Description
100	Secure	The Web server only accepts requests using HTTPS. Requests using HTTP are ignored. This is the default value.
200	Unsecure	The Web server only accepts requests using HTTP. Requests using HTTPS are ignored.
300	Both	The Web server accepts requests using HTTP or HTTPS.

If you are using HTTPS (either in “Secure” mode or “Both” mode), the web server needs a valid server certificate with “server authentication” extended key usage installed on the Aastra unit. See “Chapter 43 - Certificates Management” on page 431 for more details.

Accessing the web pages via HTTPS adds additional delay since encryption is used. To access the unit via HTTPS, your browser must support RFC 2246 (TLS 1.0).

Note that the web server does not listen to the configured modes when the management interface is down or a configuration error occurred (e.g., missing or invalid certificate for HTTPS mode) while setting up the web server.

3. Set the TCP port on which the web service listens for HTTP requests in the `serverPort` variable.

   You can also use the following line in the CLI or a configuration script:

   `web.serverPort="Value"`

4. Set the port on which the web service listens for HTTPS requests in the `secureServerPort` variable.

   You can also use the following line in the CLI or a configuration script:

   `web.secureServerPort="Value"`

HTTP User-Agent Header Format

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

You can define the text to display in the HTTP *User-Agent* header. You can use macros to include information specific to the unit.

You can also define the same information in the SIP *User-Agent* header. See "SIP User-Agent Header Format" on page 208 for more details.

To set the HTTP User-Agent header format:

1. In the *hocMIB*, set the HTTP *User-Agent* header format in the `httpUaHeaderFormat` variable.

   You can also use the following line in the CLI or a configuration script:

   `hoc.httpUaHeaderFormat="Value"`

   where *Value* may contain any text, as well as one or more of the following macros:

Table 11: Macros Supported

Macro	Description
%version%	Application version.
%mac%	MAC address.
%product%	Product name.
%profile%	Profile.
%%	Insert the % character.

For instance, the default value is:

`%product%/v%version% %profile%`

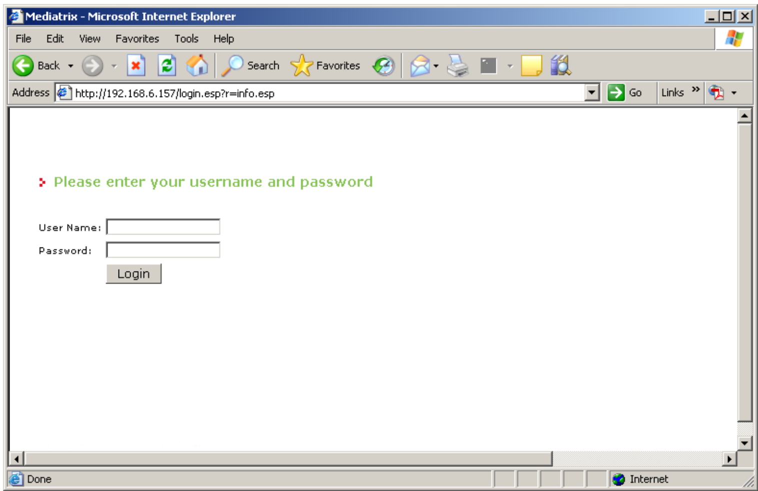
Using the Web Interface

Aastra recommends that you use the latest version of the Microsoft® Internet Explorer web browser to properly access the web interface.

▶ To use the web interface configuration:

1. In your web browser's address field, type the IP address of the Aastra unit LAN interface (if you have performed a partial reset, this is **192.168.0.10**).

Figure 8: Login Window



2. Enter the proper user name and password.

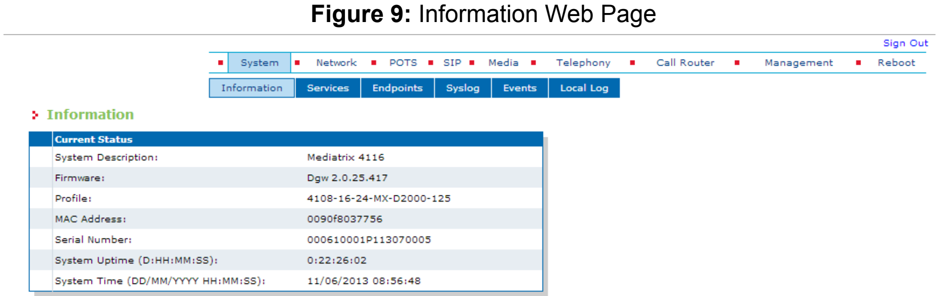
   The user name and password are case sensitive hence they must be entered properly. Default factory values are:
   - **User Name**: admin
   - **Password**: administrator

   You can also enter the user name **public** and no password.

3. Click *Login*.

   The *Information* web page displays. It stays accessible for as long as the Internet browser used to access the Aastra unit web interface is opened.

Figure 9: Information Web Page



4. Click *Sign Out* to end your Aastra web session.

   The *Login Window* web page displays.

Menu Items

The Menu frame is displayed at the top of the browser window. It contains management links that allow you to display web pages in the Content frame. The management links available vary depending on the Aastra unit you are using.

Table 12: Menu Frame Links

Link	Description
System	***Information***: Displays, in read-only format, the status of the Aastra unit.
	Services: Allows you to start/stop the services running on the Aastra unit. See "Chapter 4 - Services" on page 43 for more details.
	Hardware: Not applicable for TA7102i.
	Endpoints: Allows you to configure the administrative state of the Aastra unit's ports. See"Chapter 6 - Endpoints Configuration" on page 53 for more details.
	Syslog: Allows you to configure the Aastra unit to properly handle syslog messages and notification messages. See "Chapter 7 - Syslog Daemon Configuration" on page 57 for more details.
	Events: Allows you to associate a NOTIFICATION message and how to send it (via syslog or via a SIP NOTIFY packet). See"Chapter 8 - Notification Events" on page 63 for more details.
	Local Log: Displays local log status and entries of your Aastra unit. See "Chapter 9 - Local Log" on page 81 for more details.
Network	***Status***: Displays, in read-only format, the network parameters status of the Aastra unit.
	Host: Allows you to configure the host parameters of the Aastra unit. See "Chapter 11 - General Configuration" on page 75 for more details.
	Interfaces: Allows you to configure the uplink information used by the Aastra unit. See "Chapter 11 - General Configuration" on page 75 for more details.
	VLAN: Allows you to create and manage VLANs on the Aastra unit. See "Chapter 13 - VLAN Parameters" on page 99 for more details.
	QoS: Allows you to configure packets tagging sent from the Aastra unit. See "Chapter 14 - Local QoS (Quality of Service) Configuration" on page 101 for more details.
	Local Firewall: Allows you to configure the local firewall service of the Aastra unit. See"Chapter 15 - Local Firewall Configuration" on page 107 for more details.
	IP Routing: Allows you to configure the IP routing parameters of the Aastra unit. See "Chapter 16 - IP Routing Configuration" on page 127 for more details.
	Network Firewall: Allows you to configure the network firewall service of the Aastra unit. See "Chapter 17 - Managing the Network Firewall" on page 121 for more details.
	NAT: Allows you to configure the NAT service of the Aastra unit. See "Chapter 18 - NAT Configuration" on page 127 for more details.
	DHCP Server: Allows you to configure the the embedded DHCP server of the Aastra unit. See "Chapter 19 - DHCP Server Settings" on page 135 for more details.

Table 12: Menu Frame Links (Continued)

Link	Description
POTS	***Status***: Allows you to view the status of the Aastra unit POTS parameters. See "Chapter - POTS Parameters" on page 143for more details.
	Config: Allows you to configure the POTS parameters of the Aastra unit. See "Chapter 20 - General POTS Configuration" on page 145 for more details.
	FXS Config: Allows you to configure the FXS parameters of the Aastra unit. See "Chapter 20 - POTS Configuration" on page 145 for more details.
	FXO Config: Not applicable.
SIP	***Gateways***: Allows you to add and remove SIP gateways in the Aastra unit. See "Chapter 21 - SIP Gateways Configuration" on page 155 for more details.
	Servers: Allows you to configure the SIP server and SIP user agent parameters of the Aastra unit. See "Chapter 22 - SIP Servers" on page 159 for more details.
	Registrations: Allows you to configure the registration parameters of the Aastra unit. See "Chapter 23 - Endpoints Registration" on page 167 for more details.
	Authentication: Allows you to configure authentication parameters of the Aastra unit. See "Chapter 24 - SIP Authentication" on page 179 for more details.
	Transport: Allows you to configure the SIP transport parameters of the Aastra unit. See "Chapter 25 - SIP Transport Parameters" on page 183 for more details.
	Interop: Allows you to configure the SIP interop parameters of the Aastra unit. See "Chapter 26 - Interop Parameters" on page 189 for more details.
	Misc: Allows you to configure interoperability features of the Aastra unit. See "Chapter 27 - SIP Penalty Box" on page 211 for more details.
Media	**Codecs**: Allows you to configure the voice and data codec related parameters of the Aastra unit. See "Chapter 28 - Voice & Fax Codecs Configuration" on page 231 for more details.
	Security: Allows you to properly configure the security parameters of the Aastra unit. See "Chapter 29 - Security" on page 253 for more details.
	RTP Stats: Allows you to read and configure the RTP statistics collected by the Aastra unit. See "Chapter 30 - RTP Statistics Configuration" on page 257 for more details.
	Misc: Allows you to configure parameters that apply to all codecs. See "Chapter 31 - Miscellaneous Media Parameters" on page 263 for more details.
Telephony	***DTMF Maps***: Allows you to configure the various DTMF maps of the Aastra unit. See "Chapter 32 - DTMF Maps Configuration" on page 279 for more details.
	Call Forward: Allows you to configure three types of Call Forward. See "Chapter 33 - Call Forward Configuration" on page 287 for more details.
	Services: Allows you to configure the Aastra unit subscriber services. See "Chapter 34 - General Configuration" on page 295 for more details.
	Tone Customization: Allows you to override the pattern for a specific tone defined for the selected country. See "Chapter 35 - Tone Customization Parameters Configuration" on page 317 for more details.
	Music on Hold: Allows you to configure the Music on Hold service of the Aastra unit. See "Chapter 36 - Configuring the TFTP Server" on page 321 for more details.
	Misc: Allows you to configure the country in which the Aastra unit is located. See "Chapter 37 - Country Configuration" on page 325 for more details.

Table 12: Menu Frame Links (Continued)

Link	Description
Call Router	***Status***: Allows you to view the current status of the call routing service. See "Chapter 38 - Call Router Configuration" on page 335 for more details.
	Route Config: Allows you to configure the call routing service of the Aastra unit. See "Chapter 38 - Call Router Configuration" on page 335 for more details.
	Auto-routing: Allows you to configure the auto-routing feature of the Aastra unit. See "Chapter 39 - Auto-Routing Configuration" on page 391 for more details.
Management	***Configuration Scripts***: Allows you to configure the various configuration scripts parameters of the Aastra unit. See "Chapter 40 - Creating a Configuration Script" on page 414 for more details.
	Backup / Restore: Allows you to configure how to backup and restore the Aastra unit's configuration. See "Chapter 41 - Configuration Backup/Restore" on page 415 for more details.
	Firmware Upgrade: Allows you to configure the various firmware upgrade parameters of the Aastra unit. See "Chapter 42 - Firmware Download" on page 423 for more details.
	Certificates: Allows you to add and delete security certificates in the Aastra unit. See "Chapter 43 - Certificates Management" on page 431 for more details.
	SNMP: Allows you to configure the SNMP privacy parameters of the Aastra unit. See "Chapter 44 - SNMP Configuration" on page 437 for more details.
	CWMP: Not applicable.
	Access Control: Allows you to set the Access Control parameters of the Aastra unit. See "Chapter 45 - Users" on page 443 for more details.
	File:Allows you to use the unit's File Manager. See "File Manager" on page 449 for more details.
	Misc: Allows you to set various parameters used to manage the Aastra unit. See "Chapter 47 - Management Interface Configuration" on page 451 for more details.
Reboot	Allows you to restart the Aastra unit.

Submitting Changes

When you perform changes in the web interface and click the *Submit* button, the Aastra unit validates the changes. A message is displayed next to any invalid value. A message is also displayed if a service must be restarted and a link is displayed at the top of the page. This link brings you to the *Services* page. In this page, each service that requires to be restarted has a "*" beside its name. See "Chapter 4 - Services" on page 53 for more details.

If you are not able to restart one or more services, click the *Reboot* link in the top menu. The *Reboot* page then opens. You must click *Reboot*. This restarts the Aastra unit. If the unit is in use when you click *Reboot*, all calls are terminated.

Where to Go From Here?

If you want to configure the Aastra unit to perform a basic call, this usually involves the following:

Table 13: Basic Call Configuration Steps

Action	Description	Where to?
Configuring the POTS parameters TA7102i	You must minimally configure the FXS interfaces so that they can send and receive calls.	"Chapter 20 - POTS Configuration" on page 145
Configuring the SIP Endpoint	Configuring the SIP endpoint allows you to register your ISDN telephone or FXS interfaces to a SIP server. This includes setting the following parameters: • Registrar Server Host • Proxy Home Domain Host • User Name • Friendly Name • Gateway Name	"Chapter 22 - Introduction" on page 159 "Chapter 23 - Registration Configuration" on page 169 "Chapter 21 - SIP Gateways" on page 155
Configuring the Call Router with Routes	You must create routes that will route calls from FXS to SIP and from SIP to FXS.	"Call Router Configuration" on page 335
Configuration of the Call Router: Mapping	You must create mappings that will allow you to properly communicate from FXS to SIP and from SIP to FXS.	"Mappings" on page 358

Using Secure Communication

The Aastra unit allows you to use a secure communication whenever required. You must set the Aastra unit with security parameters:

Table 14: Secure Communication Steps

Step	Where to?
5. Transfer a valid CA certificate into the Aastra unit.	"Chapter 46 - Certificates Management" on page 557
6. Use secure signalling by enabling the TLS transport protocol.	"Chapter 25 - SIP Transport Parameters" on page 183
7. Use secure media by: • Defining the SRTP/ SRTCP base port. • Setting the RTP secure mode to "Secure" or "Secure with fallback".	"Base Ports Configuration" on page 273 "Security Parameters" on page 253

System Parameters

Page Left Intentionally Blank

CHAPTER

4

Services

This chapter describes how to view and start/stop system and network parameters of the Aastra unit.

Services Table

The Aastra unit uses many services grouped in two classes: system and user. You can perform service commands on user services, but not the system services.

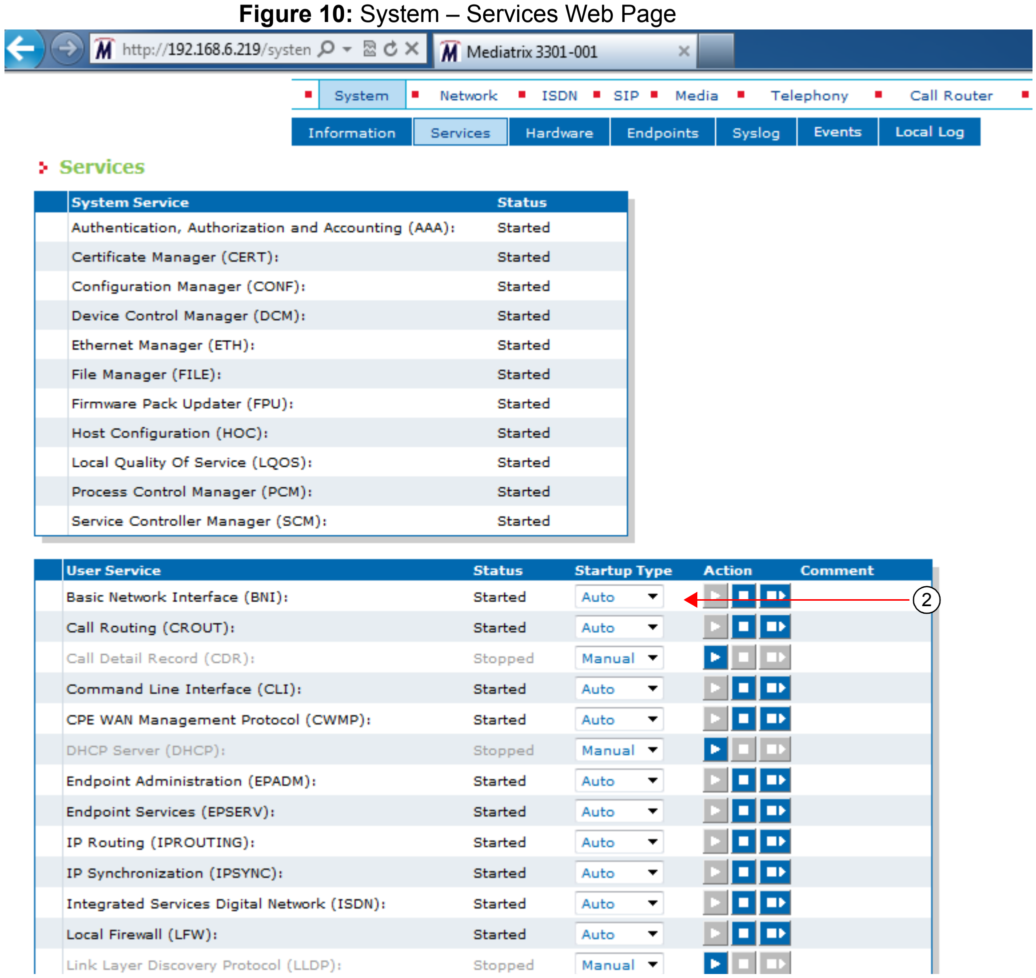
Whenever you perform changes in the various sections of the web interfaces, this usually means that you must restart a service for the changes to take effect. When a service needs to be restarted, it is displayed in bold and the message *Restart needed* is displayed in the *Comment* column.

If you are not able to restart a service because it is a system service, click the *Reboot* link in the top menu. The *Reboot* page then opens. You must click *Reboot*. This restarts the Aastra unit. If the unit is in use when you click *Reboot*, all calls are terminated.

▶ **To manage the Aastra unit services:**

1. In the web interface, click the *System* link, then the *Services* sub-link.

Figure 10: System – Services Web Page



The following are the services available.

Table 15: Aastra unit Services

Service	Description
System Services	
Authentication, Authorization and Accounting (AAA)	Authenticates a user and grants rights to perform specific tasks on the system.
Certificate Manager (CERT)	Manages certificate files and provides access to these certificates.
Configuration Manager (CONF)	Responsible of configuration scripts transfers, as well as configuration image upload/download for backup/restore of the unit configuration.
Device Control Manager (DCM)	Auto-detects and identifies the hardware components of the unit.
Ethernet Manager (ETH)	Configures the system's Ethernet ports parameters.
File Manager (FILE)	Manages the files created with the *File* transfer protocol.
Firmware Pack Updater (FPU)	Handles firmware upgrade and downgrade operations.
Host Configuration (HOC)	Configures network parameters that apply to the Aastra unit (not to a specific interface).
Local Quality Of Service (LQOS)	Configures the packets tagging sent from the Aastra unit.
Process Control Manager (PCM)	Responsible to boot and restart the unit.
Service Controller Manager (SCM)	Responsible to: • Manage services information. • Offer proxy functionality for service interoperation.
User Services	
Basic Network Interface (BNI)	Configures the IP address and network mask for the Uplink and LAN1 networks.
Call Routing (CROUT)	Routes calls between interfaces.
Call Detail Record (CDR)	
Command Line Interface (CLI)	Allows you user to configure the unit parameters by, Telnet or SSH.
CPE WAN Management Protocol (CWMP)	Not applicable.
DHCP Server (Dhcp)	Allows the user to lease IP addresses and send network configuration to hosts located on any network.
Endpoint Administration (EpAdm)	Holds basic administration and status at endpoint and unit level.
Endpoint Services (EpServ)	Manages endpoint behaviour and holds configuration parameters related to endpoints (such as DTMF maps, telephony services, etc.).
IP Routing (IpRouting)	Allows the user to configure the unit's routing table.
IP Synchronization (IpSync)	Controls the IP media synchronization using clock reference signals sent over IP.

Table 15: Aastra unit Services (Continued)

Service	Description
Integrated Services Digital Network (ISDN)	Not applicable.
Local Firewall (LFW)	Allows you to filter incoming packets whose final destination is the unit.
Link Layer Discovery Protocol (Lldp):	Used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, usually wired Ethernet.
Media IP Transport (MIPT)	Holds basic configuration parameters (such as voice/data codec) and implements basic functionality related to media stream.
Music on Hold (MOH)	Allows you to configure the Music on Hold parameters.
Network Address Translation (Nat)	Allows the user to change the source or destination address/port of a packet.
Network Firewall (Nfw)	Allows the user to filter forwarded packets.
Notifications and Logging Manager (NLM)	Handles syslog messages and notification messages.
Network Traffic Control (Ntc)	Controls the bandwidth limitation applied to physical network interfaces.
Plain Old Telephony System Lines service (POTS)	Holds basic configuration parameters (such as DTMF dialing delays) and implements basic functionality related to POTS lines (such as enabling/disabling individual lines).
SIP Endpoint (SipEp)	Manages the behaviour of the system regarding SIP.
SNMP (SNMP)	Accesses internal variables through an SNMP client. It also handles user authentication.
Telephony Interface (TELIF)	Configures the basic specification of each telephony interface.
Web (WEB)	Allows accessing the unit through web pages, using HTTP.

2. In the *User Service* section, select the service startup type of a service in the *Startup Type* column.

Table 16: Startup Types

Type	Description
Auto	The service is automatically started when the system starts.
Manual	The administrator must manually start the service.

You can put only user services in manual startup type. Proceed with caution when setting services to manual because this could prevent you from successfully contacting the unit.

3. Select if you want to perform service commands on one or more services in the *Action* column.

Table 17: Actions

Action	Description
	Starts the service.
	Stops the service.

Table 17: Actions

Action	Description
	Restarts the service.

When a service needs to be restarted to apply new configuration you have set elsewhere in the web interface, it is displayed in bold and the message *Restart needed* is displayed in the *Comment* column.

If you stop, start or restart a service, any dependent services are also affected. The tabs of the services that have been stopped or have never been started because their startup type is manual are greyed out. Upon clicking these tabs, a list of services that must be restarted is displayed.

4. Click the **Restart Required Services** button at the bottom of the page.

Graceful Restart of Services

You can set a delay to allow for telephony calls to be all completed before restarting services that need a restart.

During that delay, it is impossible to make new calls but calls in progress are not terminated. When all calls are completed, then the restart is authorized and the services that require a restart are restarted.

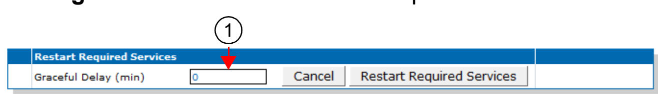
You can also set a unit restart grace period when performing a Firmware Upgrade as described in "Firmware Packs Configuration" on page 425.

▶ **To configure the graceful restart of services:**

1. In the *Restart Required Services* section, set the *Graceful Delay* field with the delay (in minutes) allowed for telephony calls to be all completed.

   At the expiration of this delay, the services are forced to restart.

Figure 11: Services – Restart Required Services Section



2. Click *Restart Required Services* to restart only the services that needed a restart for their configuration to be applied.

   If you click Cancel, this cancels the restart during the grace delay period.

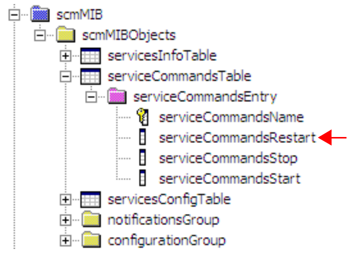
Restarting a Service via MIB

If you are using a MIB browser to access the Aastra unit configuration via SNMP, you can determine whether or not a service needs to be restarted by locating the *configurationGroup* folder of the related service and checking if the service needs to be restarted in the `needRestartInfo` variable.

Figure 12: Need Restart Info

If a specific service needs to be restarted, locate the *scmMIB*, then set the `serviceCommandsRestart` variable for this service to **restart**.

Figure 13: Restart Service



You can also start a service by setting the `serviceCommandsStart` variable for this service to **Start**.

You can also stop a service by setting the `serviceCommandsStop` variable for this service to **Stop**.

If you are not able to restart a service because it is a system service, you must restart the Aastra unit.

CHAPTER 5

Hardware Parameters

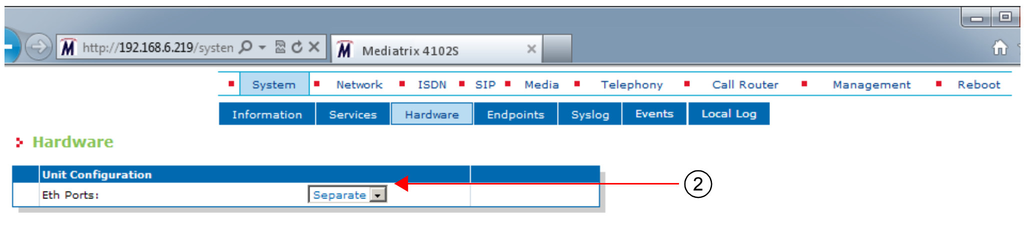
Hardware Card Configuration

For Aastra unit models that have two Ethernet ports, you can configure how each port provides a link interface.

▶ **To configure the bridging parameter:**

1. In the web interface, click the *System* link, then the *Hardware* sub-link.

Figure 14: System – Hardware Web Page (Aastra TA7102i shown)



2. In the *Unit Configuration* section, set the *Eth Ports* drop-down menu with the proper behaviour.

Table 18: Bridging Parameters

Parameter	Description
Separate	Each Ethernet port provides an independent link interface. This is the required configuration for IP Routing.
Bridge	Both Ethernet ports are bridged together and provide a single link interface.

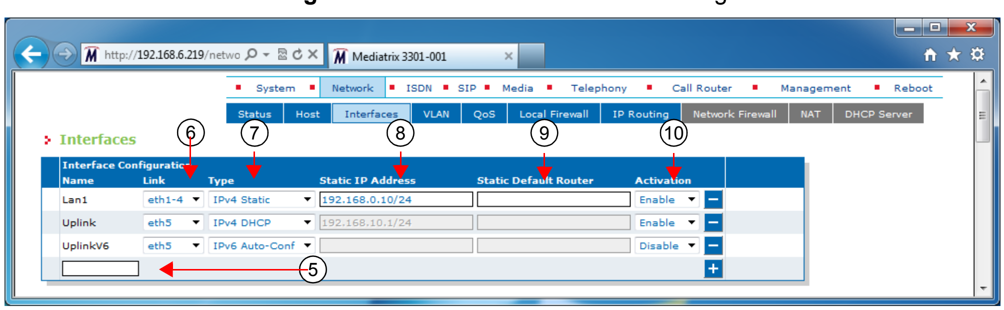
3. Click *Submit* if you do not need to set other parameters.

The following message displays:

Note: Your Ethernet configuration has changed. A link interface will be deactivated. Make sure that your network interfaces are configured accordingly prior to restarting the unit.

4. In the web interface, click the *Network* link, then the *Interfaces* sub-link.

Figure 15: Network – Interfaces Web Page



5. Enter the name of the new interface for bridging in the blank field in the bottom left of the window, then click the + button.

The name is case-sensitive. Using the special value “All” is not allowed.

6. In the *Interface Configuration* section, select the link on which to activate the interface in the *Link* column.

Select the link associated with the bridge. The name varies depending on the platform used.

7. Select the configuration source of the interface information in the *Type* drop-down menu.

Table 19: Interface Configuration Sources

Source	Description
IPv4 DHCP	The IPv4 address and network mask are provided by querying a DHCP server and using standard DHCP fields or options. Using the DHCP configuration assumes that you have properly set your DHCP server with the relevant information. DHCP servers may provide a list of IP configuration parameters to use. See “DHCP Server Configuration” on page 95 for more details.
IPv4 Static	You manually enter the IPv4 address and network mask and they remain the same every time the Aastra unit restarts. Use the static configuration if you are not using a DHCP server/PPP peer or if you want to bypass it.
IPv4 PPPoE	IPv4 over PPP connection, address and network mask are provided by the PPP peer using IPCP. PPP peers may provide a list of IP configuration parameters to use. See “PPPoE Configuration” on page 91 for more details.
IPv6 Auto-Conf	IPv6 state-less auto-configuration.
IPv6 Static	You manually enter the IPv6 address and network mask and they remain the same every time the Aastra unit restarts. Use the IPv6 static configuration if you are not using IPv6 stateless or stateful auto-configuration or if you want to bypass it.

Note: If no network is configured in IPv6, the unit does not have any IPv6 address, not even the Link-Local address. When a network is configured in IPv6, the Link-Local (FE80 ::...) address is automatically created and displayed in the Network Status information.

8. If the interface configuration source is **IPv4 Static** or **IPv6 Static**, enter the address and network mask (if applicable) of the network interface in the *Static IP address* field.

9. If the interface configuration source is **IPv4 Static** or **IPv6 Static**, set the *Static Default Router* field with the IP address of the default gateway for the network interface.

10. Define whether or not the Aastra unit should attempt to activate the corresponding network interface in the *Activation* drop-down menu.

It may not be possible to enable a network interface, for instance if another network interface is already enabled in the same subnet. The actual status of network interfaces is shown in the *Status* page.

Note: The newly created interface will be the only valid interface after the restart, make sure this interface is Enabled and correctly configured according on the Interface Configuration Source (your network).

11. Click *Submit* if you do not need to set other parameters.

The current network interface information is displayed in the *Status* page. See “Interfaces Configuration” on page 100 for more details on network interfaces.

12. Restart the Aastra unit to apply the change.

Ring Management

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser

- by using the CLI
- by creating a configuration script containing the configuration variables

You can determine how to ring more than one port. You have the following choices:

Table 20: Ring Management Parameters

Parameter	Descriprion
Cascade	The FXS ports are prevented from ringing at the same time in order to reduce the peak power usage of the device.
Simultaneous	All ports are ringing at the same time.

To set the ring management:

1. In the *MbLdpMIB*, set the `RingManagement` variable to the proper value.

   You can also use the following line in the CLI or a configuration script:

   ```
   MbLdp.RingManagement="Value"
   ```

   where *Value* may be as follows:

Table 21: Ring Management Values

Value	Description
100	Cascade
200	Simultaneous

CHAPTER 6

Endpoints State Configuration

This chapter describes how to set the administrative state of the Aastra unit's endpoints.

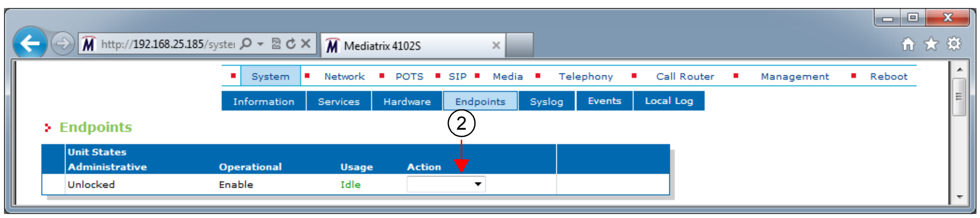
Unit Configuration

The unit configuration section allows you to define the administrative state of all the Aastra unit's endpoints.

▶ **To set the unit's endpoints parameters:**

1. In the web interface, click the *System* link, then the *Endpoints* sub-link.

Figure 16: System Configuration – Endpoints Web Page



2. In the *Unit States* section, select a temporary state for all of the unit's endpoints in the *Action* column.

This command locks/unlocks all endpoints of the Aastra unit. This state is kept until you modify it or the unit restarts. It offers the following settings:

Table 22: Action Settings

Setting	Description
Force Lock	Cancels all the endpoints registration to the SIP server. All active calls in progress are terminated immediately. No new calls may be initiated.
Lock	Cancels all the endpoints registration to the SIP server. Active calls in progress remain established until normal call termination. No new calls may be initiated.
Unlock	Registers the endpoints to the SIP server.

3. If you do not need to set other parameters, click *Submit*.

Endpoints Configuration

The endpoints configuration allows you to define the administrative state of the Aastra unit's endpoints.

▶ **To set the endpoints parameters:**

1. In the *Endpoint States* section of the *Endpoints* page, select the permanent administrative state each endpoint will have when the Aastra unit restarts in the *Initial Administrative* column.

Figure 17: Endpoint States Section

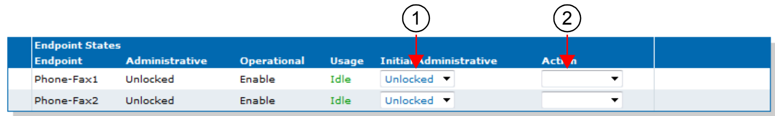


Table 23: Permanent Administrative State Settings

Setting	Description
Unlocked	Registers the endpoint to the SIP server.
Locked	The endpoint is unavailable for normal operation. It cannot be used to make and/or receive calls.

2. Select a temporary state for each endpoint in the corresponding *Action* column.

This command locks/unlocks an endpoint of the Aastra unit. This state is kept until you modify it or the unit restarts. It offers the following settings:

Table 24: Action Settings

Setting	Description
Force Lock	Cancels the endpoint registration to the SIP server. All active calls in progress are terminated immediately. No new calls may be initiated.
Lock	Cancels the endpoint registration to the SIP server. Active calls in progress remain established until normal call termination. No new calls may be initiated.
Unlock	Registers the endpoint to the SIP server.

3. If you do not need to set other parameters, click *Submit*.

Administration

The Administration section allows you to define endpoint operational state.

▶ **To set administration parameters:**

1. In the *Administration* section of the *Endpoints* page, set the *Disable Unit (All Endpoints) When No Gateways Are In State Ready* drop-down menu with the proper behaviour.

Figure 18: Administration Section

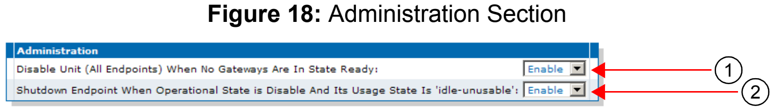


Table 25: Unit Operational State Parameters

Parameter	Description
Disable	Signaling gateways have no impact on the unit operational state

Table 25: Unit Operational State Parameters (Continued)

Parameter	Description
Enable	When all signaling gateways are not ready, the unit operational state is set to disabled.

2. Set the *Shutdown Endpoint When Operational State is Disable And Its Usage State Is 'idle-unusable'* drop-down menu with the proper behaviour.

Table 26: Endpoint Shutdown Parameters

Parameter	Description
Enable	When the usage state becomes “Idle-unusable” and the operational state becomes “Disable”, the endpoint is physically shutdown.
Disable	When an endpoint's usage state becomes “Idle-unusable” whatever the value of its operational state, the endpoint remains physically up but the calls are denied.

The default value is:

- **Enable** for the Aastra series

3. Click *Submit* if you do not need to set other parameters.

Unit Shutting Down Behaviour

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

You can configure the behaviour of the call permissions when the UnitAdminState is ShuttingDown.

The following parameters are available:

Table 27: Unit Shutting Down Behaviour Parameters

Parameter	Description
BlockNewCalls	No new requests are accepted once all activity are terminated. Endpoints cannot make and receive calls.
AllowNewCalls	New requests are accepted until all activities are simultaneously terminated. Endpoints can make and receive calls.

To set the unit shutting down behaviour:

1. In the *epAdmMIB*, locate the *UnitConfigGroup* folder.
2. Set the `behaviorWhileInUnitShuttingDownState` variable with the proper behaviour.

   You can also use the following line in the CLI or a configuration script:

   ```
   epAdm.behaviorWhileInUnitShuttingDownState="Value"
   ```

   where *Value* may be one of the following:

Table 28: Unit Shutting Down Behaviour Values

Value	Meaning
100	BlockNewCalls

Table 28: Unit Shutting Down Behaviour Values (Continued)

Value	Meaning
200	AllowNewCalls

CHAPTER

7

Syslog Configuration

This chapter describes how the Aastra unit. handles syslog messages and notification messages.

For a list and description of all syslog messages and notification messages that the Aastra unit may send, refer to the *Notification Reference Guide*.

Syslog Daemon Configuration

Standards Supported	• RFC 3164: The BSD Syslog Protocol

The Syslog daemon is a general purpose utility for monitoring applications and network devices with the TCP/IP protocol. With this software, you can monitor useful messages coming from the Aastra unit. If no Syslog daemon address is provided by a DHCP server or specified by the administrator, no messages are sent.

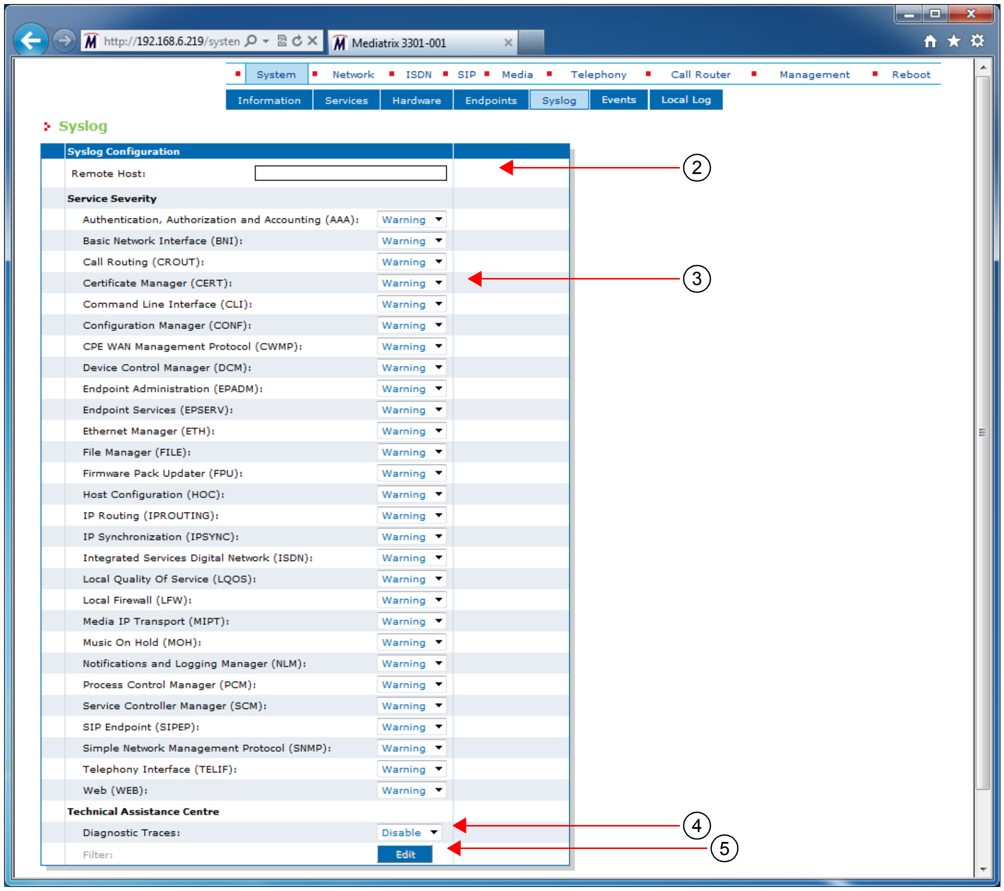
For instance, if you want to download a new firmware into the Aastra unit, you can monitor each step of the firmware download phase. Furthermore, if the unit encounters an abnormal behaviour, you may see accurate messages that will help you troubleshoot the problem.

The Aastra unit supports RFC 3164 as a “device” only (see definition of device in section 3 of the RFC).

▶ To configure the Aastra unit syslog client:

1. In the web interface, click the *System* link, then the *Syslog* sub-link.

Figure 19: System – Syslog Web Page



2. Set the static IP address or domain name and port number of the device to use to archive log entries in the *Remote Host* field.

Use the special port value zero to indicate the protocol default. For instance, the TFTP default port is 69 and the HTTP/HTTPS default port is 80.

3. In the *Service Severity* section, select the minimal severity to issue a notification message for the various services in the corresponding drop-down menus.

Any syslog message with a severity value greater than the selected value is ignored. Available values are:

Table 29: Severity Values

Severity	Description	Notification Messages Issued
Disable	N/A	No notification is issued.
Debug	Message describing in detail the unit's operations.	All notification messages are issued.
Info	Message indicating a significant event for the unit's normal operations.	Notification messages with severity “Informational” and higher are issued.
Warning	Message indicating an abnormal event or situation that could be potentially risky. The unit may not be fully operational.	Notification messages with severity “Warning” and higher are issued.

Table 29: Severity Values (Continued)

Severity	Description	Notification Messages Issued
Error	Message indicating an abnormal event or situation, the system's operation is affected. The unit may not be operational.	Notification messages with severity “Error” and higher are issued.
Critical	Message indicating a critical event or situation that requires immediate attention. The unit is not operational.	Notification messages with severity “Critical” are issued.

A higher level mask includes lower level masks, e.g., *Warning* includes *Error* and *Critical*. The default value is **Warning**.

4. In the *Technical Assistance Centre* section, enable diagnostic traces by setting the *Diagnostic Traces* drop-down menu to **Enable**.

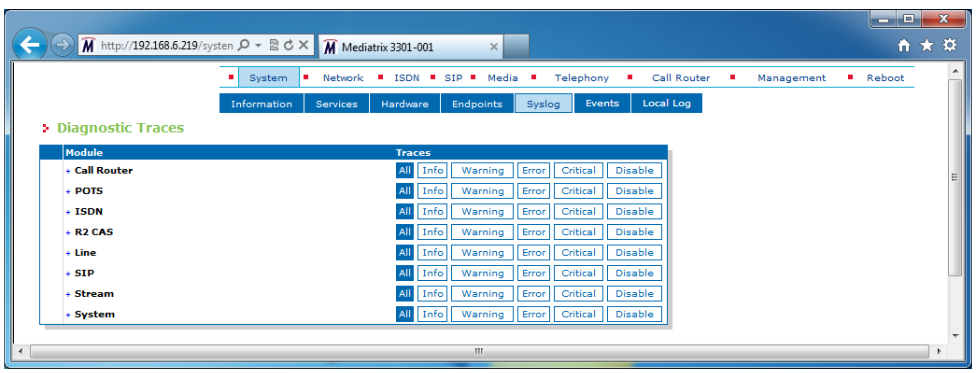
   At the request of Aastra’s Technical Support personnel, enabling these traces will allow Aastra to further assist you in resolving some issues. However, be advised that enabling this feature issues a lot of messages to the syslog host. These messages may be filtered by using the *Diagnostic Traces Filter* field.

> **Note:** Enabling all the traces could affect the performance of the Aastra unit.

5. If applicable, define the filter applied to diagnostic traces by clicking the **Edit** button in the *Filter* field.

   The following opens:

Figure 20: Diagnostic Traces Window



You can use the filter to narrow down the number of traces sent at the request of Aastra´s Technical Support personnel.

6. Click *Submit* if you do not need to set other parameters.

Configuring PCM Capture

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

Aastra Technical Support personnel may ask you to enable the PCM traces. PCM traces are an efficient tool to identify problems with:

- Echo in your network
- DTMF signals
- Caller ID signals
- Fax signals (or false Fax detection)
- Message Waiting Indicator signals
- Any other analog or digital signal

The PCM traces are two different RTP streams made specifically to record all analog signals that are either sent or received on the analog side of the Aastra unit. Only the configured port, port #1 and/or #2, are sending the PCM traces for a maximum of four simultaneous RTP streams.

The RTP streams are sent to a configurable IP address, normally an IP address on your network where it can be recorded with a packet sniffer (such as Wireshark). Moreover, they are independent from the regular RTP streams of the VoIP call.

PCM capture supports sending streams with a ptime higher than 20 ms. The Aastra unit does not support sending streams with a ptime of 10 ms.

To enable PCM capture:

1. In the *miptMIB*, locate the *pcmCaptureGroup* folder under the *debugGroup* folder.
2. Set the `pcmCaptureEnable` variable to **enable**.

   You can also use the following line in the CLI or a configuration script:

   ```
   mipt.pcmCaptureEnable="1"
   ```
3. Set the unit's endpoint on which the PCM capture must be performed in the `pcmCaptureEndpoint` variable.

   You can also use the following line in the CLI or a configuration script:

   ```
   mipt.pcmCaptureEndpoint="Value"
   ```

   The format is `InterfaceName-Channel#`. For digital interfaces (such as ISDN), you must append a `-Channel#` for the requested channel.

   The list of endpoints is available under EpAdm.EndpointTable. Valid examples (depending of the platform) are:

   - PCM capture is to be done on channel #3 of a PRI interface located in slot #2: Slot2/E1T1-3
   - PCM capture is to be done on channel #2 of a BRI interface: Bri1-2
   - PCM capture is to be done on the 16th FXS port: Port16

> **Note:** Note that PCM capture does not support capturing on multiple endpoints simultaneously.

4. Set the IP address where the captured PCM packets should be sent in the `pcmCaptureIpAddr` variable.

   You can also use the following line in the CLI or a configuration script:

   ```
   mipt.pcmCaptureIpAddr="Value"
   ```

The PCM traces destination must be set so it can be recorded in a Wireshark capture on your network, normally sent to the PC doing the capture.

Configuring the Syslog Daemon Application

You must configure the Syslog daemon server to capture those messages. Refer to your Syslog daemon's documentation to learn how to properly configure it to capture messages.

CHAPTER

8

Events Configuration

This chapter describes how to associate a NOTIFICATION message and how to send it (via syslog or via a SIP NOTIFY packet).

For a list and description of all syslog messages and notification messages that the Aastra unit may send, refer to the *Notification Reference Guide*.

Notification Events

You can configure an event router in order to apply a set of rules to select the proper transport protocol scheme. A rule entry is made up of three different values: type, criteria and action.

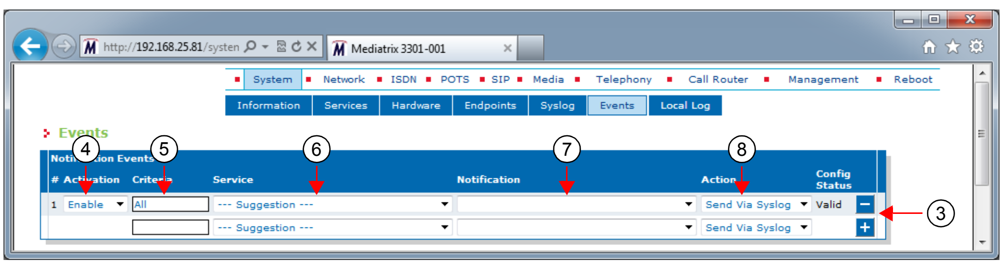
Note that more than one notification may be sent for a single event based on the event router table rules.

▶ **To configure notification events:**

1. Ensure that the severity level for all services are set according to the severity level of the notification messages that are required by the system administrator. See “Chapter 7 - Syslog Configuration” on page 71 for more details.

2. In the web interface, click the *System* link, then the *Events* sub-link.

Figure 21: System – Events Web Page



3. If you want to add a rule entry before an existing entry, locate the proper row in the table and click the + button of this row.

4. Set the *Activation* drop-down menu with the current activation state for the corresponding system event.

Table 30: Activation Parameters

Parameter	Description
Enable	This action is enabled for this system event.
Disable	This action is disabled for this system event.

5. Optional: Set the corresponding *Criteria* field with the expression an event must match in order to apply the specified action. The expression is based on the event type.

   This step is optional because a proper value may be automatically entered by the Aastra unit upon setting the *Service* (Step 5) and *Notification* (Step 6) drop-down menus.

An event of type notification uses the notification ID as expression criteria. The notification ID is the combination of the service number key and the message number key separated by a dot. The information regarding the service and message number key is available in the *Notification Reference Guide* document.

Several basic criteria can also be specified on the same line, separated by commas. Criteria can specify inclusion or exclusion. A group of exclusion criteria can follow the group of inclusion criteria. The group of exclusion criteria must begin with a hyphen (-).

Matching an inclusion criteria causes the action to be executed unless an exclusion criteria is also matched. Exclusion criteria have precedence over inclusion criteria.

Spaces are allowed before or after a basic criterion; however, spaces are not accepted within a basic criterion, i.e. before or after the dot.

Examples:

```
Service ISDN (number key = 1850)
Message %1$s: Physical link state changed to up (number key = 5)
```

The corresponding *Criteria* is: **1850.5**

You can also use the special expression **All**, which means all available services and messages.

```
Criteria 1850.All,1600.200,1600.W,-1850.500,1600.300
```

1850.All,1600.200,1600.W are inclusion criteria and **-1850.500,1600.300** are exclusion criteria. All notifications from service 1850, except notification 500, will match the expression. All notifications from service 1600 with Warning level, except notification 300, will match the expression. Notification 200 from service 1600 will match the expression, no matter the severity level.

6. In the corresponding *Service* drop-down menu, select the service for which you want to send events.

   You can use the *Suggestion* column's drop-down menu to select between suggested values, if any.

7. In the *Notification* drop-down menu, select the notification message that you want to send.

   You can use the *Suggestion* column's drop-down menu to select between suggested values, if any.

8. In the *Action* drop-down menu, select the action to apply to the system event if the criteria matches.

   The action represents a transport targeted for the event. The format of the event under which the message is carried is dependent on the protocol in use.

   The possible actions are:

Table 31: Action Parameters

Parameter	Description
Send Via Syslog	The event notification is sent using syslog as transport. See "Chapter 7 - Syslog Configuration" on page 71 for more details.
Send Via SIP	The event notification is sent using SIP Notify as transport.
Log Locally	The event notification is logged in Local Log.

9. Click the **Submit** button.

   The configuration status of the row displays on the right part of the row. It indicates whether the configuration of the row is valid.

Table 32: Configuration Status Values

Value	Description
Valid	The current content of the fields *Type*, *Criteria* and *Action* is valid.
Invalid	The current content of the fields *Type*, *Criteria* and *Action* is not valid.

Table 32: Configuration Status Values (Continued)

Value	Description
Not Supported	The current content of the fields *Type*, *Criteria* and *Action* is valid but not supported.

Deleting a Rule

You can delete a rule row from the table in the web interface.

▶ **To delete a rule entry:**

1. Click the − button of the row you want to delete.
2. Click the **Submit** button.

Monitoring Parameters

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

You can set two monitoring parameters for the Notification Events table.

▶ **To set monitoring parameters:**

1. In the *sipEpMIB*, locate the *MonitoringGroup* folder.
2. Set the `sipNotificationsGateway` variable with the SIP gateway used to send SIP NOTIFY containing the notification events.

   You can also use the following line in the CLI or a configuration script:

   ```
   sipEp.sipNotificationsGateway="Value"
   ```

   Value is the name of the SIP gateway from which the NOTIFICATION is sent.
3. Set the `maxNotificationsPerNotify` variable with the maximal number of notification events the device may have to send in one SIP NOTIFY request.

   Notifications are sent in XML elements through the SIP NOTIFY's body request.
   You can also use the following line in the CLI or a configuration script:

   ```
   sipEp.maxNotificationsPerNotify="Value"
   ```

   Value may be between 1 and 25.

CHAPTER
9

Local Log

This chapter describes local log status and entries for your Aastra unit.

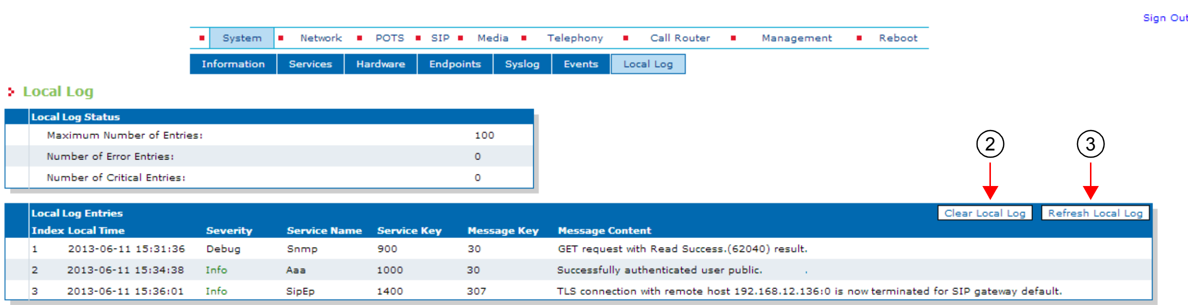
Local Log Status and Entries

You can display, clear and refresh local log status and entries.

▶ **To manage local log status and entries:**

1. In the web interface, click the *System* link, then the *Local Log* sub-link.

Figure 22: System – Local Log Web Page



The following is the *Local Log Status* information displayed.

Table 33: *Local Log Status* Parameters

Parameter	Description
Maximum Number of Entries	Maximum number of entries that the local log can contain. When adding a new entry while the local log is full, the oldest entry is erased to make room for the new one.
Number of Error Entries	Current number of error entries in the local log.
Number of Critical Entries	Current number of critical entries in the local log.

The following is the *Local Log Entries* information displayed.

Table 34: *Local Log Entries* Parameters

Parameter	Description
Local Time	Local date and time at which the log entry was inserted. Format is YYYY-MM-DD HH:MM:SS.
Severity	Severity of the log entry.
Service Name	Textual identifier of the service that issued the log entry.
Service Key	Numerical identifier of the service that issued the log entry.
Message Key	Numerical identifier of the notification message.
Message Content	The readable content of the log message.

2. Click *Clear Local Log* to clear all log entries.
3. Click *Refresh Local Log* to refresh the log entries display.

Network Parameters

Page Left Intentionally Blank

CHAPTER 10

IPv4 vs. IPv6

This chapter describes the differences between IPv4 and IPv6 addressing.

Introduction

IPv6 (Internet Protocol version 6) is the successor to the most common Internet Protocol today (IPv4). This is largely driven by the fact that IPv4's 32-bit address is quickly being consumed by the ever-expanding sites and products on the internet. IPv6's 128-bit address space should not have this problem for the foreseeable future.

IPv6 addresses, in addition to being longer, are distinguished from IPv4 addresses by the use of colons ":", e.g., 2001:470:8929:4000:201:80ff:fe3c:642f. An IPv4 address is noted by 4 sets of decimal numbers separated by periods ".", e.g., 192.168.10.1.

Please note that IPv6 addresses should be written between [ ] to allow port numbers to be set. For instance: [fd0f:8b72:5::1]:5060.

IPv4 vs. IPv6 Availability

The Aastra unit fully supports IPv4 IP addresses, as well as IPv6 IP addresses in some of its features. The following table lists all the network related features of the Aastra unit with their availability in IPv4 and IPv6.

Table 35: IPv4 vs. IPv6 Availability

Feature	IPv4	IPv6
Backup/Restore transfer	✓	✓
Command Line Interface (CLI)	✓	✓
Configuration file transfer	✓	✓
Embedded DHCP server	✓	
Firmware Transfer	✓	✓
IP Routing	✓	
IP Sync	✓	
Link Layer Discovery Protocol (LLDP) QoS settings	✓	
Local Firewall (LFW)	✓	
Network Address Translation (NAT)	✓	
Network Configuration (IP addresses, DNS and SNTP servers)	✓	✓
Network Firewall (NFW)	✓	
Online Certificate Status Protocol (OCSP)	✓	
Remote Authentication Dial In User Service (Radius)	✓	
SIP signaling and media transport	✓	✓
Simple Network Management Protocol (SNMP)	✓	

Table 35: IPv4 vs. IPv6 Availability (Continued)

Feature	IPv4	IPv6
TR-069	✓	
WEB Configuration	✓	✓

If you configure the Aastra unit with IPv6 addresses, then decide to go downgrade to a firmware version that does not support IPv6, all IPv6 networks are deleted.

Please note that IPv6 addresses should be written between [ ]. For instance: [fd0f:8b72:5::1].

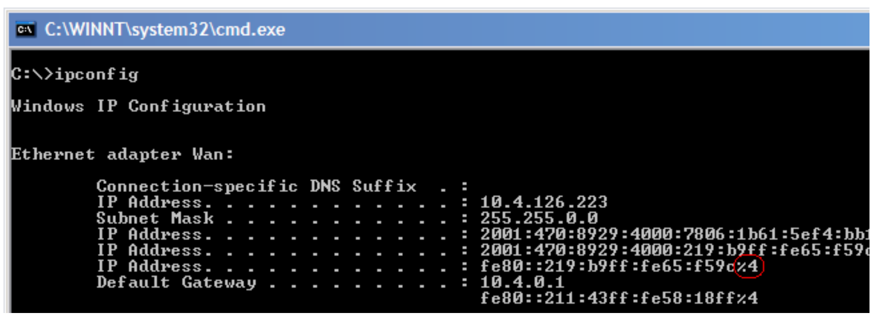
IPv6 Scope Identifier

When using an IPv6 address starting with "FE80::" (IPv6 link-local addresses), there must be additional information: the IPv6 scope identifier (this represents the network link that will be used to contact the IPv6 link-local address). The format is "[IPv6 link-local%ScopeIdentifier]".

When Contacting the unit using its IPv6 link-local Address

On Windows, the scope identifier is represented by an interface number. The interface number can be determined through the command line of Windows.

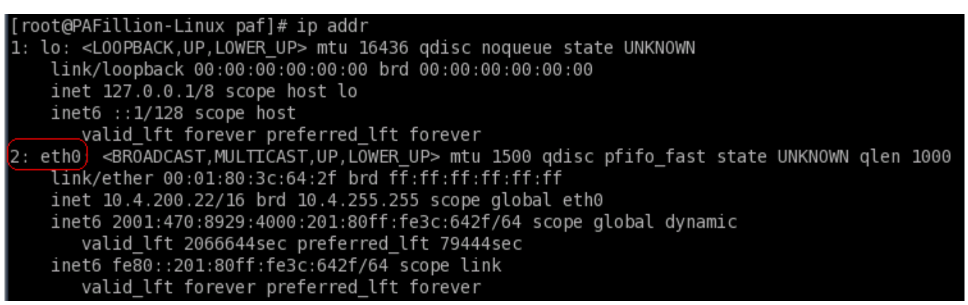
- Go to *Start* -> *Run* and type **cmd** to enter the command prompt.
- At the command prompt, type **ipconfig** and find the IPv6 address. Appended to the end of this will be a "**%x**" where x is the interface number.



To contact the IPv6 link-local IPv6 address "fe80::201:80ff:fe3c:642f", you would use:

```
[fe80::201:80ff:fe3c:642f%4]
```

On Linux, the scope identifier may be the link name or the interface number. The interface number can be determined through the Linux command line.



To contact the IPv6 link-local IPv6 address "fe80::201:80ff:fe3c:642f", you would use:

```
[fe80::201:80ff:fe3c:642f%2] or [fe80::201:80ff:fe3c:642f%eth0]
```

When Configuring the Aastra unit to use an IPv6 link-local Address

In that case, the scope identifier represents the "link" in Network/Interfaces.

For instance, if you want your unit to contact a server with the address IPv6 link-local "fe80::201:80ff:fe3c:642f", you must check on which network link the server is available. Some units have "wan" or "lan". Let’s say it is on the "wan" link. The IP address whoud then become "[fe80::201:80ff:fe3c:642f%wan]".

CHAPTER

11

Host Parameters

This chapter describes how to set the host information of the Aastra unit:

- General Configuration (automatic configuration interface)
- Host name and domain name.
- Default gateway parameters.
- DNS parameters.
- SNTP client parameters.
- Time parameters.

General Configuration

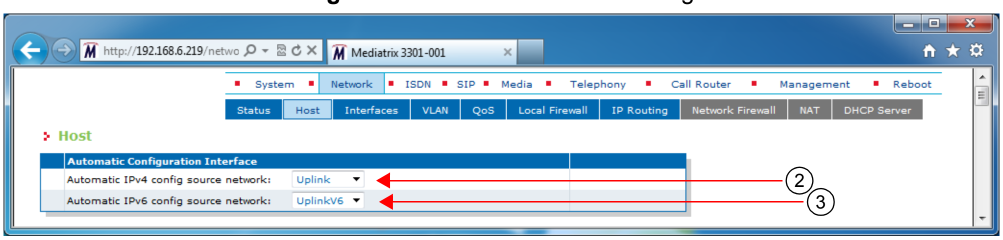
The *General Configuration* section allows you to configure the networks that will provide the automatic configuration (host name, default gateway, DNS servers and SNTP servers) used by the Aastra unit.

Automatic configuration may be provided via IPv4 (DHCPv4) and/or via IPv6 (stateless auto-configuration and DHCPv6).

To set the general configuration:

1. In the web interface, click the *Network* link, then the *Host* sub-link.

Figure 23: Network – Host Web Page



2. Set the *Automatic IPv4 config source network* drop-down menu with the IPv4 network interface that provides the automatic configuration.
3. Set the *Automatic IPv6 config source network* drop-down menu with the IPv6 network interface that provides the automatic configuration.
4. Click *Submit* if you do not need to set other parameters.

   The current automatic configuration interface is displayed in the *Status* page.

Host Configuration

The *Host Configuration* section allows you to configure the host name and domain name of the Aastra unit.

▶ To set the host configuration:

1. In the *Host Configuration* section of the *Host* page, select the configuration source of the domain name information in the *Domain Name Configuration Source* drop-down menu.

Figure 24: Host Name Configuration Section

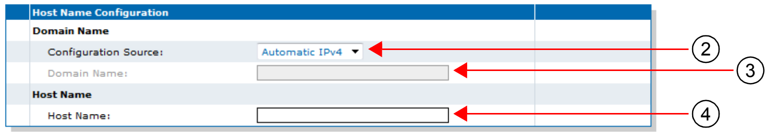


Table 36: Host Name Configuration Sources

Source	Description
Automatic IPv4	The domain name is automatically obtained from the network. The value obtained depends on the connection type of the automatic network interface (see "General Configuration" on page 75) if any. Using the automatic configuration assumes that you have properly set your network server with the relevant information. **Note:** Some Uplink connection types (for example *Static* and *PPPoE*) cannot obtain domain name information from the network, and therefore lead to no domain name being applied to the system.
Automatic IPv6	The domain name is automatically obtained from the IPv6 network defined in the *Automatic IPv6 config source network* drop-down menu.
Static	You manually enter the domain name and it remains the same every time the Aastra unit restarts. Use the static configuration if you are not using a network server or if you want to bypass it.

When switching from the Static to Automatic IPv4 or Automatic IPv6 configuration source, the last value correctly obtained from the network (if any) is applied to the system.

Static Configuration Source Only

2. Set the system's domain name in the *Domain Name* field.

A domain name is a name of a device on the Internet that distinguishes it from the other systems on the network. For instance: example.com.

3. Set the system's host name in the *Host Name* field.

The host name is the unique name by which the device is known on a network. It may contain any of the following characters:

- A to Z and a to z letters
- 0 to 9 digits
- -._~
- !$&'()*+=

Certain restrictions apply to this name:

- The host name must be shorter than 64 characters.
- The host name must not start with a period.
- The host name must not contain double quotes, semicolons, curly braces, spaces, and commas.
- The host name must not contain the following characters: :/?#[@

4. Click *Submit* if you do not need to set other parameters.

The current domain name is displayed in the *Status* page.

Default Gateway Configuration

The default gateway (also known as default router) is the gateway to which the Aastra unit sends packets when all other internally known routes have failed.

▶ **To set the default gateway configuration:**

IPv4 Configuration

1. In the *Default Gateway Configuration – IPv4* section of the *Host* page, select the IPv4 configuration source of the default gateway information in the *Configuration Source* drop-down menu.

Figure 25: Default Gateway Configuration Section

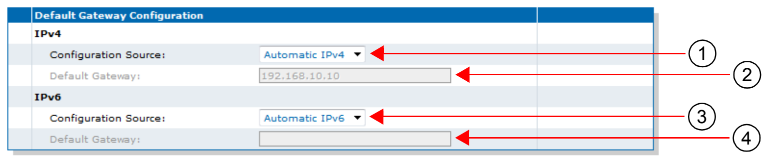


Table 37: Default Gateway Configuration Sources

Source	Description
Automatic IPv4	The default gateway is automatically obtained from the network. The value obtained depends on the connection type of the automatic network interface (see "General Configuration" on page 75) if any. Using the automatic configuration assumes that you have properly set your network server with the relevant information. **Note:** Some Uplink connection types (for example *Static*) cannot obtain default gateway information from the network, and therefore lead to no default gateway being applied to the system.
Static	You manually enter the IP address of the default gateway and it remains the same every time the Aastra unit restarts. Use the static configuration if you are not using a network server or if you want to bypass it.

When switching from the Static to Automatic configuration source, the last value correctly obtained from the network (if any) is applied to the system.

IPv4 Static Configuration Source Only

2. If the default gateway configuration source is **Static,** enter the static default gateway address in the *IP address* field.

This can be an IP address or domain name. The default value is **192.168.10.10**.

IPv6 Configuration

3. In the *Default Gateway Configuration – IPv6* section of the *Host* page, select the IPv6 configuration source of the default gateway information in the *Configuration Source* drop-down menu.

Table 38: IPv6 Default Gateway Configuration Sources

Source	Description
Automatic IPv6	The default gateway name is automatically obtained from the IPv6 network defined in the *Automatic IPv6 config source network* drop-down menu.
Static	You manually enter the IPv6 address of the default gateway and it remains the same every time the Aastra unit restarts. Use the static configuration if you are not using a network server or if you want to bypass it.

When switching from the Static to Automatic IPv6 configuration source, the last value correctly obtained from the network (if any) is applied to the system.

4. If the default gateway configuration source is **Static,** enter the static default gateway IPv6 address in the *IP address* field.

   This can be an IP address or domain name.

5. Click *Submit* if you do not need to set other parameters.

   The current default gateway address is displayed in the *Status* page.

DNS Configuration

Standards Supported	• RFC 1034: Domain Names - Concepts and Facilities • RFC 1035: Domain Names - Implementation and Specification • RFC 1886: DNS Extensions to support IP version 6 • RFC 2181: Clarifications to the DNS Specification

You can use up to four Domain Name Servers (DNS) to which the Aastra unit can connect. The DNS servers list is the ordered list of DNS servers that the Aastra unit uses to resolve network names. DNS query results are cached on the system to optimize name resolution time.

To set the DNS configuration:

1. In the *DNS Configuration* section of the *Host* page, select the configuration source of the DNS information in the *Configuration Source* drop-down menu.

Figure 26: DNS Configuration Section

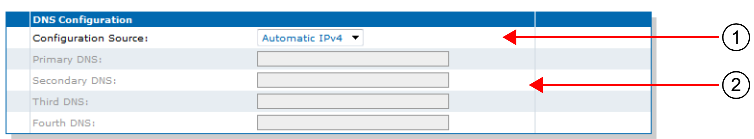


Table 39: DNS Configuration Sources

Source	Description
Automatic IPv4	The DNS servers are automatically obtained from the network. The value obtained depends on the connection type of the automatic network interface (see "General Configuration" on page 75) if any. Using the automatic configuration assumes that you have properly set your network server with the relevant information. **Note:** Some Uplink connection types (for example *Static*) cannot obtain DNS information from the network, and therefore lead to no DNS servers being applied to the system.
Automatic IPv6	The DNS servers are automatically obtained from the IPv6 network defined in the *Automatic IPv6 config source network* drop-down menu.
Static	You manually enter up to four DNS servers IP addresses and they remain the same every time the Aastra unit restarts. Use the static configuration if you are not using a network server or if you want to bypass it.

When switching from the Static to Automatic IPv4 or Automatic IPv6 configuration source, the last values correctly obtained from the network (if any) are applied to the system.

Static Configuration Source Only

2. If the DNS configuration source is **Static,** enter up to four static DNS addresses in the following fields:

- Primary DNS
- Secondary DNS
- Third DNS
- Fourth DNS

3. Click *Submit* if you do not need to set other parameters.

The current list of DNS servers is displayed in the *Status* page.

SNTP Configuration

Standards Supported	• RFC 2030: Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI • bootp-dhcp-option-88

The Simple Network Time Protocol (SNTP) enables the notion of time (date, month, time) into the Aastra unit. SNTP is used to synchronize a SNTP client with a SNTP or NTP server by using UDP as transport. It updates the internal clock of the unit to maintain the system time accurate. It is required when dealing with features such as the caller ID.

The Aastra unit implements a SNTP version 3 client.

Note: The Aastra unit hardware does not include a real time clock. The unit uses the SNTP client to get and set its clock. As certain services need correct time to work properly (such as HTTPS), you should configure your SNTP client with an available SNTP server in order to update and synchronise the local clock at boot time.

▶ **To set the SNTP client of the** Aastra unit**:**

1. In the *SNTP Configuration* section of the *Host* page, select the configuration source of the SNTP information in the *Configuration Source* drop-down menu.

Figure 27: SNTP Configuration Section

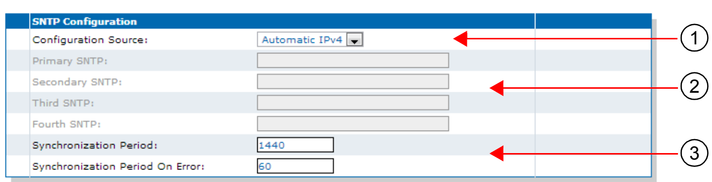


Table 40: SNTP Configuration Sources

Source	Description
Automatic IPv4	The SNTP parameters are automatically obtained from the network. The value obtained depends on the connection type of the automatic network interface (see “General Configuration” on page 75) if any. Using the automatic configuration assumes that you have properly set your network server with the relevant information. **Note:** Some Uplink connection types (for example *Static* and *PPPoE*) cannot obtain SNTP information from the network, and therefore lead to no SNTP parameters being applied to the system.
Automatic IPv6	The SNTP parameters are automatically obtained from the IPv6 network defined in the *Automatic IPv6 config source network* drop-down menu.

Table 40: SNTP Configuration Sources (Continued)

Source	Description
Static	You manually enter the values and they remain the same every time the Aastra unit restarts. Use the static configuration if you are not using a network server or if you want to bypass it.

When switching from the Static to Automatic IPv4 or Automatic IPv6 configuration source, the last values correctly obtained from the network (if any) are applied to the system.

Static Configuration Source Only

2. If the SNTP configuration source is **Static**, enter up to four static SNTP server IP addresses or domain names and port numbers in the following fields:

- Primary SNTP
- Secondary SNTP
- Third SNTP
- Fourth SNTP

3. Set the synchronization information:

Table 41: SNTP Synchronization Information

Field	Description
Synchronisation Period	Time interval (in minutes) between system time synchronization cycles. Each time this interval expires, a SNTP request is sent to the SNTP server and the result is used to set the system time. The maximum value is set to 1 440 minutes, which corresponds to 24 hours.
Synchronisation Period on Error	Time interval (in minutes) between retries after an unsuccessful attempt to reach the SNTP server. The maximum value is set to 1 440 minutes, which corresponds to 24 hours.

4. Click *Submit* if you do not need to set other parameters.

The current SNTP host is displayed in the *Status* page.

Time Configuration

Standards Supported	• bootp-dhcp-option-88

You can define the current system date and time configured in the unit by specifying in which time zone the unit is located.

If the time seems not valid, verify the SNTP configuration in "SNTP Configuration" on page 79.

▶ **To set the time of the Aastra unit:**

1. In the *Time Configuration* section of the *Host* page, enter a valid string in the *Static Time Zone* field.

Figure 28: Time Configuration Section

The format of the string is validated upon entry. Invalid entries are refused. The default value is:

`EST5DST4,M4.1.0/02:00:00,M10.5.0/02:00:00`

A POSIX string is a set of standard operating system interfaces based on the UNIX operating system. The format of the IEEE 1003.1 POSIX string is defined in the *bootp-dhcp-option-88* Internet draft as:

```
STDOFFSET[DST[OFFSET],[START[/TIME],END[/TIME]]]
```

Refer to the following sub-sections for explanations on each part of the string.

2. Click *Submit* if you do not need to set other parameters.

The current system time is displayed in the *Status* page.

STD / DST

Three or more characters for the standard (STD) or alternative daylight saving time (DST) time zone. Only STD is mandatory. If DST is not supplied, the daylight saving time does not apply. Lower and upper case letters are allowed. All characters are allowed except digits, leading colon (:), comma (,), minus (-), plus (+), and ASCII NUL.

OFFSET

Difference between the GMT time and the local time. The offset has the format *h[h][:m[m][:s[s]]]*. If no offset is supplied for DST, the alternative time is assumed to be one hour ahead of standard time. One or more digits can be used; the value is always interpreted as a decimal number.

The hour value must be between 0 and 24. The minutes and seconds values, if present, must be between 0 and 59. If preceded by a minus sign (-), the time zone is east of the prime meridian, otherwise it is west, which can be indicated by the preceding plus sign (+). For example, New York time is GMT 5.

START / END

Indicates when to change to and return from the daylight saving time. The *START* argument is the date when the change from the standard to the daylight save time occurs; *END* is the date for changing back. If *START* and *END* are not specified, the default is the US Daylight saving time start and end dates. The format for start and end must be **one** of the following:

- **n** where *n* is the number of days since the start of the year from 0 to 365. It must contain the leap year day if the current year is a leap year. With this format, you are responsible to determine all the leap year details.
- **Jn** where *n* is the Julian day number of the year from 1 to 365. Leap days are not counted. That is, in all years – including leap years – February 28 is day 59 and March 1 is day 60. It is impossible to refer to the occasional February 29 explicitly. The *TIME* parameter has the same format as *OFFSET* but there can be no leading minus (-) or plus (+) sign. If *TIME* is not specified, the default is *02:00:00*.
- **Mx[x].y.z** where *x* is the month, *y* is a week count (in which the z day exists) and *z* is the day of the week starting at 0 (Sunday). For instance:

  `M10.4.0`

  is the fourth Sunday of October. It does not matter if the Sunday is in the 4th or 5th week.

  `M10.5.0`

  is the last Sunday of October (5 indicates the last z day). It does not matter if the Sunday is in the 4th or 5th week.

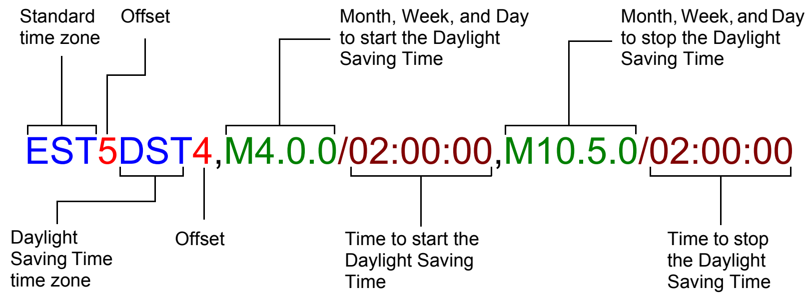
  `M10.1.6`

  is the first week with a Saturday (thus the first Saturday). It does not matter if the Saturday is in the first or second week.

  The *TIME* parameter has the same format as *OFFSET* but there can be no leading minus (-) or plus (+) sign. If TIME is not specified, the default is *02:00:00*.

Example

The following is an example of a proper POSIX string:



The following are some valid POSIX strings:

Table 42: Valid POSIX Strings

Time Zone	POSIX String
Pacific Time (Canada & US)	PST8PDT7,M3.2.0/02:00:00,M11.1.0/02:00:00
Mountain Time (Canada & US)	MST7MDT6,M3.2.0/02:00:00,M11.1.0/02:00:00
Central Time (Canada & US)	CST6CDT5,M3.2.0/02:00:00,M11.1.0/02:00:00
Eastern Time Canada & US)	EST5EDT4,M3.2.0/02:00:00,M11.1.0/02:00:00
Atlantic Time (Canada)	AST4ADT3,M3.2.0/02:00:00,M11.1.0/02:00:00
GMT Standard Time	GMT0DMT-1,M3.5.0/01:00:00,M10.5.0/02:00:00
W. Europe Standard Time	WEST-1DWEST-2,M3.5.0/02:00:00,M10.5.0/03:00:00
China Standard Time	CST-8
Tokyo Standard Time	TST-9
Central Australia Standard Time	CAUST-9:30DCAUST-10:30,M10.5.0/02:00:00,M3.5.0/02:00:00
Australia Eastern Standard Time	AUSEST-10AUSDST-11,M10.5.0/02:00:00,M3.5.0/02:00:00
UTC (Coordinated Universal Time)	UTC0

Additional Parameters

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

Configuring DNS Records Randomization

You can define how the DNS A/AAAA records are accessed from the device's internal DNS cache using the DnsCacheRecordsRandomization variable.

The following values are available:

Table 43: DNS Cache Records Randomization Values

Value	Description
Enable	When DNS A/AAAA records are accessed from the cache, they are sent to requesting service in a randomized order.
Disable	When DNS A/AAAA records are accessed from the cache, they are sent to requesting service in the same order they were originally received from the network. This is the default value.

▶ **To configure DNS Cache records randomization:**

1. In the *hocMIB*, set the `DnsCacheRecordsRandomization` variable.

You can also use the following line in the CLI or a configuration script:

```
hoc.DnsCacheRecordsRandomization="Value"
```

where *Value* may be as follows:

Table 44: DNS Cache Records Randomization Values

Value	Meaning
0	Disable
1	Enable

Configuring Pre-resolved Static FQDNs

You can configure up to 10 pre-resolved FQDNs. The StaticHosts table allows configuring FQDNs with static IP addresses. When a device attempts to reach a FQDN configured in this table, the static IP addresses will be used instead of resolving the FQDN.

The following parameters are available:

Table 45: Static Host Command Parameters

Parameter	Description
Name	Name (FQDN) of the static host. This name must be unique across the table. The name only accepts valid FQDNs as defined by RFC 3986 (Uniform Resource Identifier (URI): Generic Syntax). In addition, strict validation is applied, i.e. the suggested syntax defined in RFC 1035 is enforced.
IpAddresses	List of static IP addresses associated with the FQDN specified in the StaticHosts.Name variable. This list contains numerical IPv4 or IPv6 addresses. IP addresses MUST be separated by a comma (,).
Index	Index in the table. A value of zero (default) causes automatic selection of the largest current index value + 1. If the index value already exists in the table, the insertion is refused. This parameter is optional.

▶ **To insert a new static host:**

1. You can use one of the following lines in the CLI or a configuration script:

```
hoc.InsertStaticHost Index="value" Name="hostname" IpAddresses="address,address1"
hoc.InsertStaticHost Name="hostname" IpAddresses="address,address1"
```

where:

- *value* can be an integer. This is an optional parameter.
- *hostname* is a unique valid FQDN as define by RFC 3986.

- *address* and *address1* are numerical IPv4 or IPv6 addresses separated by a comma.

▶ To delete a static host:

1. In the *hocMIB*, delete the host name using the *Delete* command.
   You can also use one of the following lines in the CLI or a configuration script:
   `hoc.StaticHosts.Delete[Index=value]=Delete`
   where *value* can be an integer.

Updating the "sysname" or "syslocation"

You can specify the name and location of the Aastra unit. This information is for display purposes only and does not affect the behavior of the unit.

▶ To set the sysname and syslocation parameters:

1. In the *hocMIB*, set the system name in the `systemName` variable.
   You can also use the following line in the CLI or a configuration script:
   `hoc.systemName="Value"`
   The value of this variable is also returned by the "sysName" object in SNMPv2-MIB.
2. Set the system location in the `systemLocation` variable.
   You can also use the following line in the CLI or a configuration script:
   `hoc.systemLocation="Value"`
   The value of this variable is also returned by the "sysLocation" object in SNMPv2-MIB.

CHAPTER 12

Interface Parameters

This chapter describes how to set the interfaces of the Aastra unit:

- How to reserve an IP address in a network server.
- Link Connectivity Detection
- Partial Reset
- Managing interfaces.
- PPPoE parameters.
- LLDP Configuration
- Ethernet Link Configuration
- DHCP Server Configuration
- Ethernet Connection Speed
- Configuring a MTU Value

Reserving an IP Address

Before connecting the Aastra unit to the network, Aastra strongly recommends that you reserve an IP address in your network server – if you are using one – for the unit you are about to connect. This way, you know the IP address associated with a particular unit.

Network servers generally allocate a range of IP addresses for use on a network and reserve IP addresses for specific devices using a unique identifier for each device. The Aastra unit unique identifier is its media access control (MAC) address. You can locate the MAC address as follows:

- It is printed on the label located on the bottom side of the unit.
- It is stored in the *Device Info* page of the web interface.
- You can take one of the telephones connected to the Aastra unit and dial ***#*1** on the keypad. The MAC address of the Aastra unit will be stated.

Aastra recommends to reserve an IP address with an infinite lease for each Aastra unit on the network.

Link Connectivity Detection

Each Ethernet port of the Aastra unit is associated with an Ethernet link. This information is available in the *Ethernet Ports Status* section of the *Network / Status* page. A link has connectivity if at least one of its port status is not disconnected.

The link connectivity is periodically polled (every 500 milliseconds). It takes two consecutive detections of the same link state before reporting a link connectivity transition. This avoids reporting many link connectivity transitions if the Ethernet cable is plugged and unplugged quickly.

Partial Reset

When a partial reset is triggered, the Rescue interface is configured and enabled with:

- its hidden IPv4 link configuration values
- its hidden IPv4 address configuration

- an IPv6 link-local address on all network links

Hidden values are set by the unit's profile.

Just before the Rescue is configured, all IPv4 network interfaces that could possibly conflict with the Rescue interface are disabled.

If the BNI Service is stopped when the partial reset occurs, it is started and the above configuration is applied.

Interfaces Configuration

Standards Supported	• IEEE 802.1Q – Virtual Bridged Local Area Networks • RFC 2460: IPv6 • RFC 2464: Transmission of IPv6 Packets over Ethernet Networks • RFC 4193: Unique_local_address • RFC 4291: IP Version 6 Addressing Architecture[a] • RFC 4443: ICMPv6 • RFC 4861: IPv6_neighbor_discovery • RFC 4862: IPv6_stateless_autoconf

a. Site-local address are deprecated.

The *Interface Configuration* section allows you to add and remove up to 48 network interfaces. By default, this section contains the following network interfaces:

- The *Uplink* interface, which defines the uplink information required by the Aastra unit to properly connect to the WAN. The *Uplink* network interface is the IP interface that encapsulates the following link interface (WAN connection):
  - *eth1* (TA7102i), *wan* for the Aastra TA7102i

  By default, this interface uses the IPv4 DHCP connection type.
- The *Rescue* interface, which defines the address and network mask to use to contact the Aastra unit after a partial reset operation. You cannot delete this interface. See "Partial Reset" on page 15 for more details.
- The LAN interface IPv4 address and network mask.

The current status of the network interfaces is displayed in the *Status* page. It allows you to know which interfaces are actually enabled. Enabled networks are activated when their configured link gets connectivity and are deactivated as soon as the link connectivity is lost. See "Link Connectivity Detection" on page 85 for more details.

The *Interfaces Status* section of the *Status* page displays the status of all currently enabled network interfaces, including interfaces with an invalid configuration or waiting for a response.

When configuring network interfaces, Aastra recommends to have a syslog client properly configured and enabled in order to receive any message related to the network interfaces behaviour. The interface used to access the syslog client must also be properly enabled. See "Chapter 7 - Syslog Configuration" on page 71 for more details on enabling a syslog client.

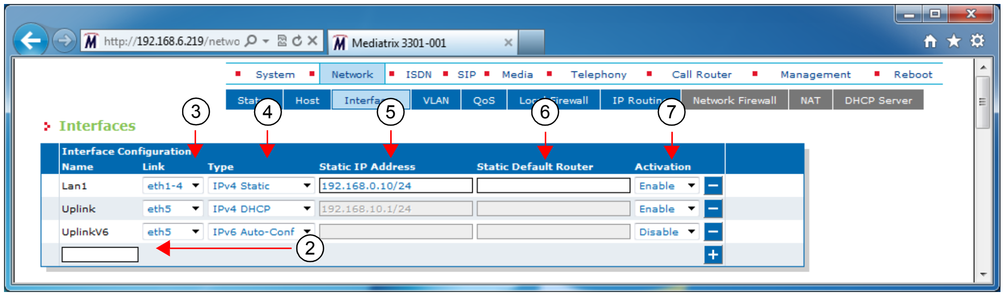
Caution: Use extreme care when configuring network interfaces, especially when configuring the network interface used to contact the unit for management. Be careful never to disable or delete the network interface used to contact the unit. Also be careful to always set the unit's management interface to be an interface that you can contact.

Note: When performing a partial reset (see "Partial Reset" on page 15 for more details), the management interface used for SNMP, CLI and WEB is automatically set to the *Rescue* interface. In that case, you must change the Aastra unit system management network interface to something other than *Rescue*. Note that you must be able to contact the interface you select.

▶ To configure interfaces parameters:

1. In the web interface, click the *Network* link, then the *Interfaces* sub-link.

Figure 29: Network – Interfaces Web Page



2. If you want to add a new interface, enter its name in the blank field in the bottom left of the window, then click the button.

   The name is case-sensitive. Using the special value “All” is not allowed.

   You can use the following ASCII codes in the network interface name:

49 1	77 M	103 g
50 2	78 N	104 h
51 3	79 O	105 i
52 4	80 P	106 j
53 5	81 Q	107 k
54 6	82 R	108 l
55 7	83 S	109 m
56 8	84 T	110 n
57 9	85 U	111 o
65 A	86 V	112 p
66 B	87 W	113 q
67 C	88 X	114 r
68 D	89 Y	115 s
69 E	90 Z	116 t
70 F	95 _, underscore	117 u
71 G	97 a	118 v
72 H	98 b	119 w
73 I	99 c	120 x
74 J	100 d	121 y
75 K	101 e	122 z
76 L	102 f	

   A valid network interface name must be compliant with the following rules:

   - It must start with a letter
   - It cannot contain characters other than letters, numbers, underscores.

   If your Aastra unit contains an invalid interface name created in a previous firmware version without the validation feature, the invalid interface name will be modified everywhere it appears on the first restart and a syslog notification will be sent.

   You can also delete an existing network interface by clicking the corresponding button. You cannot delete the *Rescue* interface.

3. In the *Interface Configuration* section, select the link on which to activate the interface in the *Link* column.

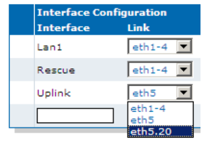
   A VLAN is listed with the following syntax:

   `Link.VLAN ID`

   For instance, if you have added VLAN 20 on the interface eth5, it is listed as follows:

   `eth5.20`

Figure 30: VLAN Example



4. Select the configuration source of the interface information in the *Type* drop-down menu.

Table 46: Interface Configuration Sources

Source	Description
IPv4 DHCP	The IPv4 address and network mask are provided by querying a DHCP server and using standard DHCP fields or options. Using the DHCP configuration assumes that you have properly set your DHCP server with the relevant information. DHCP servers may provide a list of IP configuration parameters to use. See “DHCP Server Configuration” on page 95 for more details.
IPv4 Static	You manually enter the IPv4 address and network mask and they remain the same every time the Aastra unit restarts. Use the static configuration if you are not using a DHCP server/PPP peer or if you want to bypass it.
IPv4 PPPoE	IPv4 over PPP connection, address and network mask are provided by the PPP peer using IPCP. PPP peers may provide a list of IP configuration parameters to use. See “PPPoE Configuration” on page 91 for more details.
IPv6 Auto-Conf	IPv6 state-less auto-configuration. See “IPv6 Autoconfiguration Interfaces” on page 89 for more details.
IPv6 Static	You manually enter the IPv6 address and network mask and they remain the same every time the Aastra unit restarts. Use the IPv6 static configuration if you are not using IPv6 stateless or stateful auto-configuration or if you want to bypass it.

Note: If no network is configured in IPv6, the unit does not have any IPv6 address, not even the Link-Local address. When a network is configured in IPv6, the Link-Local (FE80 ::...) address is automatically created and displayed in the Network Status information.

5. If the interface configuration source is **IPv4 Static** or **IPv6 Static**, enter the address and network mask (if applicable) of the network interface in the *Static IP address* field.

6. If the interface configuration source is **IPv4 Static** or **IPv6 Static**, set the *Static Default Router* field with the IP address of the default gateway for the network interface.

7. Define whether or not the Aastra unit should attempt to activate the corresponding network interface in the *Activation* drop-down menu.

   It may not be possible to enable a network interface, for instance if another network interface is already enabled in the same subnet. The actual status of network interfaces is shown in the *Status* page.

8. Click *Submit* if you do not need to set other parameters.

   The current network interface information is displayed in the *Status* page.

Table 47: Network Interface Status

Status	Description
Disabled	The interface is not operational because it is explicitly disabled or the link interface is unavailable.
Invalid Config	The interface is not operational because its configuration is not valid.

Table 47: Network Interface Status (Continued)

Status	Description
Network Conflict	The interface is configured with an IP address that is already used on the network.
Link Down	The interface is configured with a link that has no connectivity.
Waiting Response	The interface is not operational because a response from a peer or server is required.
Active	The interface is operational.

IPv6 Autoconfiguration Interfaces

When the *Type* drop-down menu is set to **IPv6 Auto-Conf**, the network interface is an IPv6 over Ethernet connection with IP parameters obtained by stateless auto-configuration or stateful (DHCPv6) configuration.

Autoconfiguration of IPv6 address is first initiated using state-less autoconfiguration. Stateful autoconfiguration is initiated only if one of the following conditions is met:

- The router explicitly required stateful autoconfiguration by setting the “managed” or “other” flag of the router advertisement.
- No router advertisement was received after 3 router solicitations. RFC 4861 defines the number of router solicitations to send and the 4 seconds interval between the sent router solicitations.

Stateless Autoconfiguration

All IPv6 addresses present in the router advertisements are applied to the network interface. Each IPv6 address is assigned a network name based on the configured network name with a suffix in the following format: ConfiguredNetworkName-XX-Y.

XX is the address scope

- GU (Global Unique)
- UL (Unique Local)
- LL (Link-Local)

Y is a unique ID for the address scope.

Spanning Tree Protocol vs Stateless Autoconfiguration

Many network switches use the Spanning Tree Protocol (STP) to manage Ethernet ports activity. STP uses a detection timeout before a router advertisement is sent to the Aastra unit. The default value for this timeout is usually 30 seconds. However, when the unit wants to get an IPv6 address in Stateless autoconfiguration, this timeout is too long and the unit falls into Stateful Autoconfiguration mode <u>before</u> it receives the router advertisement. This results in the unit receiving a DHCPv6 address.

To solve the issue, check if the default STP detection timeout value in your router can be modified. If so, set it to a value of 8 s or less. If you cannot modify the timeout value, Aastra recommends to disable the Spanning Tree Protocol on the network to which the unit is connected.

Stateful Autoconfiguration

Stateful autoconfiguration is managed by DHCPv6. The DHCPv6 lease is negotiated according to RFC 3315 with the limitations listed in section 1.5. DHCPv6 may be used to obtain the following information (depending on the router advertisement flags):

- IPv6 addresses (when the router advertisement “managed” flag is set)
- Other configuration (when the router advertisement “other” flag is set)

If only the “other” flag is set in the router advertisement, the DHCPv6 client only sends an information request to the DHCPv6 server, otherwise it sends a DHCPv6 solicit message. If the flags change over time, only the transitions from “not set” to “set“ are handled.

Network Interface Priority

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

You can prioritize the network interfaces of the Aastra unit. In case of address conflicts between two or more network interfaces, the network interface with the highest priority will remain enabled and the other interfaces will be disabled. If the priority is the same, only the first enabled network interface will be able to use the IP address. When a conflict ends, all network interfaces concerned automatically return to an operational state.

The actual status of network interfaces is displayed in the *Status* web page.

To set the network interface priority:

1. In the *ethMIB*, set the `networkInterfacesPriority` variable with the proper value for the corresponding interface.

   You can also use the following line in the CLI or a configuration script:

   ```
   eth.networkInterfacesPriority="Value"
   ```

   where *Value* may be any number between 0 and 100.

Rescue Interface Configuration

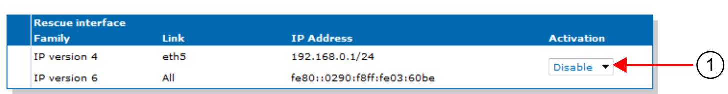
You can define whether or not the Aastra unit should attempt to activate the rescue network interface.

Caution: Please be careful when using this section.

To enable/disable the Rescue interface:

1. In the *Rescue interface* section, define whether or not the Aastra unit should attempt to activate the corresponding network interface in the *Activation* drop-down menu.

   Figure 31: Rescue Interface Configuration Section

   It may not be possible to enable a network interface, for instance if another network interface is already enabled in the same subnet. The actual status of network interfaces is shown in the *Status* page.

2. Click *Submit* if you do not need to set other parameters.

PPPoE Configuration

Standards Supported	• RFC 1332 – The PPP Internet Protocol Control Protocol (IPCP) • RFC 1334 – PPP Authentication Protocols[a] • RFC 1661 – The Point-to-Point Protocol (PPP) • RFC 1877 – PPP Internet Protocol Control Protocol Extensions for Name Server Addresses[b] • RFC 1994 – Challenge Handshake Authentication Protocol (CHAP) • RFC 2516 – A Method for Transmitting PPP Over Ethernet (PPPoE)

a. Section 2 (PAP), section 3 is obsoleted by RFC 1994

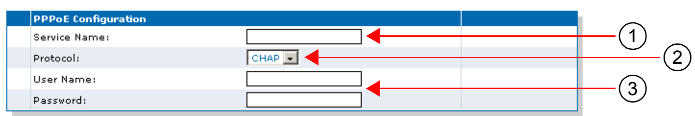
b. Supported except for sections 1.2 and 1.4

The *PPPoE Configuration* section applies only if you have selected the PPPoE connection type in the *Interface Configuration* section of the web page.

▶ **To configure PPPoE parameters:**

1. In the *PPPoE Configuration* section, set the name of the service requested to the access concentrator (AC) when establishing the next PPPoE connection in the *Service Name* field.

Figure 32: PPPoE Configuration Section



This is used as the *Service-Name* field of the packet broadcasted to the access concentrators. See RFC 2516 section 5.1 for details.

The field may be set with any string of characters, with a maximum of 255 characters.

If you leave this field empty, the Aastra unit looks for any access concentrator.

2. Select the authentication protocol to use for authenticating the system to the PPP peer in the *Protocol* drop-down menu.

   - PAP: Use the Password Authentication Protocol.
   - CHAP: Use the Challenge Handshake Authentication Protocol.

3. Set the PPP user name and password that identify the system to the PPP peer during the authentication process in the *User Name* and *Password* fields.

> **Caution:** The *User Name* and *Password* fields are not accessible if you have the User or Observer access right. See “Users” on page 591 for more details.

When connecting to an access concentrator, it may request that the Aastra unit identifies itself with a specific user name and password.

There are no restrictions, you can use any combination of characters.

4. Click *Submit* if you do not need to set other parameters.

The current PPPoE information is displayed in the *Status* page.

PPP Negotiation

When the Aastra unit restarts, it establishes the connection to the access concentrator in conformance with the RFCs listed in “PPPoE Configuration” on page 91.

When establishing a PPP connection, the Aastra unit goes through three distinct phases:

- Discovery phase
- Authentication phase
- Network-layer protocol phase

Discovery Phase

The Aastra unit broadcasts the value of the *Service Name* field.

The access concentrator with a matching service name answers the Aastra unit.

- If no access concentrator answers, this creates a “PPPoE failure” error.
- If more than one access concentrators respond to the discovery, the Aastra unit tries to establish the PPP connection with the first one that supports the requested service name.

Authenthication Phase

If the access concentrator requests authentication, the Aastra unit sends the ID/secret pair configured in the *User Name* and *Password* fields. If the access concentrator rejects the authentication, this creates an “authentication failure” error.

Network-Layer Protocol Phase

The Aastra unit negotiates an IP address. The requested IP address is the one from the last successful PPPoE connection. If the Aastra unit never connected by using PPPoE (or after a factory reset), it does not request any specific IP address.

DHCP Client Identifier Presentation

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

You can define the method to use to present the value of the Client Identifier (Option 61) field through a DHCP request. The following values are available:

Table 48: DHCP Client Identifier Presentation Parameters

Parameter	Description
Disabled	The Client Identifier option is not presented in a DHCP request.
MacAscii	The Client Identifier value is presented as the client MAC address in ASCII format. The MAC address is represented in lowercase.
MacBinary	The Client Identifier value is presented as the client MAC address in binary format.

To define the DHCP client identifier presentation:

1. In the *bniMIB*, locate the *DhcpClientGroup* folder.
2. Set the `dhcpClientIdentifierPresentation` variable with the proper presentation.

   You can also use the following line in the CLI or a configuration script:

   ```
   bni.dhcpClientIdentifierPresentation="Value"
   ```

where *Value* may be one of the following:

Table 49: DHCP Client Identifier Presentation Values

Value	Meaning
100	Disabled
200	MacAscii
300	MacBinary

LLDP Configuration

The Link Layer Discovery Protocol (LLDP) service is used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, usually wired Ethernet.

The *LLDP Configuration* section allows you to configure parameters related to LLDP.

▶ **To configure LLDP parameters:**

1. In the *LLDP Configuration* section, set the network interface name on which LLDP should be enabled in the *Network Interface* drop-down menu.

Figure 33: LLDP Configuration Section

LLDP cannot be activated on multiple network interfaces simultaneously.

2. Select the address type to populate the chassis ID device identifier in the *Chassis ID* drop-down menu.

Table 50: Chassis ID Parameters

Parameter	Description
MAC Address	The MAC address.
Network Address	The IP address (or 0.0.0.0 if DHCP is not obtained yet).

3. Select whether to enable the LLDP-MED protocol override of the VLAN ID, User Priority and DiffServ values in the *Override Network Policy* drop-down menu.

Table 51: Override Network Policy Parameters

Parameter	Description
Enable	The service listens for LLDP advertisements, and overrides the previously configured VLAN ID, User Priority and DiffServ with the values received.
Disable	The service only publishes its characteristics and configurations by LLDP, and does not override anything.

The LLDP-MED (Media Endpoint Discovery) protocol is an enhancement of LLDP.

4. Click *Submit* if you do not need to set other parameters.

The current LLDP information is displayed in the *Status* page.

Ethernet Link Configuration

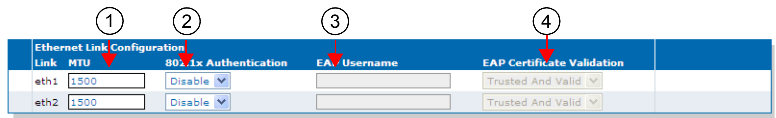
Standards Supported	• IEEE 802.1X-2001 – Port Based Network Access Control

The *Ethernet Link Configuration* section allows you to configure the MTU as well as IEEE 802.1X authentication.

▶ **To configure Ethernet link parameters:**

1. In the *Ethernet Link Configuration* section, set the *MTU* field of a specific Ethernet link with a proper value.

Figure 34: Ethernet Link Configuration Section



The *Maximum Transmission Unit* (MTU) is a parameter that determines the largest packet than can be transmitted by an IP interface (without it needing to be broken down into smaller units). Each interface used by TCP/IP may have a different MTU value specified. See “Appendix C - Maximum Transmission Unit (MTU)” on page 639 for more details on MTU.

The range is from 576 to 1500 bytes. All VLAN connections use the MTU size configured on their related Ethernet link.

Note: The MTU value applied for a PPPoE connection is the smallest of the value negotiated with the server and the value configured here.

2. Define the IEEE 802.1x authentication protocol activation to use for a specific Ethernet link in the corresponding *802.1x Authentication* drop-down menu.

802.1X Authentication is a tag optionally added to the Ethernet frame header to specify the support of the IEEE 802.1X Authentication. It allows getting authorization and access to secured network(s).

Table 52: 802.1x Authentication Parameters

Parameter	Description
Disable	The IEEE 802.1x authentication protocol is disabled on the Ethernet link interface.
Enable	The IEEE 802.1x authentication protocol using the EAP-TLS authentication method is enabled on the Ethernet link to get an access, through an IEEE 802.1x EAP-TLS authenticator (such as an IEEE 802.1x capable network device), to secured network(s). The Ethernet link interface remains always 'UP' whatever the result of the IEEE 802.1x authentication.

3. Set the username used to authenticate each Ethernet link interfaces during the IEEE 802.1x EAP-TLS authentication process in the corresponding *EAP Username* field.

This parameter is used only when the IEEE 802.1x authentication is enabled (*802.1x Authentication* drop-down menu set to **Enabled**).

4. Define the IEEE 802.1x level of validation used by the device to authenticate the IEEE 802.1x EAP-TLS peer's certificate.

This parameter also controls the criteria used to select the host certificate sent during the authentication handshakes..

Table 53: 802.1x Certificate Validation Parameters

Parameter	Description
No Validation	No validation is performed on the peer's certificate. Authentication with the peer is attempted even if the system time is not synchronized. If more than one host certificate is configured for an EAP-TLS usage, the one with the latest expiration date is used.
Trusted And Valid	Allow a connection to the network by validating if the authentication peer's certificate is trusted and valid. The IEEE 802.1x authentication is attempted only if the system time is synchronized. If more than one host certificate is configured for an EAP-TLS usage, the one that is currently valid and with the latest expiration date is used.

5. Click *Submit* if you do not need to set other parameters.

The current status of the network interfaces is displayed in the *Status* page. It allows you to know which interfaces are actually enabled.

Table 54: Ethernet Link Interface State

State	Description
Disconnected	The link interface is physically disconnected.
Up	The link interface is physically connected and considered as usable by network interface(s).

DHCP Server Configuration

Standards Supported	• RFC 2131 – Dynamic Host Configuration Protocol[a] • RFC 2132 – DHCP Options and BOOTP Vendor Extensions[b] • RFC 3315: DHCPv6[c]

a. Supports the client side of the protocol

b. Only sections 3.3, 3.5, 3.8 and 8.3

c. Supports the client side of the protocol

Note: This section applies only if you are using the DHCP connection type ("Interfaces Configuration" on page 86).

DHCP servers generally allocate a range of IP addresses for use on a network and reserve IP addresses for specific devices using a unique identifier for each device. The Aastra unit unique identifier is its media access control (MAC) address.

You can locate the MAC address as follows:

- on the label located on the bottom side of the unit.
- in the *System* > *Information* web page
- you can dial the following digits on a telephone connected to the Aastra unit:

  `*#*1`

  The Aastra unit answers back with its MAC address. This applies to units with FXS interfaces. See "General POTS Configuration" on page 160 for more details.

Aastra recommends to reserve an IP address with an infinite lease for each Aastra unit on the network.

DHCP Negotiation

The DHCP lease is negotiated according to RFC 2131 (supports the client side of the protocol) and RFC 2132 (only sections 3.3, 3.5, 3.8 and 8.3). The following paramaters are set

Table 55: DHCP Parameters

DHCP Parameter	Value
Host Name (option 12)	Set according to the *Host Name* parameter of the *Network > Host* page (“Host Configuration” on page 89). This option cannot be empty according to RFC 2132. If the *Host Name* parameter is empty, the DHCP option 12 is not sent.
Vendor Class Identifier (option 60)	Set according to the *System Description* parameter of the *System > Information* page.
Client identifier (option 61)	Set according to *MAC Address* parameter of the *System > Information*.

Ethernet Connection Speed

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

You can set the speed and duplex of the Ethernet connection of the Aastra unit. The following values are available:

Table 56: Ethernet Ports Speed and Duplex Supported

Parameter	Description
Auto	Automatic negociation of speed and duplex.
Half10	10 Mbit/s Half-duplex.
Full10	10 Mbit/s Full-duplex.
Half100	100 Mbit/s Half-duplex.
Full100	100 Mbit/s Full-duplex.

A half-duplex connection refers to a transmission using two separate channels for transmission and reception, while a full-duplex connection refers to a transmission using the same channel for both transmission and reception.

If unknown, set the variable to **Auto** so that the Aastra unit can automatically detect the network speed.

Caution: Whenever you force a connection speed / duplex mode, be sure that the other device and all other intermediary nodes used in the communication between the two devices have the same configuration. See "Speed and Duplex Detection Issues" on page 98 for more details.

The current speed and duplex configuration is displayed in the *Network* > *Status* page under the *Ethernet Ports Status* section.

To set the Ethernet connection speed and duplex:

1. In the *ethMIB*, locate the *portsTable* folder.
2. Set the `portsSpeed` variable with the proper Ethernet speed and duplex.

   You can also use the following line in the CLI or a configuration script:

   ```
   eth.portsSpeed="Value"
   ```

   where *Value* may be one of the following:

Table 57: Ethernet Ports Speed and Duplex Values

Value	Meaning
100	Auto
200	Half10
300	Full10
400	Half100
500	Full100

Speed and Duplex Detection Issues

There are two protocols for detecting the Ethernet link speed:

- An older protocol called parallel detection.
- A more recent protocol called auto-negotiation (IEEE 802.3u).

The auto-negotiation protocol allows to detect the connection speed and duplex mode. It exchanges capabilities and establishes the most efficient connection. When both endpoints support the auto-negotiation, there are no problems. However, when only one endpoint supports auto-negotiation, the parallel detection protocol is used. This protocol can only detect the connection speed; the duplex mode cannot be detected. In this case, the connection may not be established.

The Aastra unit has the possibility to force the desired Ethernet link speed and duplex mode by disabling the auto-negotiation and selecting the proper setting. When forcing a link speed at one end, be sure that the other end (a hub, switch, etc.) has the same configuration. To avoid any problem, the link speed and duplex mode of the other endpoint must be exactly the same.

CHAPTER
13

VLAN Parameters

This chapter describes how to create and manage dynamic VLANs on the Aastra unit.

VLAN Configuration

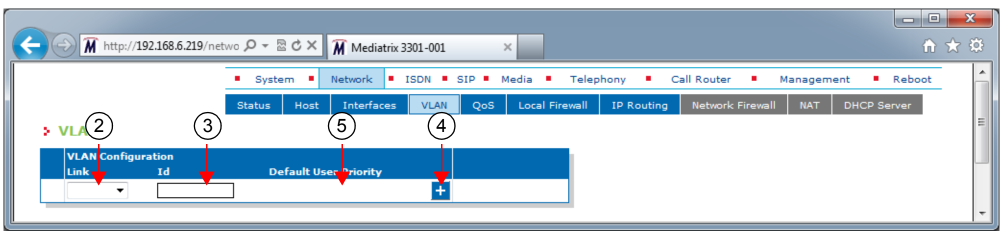
A *virtual LAN* is a network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. You can add VLANs on the Ethernet links of the Aastra unit. You can currently add or manage up to a maximum of 16 VLANs.

Caution: When working with VLANs, take care not to cut your access to the unit, for instance by putting the Uplink on a VLAN to which your PC does not have access and then setting the management interface to Uplink.

▶ **To add a VLAN:**

1. In the web interface, click the *Network* link, then the *VLAN* sub-link.

Figure 35: Network – VLAN Web Page



2. Select the Ethernet link over which the VLAN interface is built in the *Link* drop-down menu.
3. Set the VLAN ID used by the VLAN interface in the *Id* field.

   This is a 12 bit field in the 802.1Q tag carrying an ID that differentiates frames containing this ID from frames containing different IDs or no 802.1Q tag at all.

   To systems supporting Ethernet 802.1Q, frames containing the same VLAN ID are considered as belonging to the same virtual LAN, and frames containing different IDs are considered as not belonging to the same virtual LAN, even though they use the same physical LAN.
4. Click on the + button.
5. Set the default user priority value the interface uses when tagging packets in the *Default User Priority* field.

   You can also set specific service class values in the Quality of Service page. See "Chapter 14 - Local QoS (Quality of Service) Configuration" on page 115 for more details.
6. Click *Submit* if you do not need to set other parameters.

   You can also delete an existing VLAN by clicking the corresponding − button.

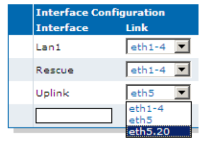
   Once you have added a VLAN, you must select this VLAN on an interface to activate it. You can do so in the *Link* column of the *Interface Configuration* section in the *Network* > *Interfaces* page ("Interfaces Configuration" on page 100). The VLAN is listed with the following syntax:

   `Link.VLAN ID`

   For instance, if you have added VLAN 20 on the interface eth5, it is listed as follows:

   `eth5.20`

Figure 36: VLAN Example



CHAPTER 14

Local QoS (Quality of Service) Configuration

This chapter describes how to configure the local QoS parameters. The local QoS tags packets sent from the Aastra unit. It does not process nor classify packets coming from the network.

Introduction

QoS (Quality of Service) features enable network managers to decide on packet priority queuing. The Dgw v2.0 application supports the Differentiated Services (DS) field and 802.1q taggings.

The Dgw v2.0 application supports the Real Time Control Protocol (RTCP), which is used to send packets to convey feedback on quality of data delivery.

The Dgw v2.0 application does not currently support the Voice Band Data service class. It also does not support RSVP (Resource Reservation Protocol).

Differentiated Services (DS) Field

Standards Supported	RFC 2475: An Architecture for Differentiated Services

Differentiated Services (DiffServ, or DS) is a protocol for specifying and controlling network traffic by class so that certain types of traffic – for example, voice traffic, which requires a relatively uninterrupted flow of data, might get precedence over other kinds of traffic.

What are Differentiated Services?

Differentiated Services avoids simple priority tagging and depends on more complex policy or rule statements to determine how to forward a given network packet. An analogy is made to travel services, in which a person can choose among different modes of travel – train, bus, airplane – degree of comfort, the number of stops on the route, standby status, the time of day or period of year for the trip, and so forth.

For a given set of packet travel rules, a packet is given one of 64 possible forwarding behaviors – known as per hop behaviors (PHBs). A six-bit field, known as the Differentiated Services Code Point (DSCP), in the Internet Protocol header specifies the per hop behavior for a given flow of packets. The DS field structure is presented below:

```
0   1   2   3   4   5   6   7
+---+---+---+---+---+---+---+---+
| DSCP                  |  CU   |
+---+---+---+---+---+---+---+---+
MSB                           LSB
```

- *DSCP*: Differentiated Services CodePoint.
- *CU*: Currently Unused. The CU bits should always be set to 0.

For both signalling and media packets, the DSCP field is configurable independently. The entire DS field (TOS byte) is currently configurable.

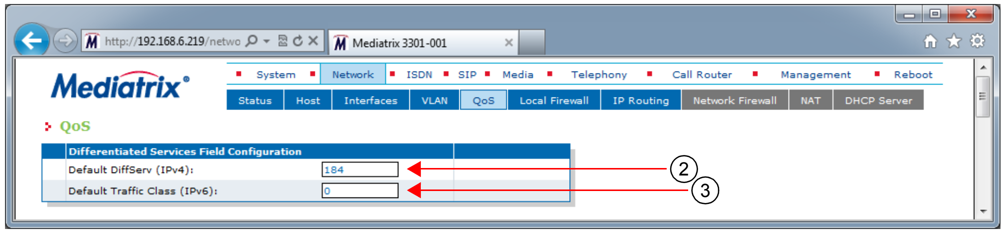
DiffServ replaces the first bits in the ToS byte with a differentiated services code point (DSCP). It uses the existing IPv4 Type of Service octet.

It is the network administrator's responsibility to provision the Aastra unit with standard and correct values.

▶ **To configure the Aastra unit DiffServ value:**

1. In the web interface, click the *Network* link, then the *QoS* sub-link.

Figure 37: Network – QoS Web Page



2. Set the default Differentiated Services value used by the unit for all generated packets in the *Default DiffServ (IPv4)* field.

You can override this value by setting specific service class values. See "Specific Service Class Configuration" on page 103 for more details.

This 8-bit value is directly set in the TOS field (2nd byte) of the header of transmitted IPv4 packets, allowing you to use either DiffServ or TOS mapping.

The DiffServ value is 1 octet scalar ranging from 0 to 255. The DSCP default value should be 101110. This results in the DS field value of 10111000 (184d). This default value would result in a value of "101" precedence bits, low delay, high throughput, and normal reliability in the legacy IP networks (RFC 791, RFC 1812). Network managers of legacy IP networks could use the above-mentioned values to define filters on their routers to take advantage of priority queuing. The default value is based on the Expedited Forwarding PHB (RFC 2598) recommendation.

Note: RFC 3168 now defines the state in which to set the two least significant bits in the TOS byte. On the other hand, this RFC only applies to TCP transmissions and the bits are thus set to "0" in the Aastra unit. This has the following effects:

- The TOS values for UDP packets are the same as in the MIB.
- The TOS values for TCP packets are equal to the closest multiple of 4 value that is not greater than the value in the MIB.

You can find references on DS field under the IETF working group DiffServ. For more information, please refer to the following RFC documents:

- Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (RFC 2474)
- An Architecture for Differentiated Services (RFC 2475)
- Assured Forwarding PHB Group (RFC 2597)
- An Expedited Forwarding PHB (RFC 2598)

3. Set the Default Traffic Class value used by the unit for all generated IPv6 packets in the *Default Traffic Class (IPv6)* field.

Specific service class values may be set in the Service Classes table. See "Specific Service Class Configuration" on page 103 for more details.

The 8-bit Traffic Class field in the IPv6 header is available for use by originating nodes and/or forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets.

4. Click *Submit* if you do not need to set other parameters.

IEEE 802.1q

The 802.1q standard recommends the use of the 802.1q VLAN tags for Ethernet frames traffic prioritization. VLAN tags are 4-byte headers in which three bits are reserved for priority indication. The values of the priority bits shall be provisioned.

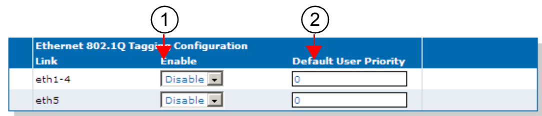
The 802.1q standard comprises the 802.1p standard.

It is the network administrator's responsibility to provision the Aastra unit with standard and correct values.

▶ **To enable the IEEE 802.1q user priority configuration:**

1. In the *Ethernet 802.1Q Tagging Configuration* section of the *QoS* page, select **Enable** in the *Enable* column for each interface on which you want to enable user priority tagging.

Figure 38: Ethernet 802.1Q Tagging Configuration Section



The VLAN ID part of the 802.1Q tag is always set to 0.

2. Set the default user priority value each interface uses when tagging packets in the *Default User Priority* column.

   You can override each value by setting specific service class values. See "Specific Service Class Configuration" on page 103 for more details.

   The user priority is a 3 bit field in the 802.1Q tag that carries a priority value ranging from 0 to 7 and may be used by switches to prioritize traffic. The 802.1q default priority value should be 6 for both signalling and media packets.

3. Click *Submit* if you do not need to set other parameters.

Specific Service Class Configuration

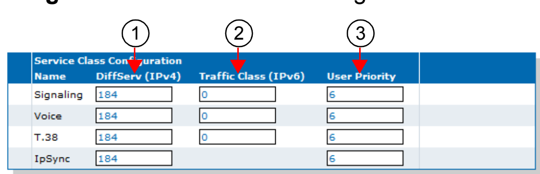
You can override the default value set in the DiffServ and 802.1q sections for each service class of the Aastra unit:

- Signalling
- Voice
- T.38
- IP Sync (IP Sync is not available in IPv6)

▶ **To set specific service class values:**

1. In the *Service Class Configuration* section of the *QoS* page, set a specific DiffServ value for each class in the *DiffServ (IPv4)* column.

Figure 39: Service Class Configuration Section



See "Differentiated Services (DS) Field" on page 101 for more details.

2. Set the Default Traffic Class value used in IPv6 packets for each class in the *Traffic Class (IPv6)* column.

The 8-bit Traffic Class field in the IPv6 header is available for use by originating nodes and/or forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets.

3. Set a specific user priority for each class in the *User Priority* column.

   See “IEEE 802.1q” on page 103 for more details.

4. Click *Submit* if you do not need to set other parameters.

Network Traffic Control Configuration

You can apply a bandwidth limitation on the network interfaces. The limitations are applied on raw data on the physical link and not only on the payload of the packets. All headers, checksums and control bits (TCP, IP, CRC, etc.) are considered in the actual bandwidth.

A bandwidth limitation is applied on a physical link and not on a high-level network interfaces. All high-level network interfaces (including VLANs) using the same physical link are affected by a configured limitation. This limitation is applied egress only (outgoing traffic).

If the NTC service is stopped, this section is not displayed in the *QoS* page. See “Chapter 4 - Services” on page 53 on information on how to start the service. Starting the NTC service enables Traffic Shaping even if bandwidth limitation is disabled.

Bandwidth limitation is an average of the amount of data sent per second. It is thus normal that the unit sends a small burst of data after a period of silence.

Note that the NTC service sends packets on the physical link according to their respective priorities as described below. Lower priority packets are dropped first.

Table 58: Physical Link Priorities

Priority	Description
1	Highest priority. Packets originating from the unit with 802.1p priority set to 7.
2	Packets originating from the unit with 802.1p priority set to 6.
3	Packets originating from the unit with 802.1p priority set to 5.
4	Packets originating from the unit with 802.1p priority set to 4.
5	Packets originating from the unit with 802.1p priority set to 3.
6	Packets originating from the unit with 802.1p priority set to 2.
7	Packets originating from the unit with 802.1p priority set to 1.
8	Packets originating from the unit with 802.1p priority set to 0.
9	Lowest priority. Packets originating from **another link interface** (routed packets).

Packets that exceed the defined bandwidth are eventually dropped (when the buffers are exceeded). This implies that data bursts can suffer a slight amount of packet loss. The different codecs configured and the desired number of simultaneous channels should be taken into account when choosing a bandwidth limit to prevent call drops, choppy voice or inconstant ptime. The NTC service can impact the execution of other processes if the number of packets to process is too high. (High traffic and/or low limit).

▶ **To set network traffic control parameters:**

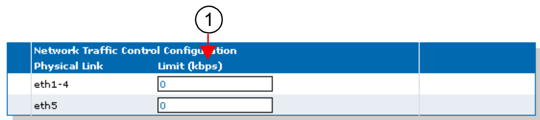
1. In the *Network Traffic Control Configuration* section of the *QoS* page, set the corresponding Egress Limit field with the egress bandwidth limitation for the selected link interface.

   The range is from 64 to 40960 kilobits per second.

   The value 0 means no bandwidth limitation and no prioritization.

This value must be set according to the upstream bandwidth limit of the network on this link. Set to 0 (disable) if the network bandwidth exceeds 40960 kbps or if it exceeds the effective limit of this device.

Figure 40: Network Traffic Control Configuration Section



2. Click *Submit* if you do not need to set other parameters.

CHAPTER
15

Local Firewall Configuration

This chapter describes how to configure the local firewall parameters.

- Setting the default policy
- Creating/editing a firewall rule
- Moving a firewall rule
- Deleting a firewall rule
- Disabling the local firewall

Managing the Local Firewall

The local firewall allows you to dynamically create and configure rules to filter packets. The traffic is analyzed and filtered by all the rules configured.

Note: The Aastra unit's local firewall settings do not support IPv6. See "IPv4 vs. IPv6" on page 85 for more details.

Since this is a local firewall, rules apply only to incoming packets with the unit as destination.

Incoming packets for an IP communication established by the unit are always accepted (Example : If the Aastra unit sends a DNS request, the answer will be accepted).

Rules priority is determined by their position in the table.

The maximum number of rules allowed in the configuration is 20.

Caution: Enabling the local firewall and adding rules has an impact on the Aastra unit's overall performance as the firewall requires additional processing. The more rules are enabled, the more overall performance is affected. Furthermore, Aastra recommends to use a 30 ms packetization time when the firewall is enabled (instead of a 20 ms ptime, for instance) in order to simultaneously use all the channels available on the unit.

Partial Reset

When a partial reset is triggered and the firewall is enabled, the configuration is rolled back if it was being modified. A new rule is then automatically applied in the firewall to allow access to the 'Rescue' interface. However, if the firewall is disabled, the configuration is rolled back but no rule is added.

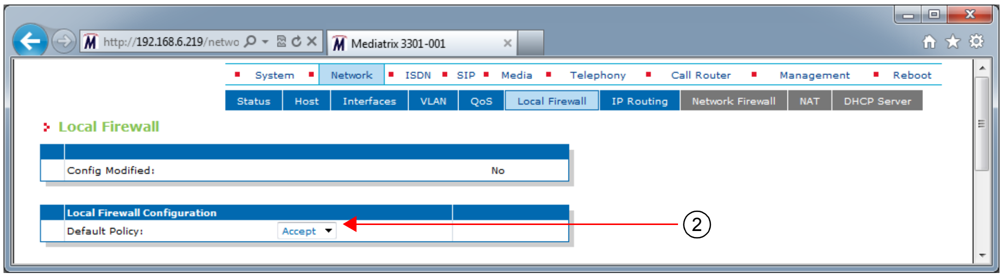
Setting the Default Policy

The default policy defines the action the Aastra unit must take when a packet does not match any rule.

▶ To set the default policy:

1. In the web interface, click the *Network* link, then the *Local Firewall* sub-link.

Figure 41: Network – Local Firewall Web Page



2. In the *Local Firewall Configuration* section, define the *Default Policy* drop-down menu.

Table 59: Default Policy Parameters

Parameter	Description
Accept	Lets the packet through.
Drop	Drops the packet without any notification.

Caution: Make sure there are some rules with the *Action* parameter set to **Accept** in the local firewall BEFORE applying changes that set the default policy to *Drop*. If you do not comply with this warning, you will lose contact with the unit and a partial or factory reset will be required.

Setting the default policy to **Drop** or adding a rule automatically enables the local firewall. Enabling the local firewall may have a negative impact on performance.

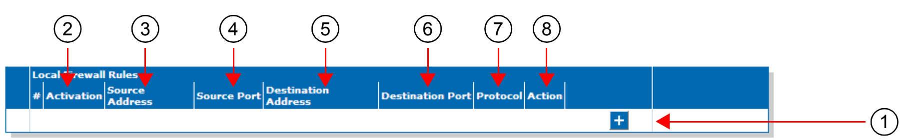
Creating/Editing a Firewall Rule

The web interface allows you to create a firewall rule or modify the parameters of an existing one.

▶ To create or edit a firewall rule:

1. In the *Local Firewall Rules* section of the *Local Firewall* page, do one of the following:
   - If you want to add a rule before an existing entry, locate the proper row in the table and click the + button of this row.
   - If you want to add a rule at the end of the existing rows, click the + button at the bottom right of the section.

Figure 42: Local Firewall Rules Section



Note: When you add a new rule, edit an existing rule, or delete a rule, you can see a yellow **Yes** in the *Config Modified* section at the top of the window. It warns you that the configuration has been modified but not applied (i.e., the *Firewall* section of the *Status* page differs from the *Local Firewall*). The *Local Firewall* sub-menu is a working area where you build up a local firewall configuration. While you work in this area, the configured parameters are saved but not applied (i.e., they are not used to filter incoming packets). The yellow **Yes** flag warns you that the configuration has been modified but is not applied.

2. Set the current activation state for this rule in the corresponding *Activation* drop-down menu.

Table 60: Firewall Rule Activation State Parameters

Parameter	Description
Enable	This rule is active in the firewall.
Disable	This rule is not in the firewall.

Only enabled rules may be applied to the firewall.

3. Enter the source address of the incoming packet in the corresponding *Source Address* field.

Use one of the following syntax:

Table 61: Source Address Parameters

Parameter	Description
`address[/mask]`	Can either be a network IP address (using `/mask`) or one of the host IP addresses. The mask must be a plain number specifying the number of binary 1s at the left side of the network mask (a mask of 24 specifies a network mask of `255.255.255.0`).
`networkInterfaceName/`	The value must already exist in the *Interface Configuration* table (see "Interfaces Configuration" on page 100 for more details). The interface name is case sensitive, hence it must be entered properly. If the specified network interface is disabled or removed, the rule is automatically disabled thus removed from the firewall. When the network interface is enabled or added back, the rule is automatically enabled and applied in the firewall. **Note:** It is mandatory to use the suffix "/" to indicate that the network address of this interface is used instead of the host address.

Leaving the default empty string matches any address.

4. Enter the source port of the incoming packet in the corresponding *Source Port* field.

You can enter a single port or a range of ports. In the case of a range of ports, use the following format:

`port[-port]`

Leaving the default empty string means that no filtering is applied on the source port, thus matching any port.

This parameter is only effective when the *Protocol* drop-down menu is set to **TCP** or **UDP** (see Step 7).

5. Enter the destination address of the incoming packet in the corresponding *Destination Address* field.

Use one of the following syntax:

Table 62: Source Address Parameters

Parameter	Description
`address`	Must be one of the host IP addresses. Specifying a network address is invalid since this is a local firewall.

Table 62: Source Address Parameters (Continued)

Parameter	Description
`networkInterfaceName`	The host address of this interface is used. The value must already exist in the *Interface Configuration* table (see "Interfaces Configuration" on page 100 for more details). The interface name is case sensitive, hence it must be entered properly. If the specified network interface is disabled or removed, the rule is automatically disabled thus removed from the firewall. When the network interface is enabled or added back, the rule is automatically enabled and applied in the firewall.

Leaving the default empty string matches any address.

6. Enter the destination port of the incoming packet in the corresponding *Destination Port* field.

   You can enter a single port or a range of ports. In the case of a range of ports, use the following format:

   `port[-port]`

   Leaving the default empty string means that no filtering is applied on the destination port, thus matching any port.

   This parameter is only effective when the *Protocol* drop-down menu is set to **TCP** or **UDP** (see Step 7).

7. Select the protocol of the incoming packet to filter in the corresponding *Protocol* drop-down menu.

Table 63: Firewal Rule Protocol Parameters

Parameter	Description
All	Matches packets using any protocols.
TCP	Matches only TCP packets.
UDP	Matches only UDP packets.
ICMP	Matches only ICMP packets.

8. Select the action to take in the corresponding *Action* field.

Table 64: Firewal Rule Action Parameters

Parameter	Description
Accept	Lets the packet through.
Reject	Sends back an ICMP port unreachable in response to the matched packet. The packet is then dropped.
Drop	Drops the packet without any notification.

   Note that if a connection is already established before creating a rule that rejects it, this connection stays active despite the rule applied.

9. Click the **Apply** button to activate the enabled rules.

   The current enabled rules applied are displayed in the *Network* > *Status* web page, *Firewall* section, which contains the active configuration in the firewall. You can also see that the yellow *Config Modified* **Yes** flag is cleared.

Moving a Firewall Rule

The firewall rules sequence is very important because rules priority is determined by their position in the table. If you want the unit to try to match one rule before another one, you must put that rule first.

To move a rule up or down:

1. Either click the ^ or v arrow of the rule you want to move until the entry is properly located.
2. Click the **Apply** button to update the *Network* > *Status* web page.

Deleting a Firewall Rule

You can delete a rule from the table in the web interface.

To delete a rule entry:

1. Click the − button of the rule you want to move.
2. Click the **Apply** button to update the *Network* > *Status* web page.

Disabling the Local Firewall

When the local firewall is enabled, it has an impact on the Aastra unit's overall performance as the firewall requires CPU power. You can disable the firewall if you do not need it, thus not impacting performance.

To disable the firewall:

1. In the *Local Firewall Configuration* section, set the default policy to **Accept** with no rules in the local firewall.
2. Restart the Aastra unit.

CHAPTER
16

IP Routing Configuration

This chapter describes how to configure the IP Routing parameters of the Aastra unit.

- IPv4 Forwarding
- Creating/editing an IP routing rule
- Moving an IP routing rule
- Deleting an IP routing rule
- IP routing examples

Managing IP Routing

The IP Routing service allows the Aastra unit to perform advanced routing based on the packet's criteria (source IP address and source Ethernet link), which allows the packet to be forwarded to a specific network. You can create up to four advanced IP routes.

Note: The Aastra unit's IP Routing settings do not support IPv6. See "IPv4 vs. IPv6 Availability" on page 85 for more details.

Packets matching a list of criteria should[1] use advanced IP routes instead of routes present in the main routing table of the unit.

IP Routing works together with the following services:

- Network Firewall ("Chapter 17 - Network Firewall Configuration" on page 135)
- NAT ("Chapter 18 - NAT Configuration" on page 141)
- DHCP server ("Chapter 19 - DHCP Server Settings" on page 149)
- Network Traffic Control ("Network Traffic Control Configuration" on page 118)

These services must be properly configured.

When the IP Routing service is started, IP routing is activated even if there is no configured rule (the Aastra unit will forward received packets). If the IP Routing service is stopped, IP forwarding is disabled, this tab is greyed out and the parameters are not displayed. See "Chapter 4 - Services" on page 53 on information on how to start the service.

Caution: Enabling the IP routing service and adding rules has an impact on the Aastra unit's overall performance as IP routing requires additional processing. The more rules are enabled, the more overall performance is affected. Furthermore, Aastra recommends to use a 30 ms packetization time when IP routing is enabled (instead of a 20 ms ptime, for instance) in order to simultaneously use all the channels available on the unit.

IPv4 Forwarding

IPv4 forwarding allows you to control the IPv4 forwarding feature and the Advanced IP Routes. When set to Enabled, IPv4 Forwarding is enabled and the Advanced IP Routes are applied. When set to Disabled, IPv4 Forwarding is disabled and the Advanced IP Routes are not applied (the *Advanced IP Routes* section of the *IP Routing* page is disabled).

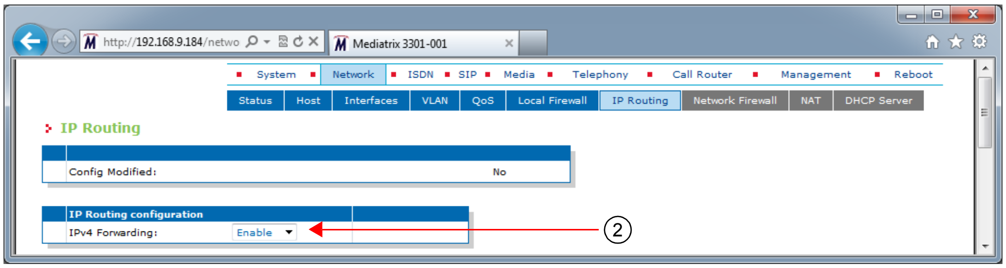
1. A packet matching a route uses the custom routing table first and then the main routing table if no route in the custom routing table was able to send the packet to the desired destination IP address.

▶ **To manage IPv4 forwarding:**

1. In the web interface, click the *Network* link, then the *IP Routing* sub-link.

2. In the *IP Routing Configuration* section of the *IP Routing* page, define whether or not IPv4 forwarding is enabled by setting the *IPv4 Forwarding* drop-down menu accordingly.

Figure 43: IPv4 Forwarding Configuration Section



3. Click the **Submit & Apply** button to update the *Network* > *Status* web page.

Creating/Editing an IP Routing Rule

The web interface allows you to create a routing rule or modify the parameters of an existing one.

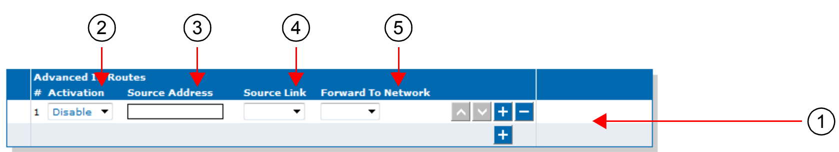
▶ **To create or edit a routing rule:**

1. In the *Advanced IP Routes* section of the *IP Routing* page, do one of the following:

- If you want to add a rule before an existing entry, locate the proper row in the table and click the + button of this row.
- If you want to add a rule at the end of the existing rows, click the + button at the bottom right of the section.

Note: When you add a new rule, edit an existing rule or delete a rule, you can see a yellow **Yes** in the *Config Modified* section at the top of the window. It warns you that the configuration has been modified but not applied (i.e., the *Advanced IP Routes* section of the *Status* page differs from the *IP Routing* page). The *IP Routing* sub-menu is a working area where you build up a routing configuration. While you work in this area, the configured parameters are saved but not applied (i.e., they are not used to route packets). The yellow **Yes** flag warns you that the configuration has been modified but is not applied.

Figure 44: Advanced IP Routes Section



2. Set the required state for this rule in the corresponding *Activation* drop-down menu.

Table 65: IP Routing Rule Activation Parameters

Parameter	Description
Enable	Activates this route.
Disable	Does not activate this route.

Only enabled rules may be applied to the routing table.

3. Enter the source IP address criteria an incoming packet must have to match this rule in the *Source Address* field.

Use the following syntax:

Table 66: Source Address Syntax

Syntax	Description
`address[/mask]`	Can either be a network IP address (using `/mask`) or one of the host IP addresses. The mask must be a plain number specifying the number of binary 1s at the left side of the network mask (a mask of 24 specifies a network mask of `255.255.255.0`). For instance: • 192.168.0.11 • 192.168.1.0/24
`networkInterfaceName[/]`	The value must already exist in the *Interface Configuration* table (see "Interfaces Configuration" on page 100 for more details). The interface name is case sensitive, hence it must be entered properly. If the specified network interface is disabled or removed, the rule is automatically disabled thus removed from the NAT. When the network interface is enabled or added back, the rule is automatically enabled and applied. For instance: • Lan1/ (Lan1 network address) **Note:** It is mandatory to use the suffix "/" to indicate that the network address of this interface is used instead of the host address.

When left empty, any source address matches this rule.

4. Enter the source link criteria an incoming packet must have to match this rule in the *Source Link* field.

   When left empty, packets received on any link match this rule.

5. Select the network on which the packet is forwarded in the *Forward to Network* drop-down menu.

6. Click the **Submit & Apply** button to activate the enabled rules.

   The current applied rules applied are displayed in the *Network* > *Status* web page, *Advanced IP Routes* section, which contains the active configuration of the custom routing tables. You can also see that the yellow *Config Modified* **Yes** flag is cleared.

Note: You can revert back to the configuration displayed in the *Status* web page at any time (including the disabled rules) by clicking the **Rollback** button at the bottom of the page. All modified settings in the *IP Routing* page will be lost.

Moving an IP Routing Rule

The IP routing rules sequence is very important because only one forwarding rule is applied on a packet. Rules priority is determined by their position in the table. If you want the unit to try to match one rule before another one, you must put that rule first.

► **To move a rule up or down:**

1. Either click the or arrow of the rule you want to move until the entry is properly located.
2. Click the **Submit & Apply** button to update the *Network* > *Status* web page.

Deleting an IP Routing Rule

You can delete a rule from the table in the web interface.

▶ **To delete a rule entry:**

1. Click the button of the rule you want to move.
2. Click the **Submit & Apply** button to update the *Network* > *Status* web page.

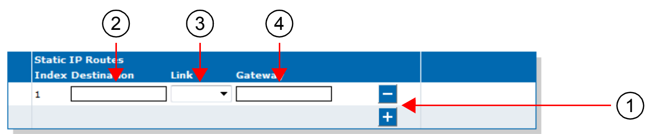
Static IPv4 Routes

You can add or delete static IPv4 routes in the Aastra unit. A "static" route means that the route is configured manually by the administrator. It can be configured through two different methods: through unit provisioning or through a DHCP server ("DHCPv4 Classless Static Route Option" on page 117).

▶ **To manage static IPv4 routes:**

1. In the *Static IP Routes* section of the *IP Routing* page, do one of the following:
   - If you want to add a route, click the button at the bottom of the section.
   - If you want to delete an existing route, click the button of the route you want to move.

Figure 45: Static IP Routes Section



This section is not available if IPv4 forwarding is disabled.

2. Specify the destination IP address criteria that an outgoing packet must have to match this route in the corresponding *Destination* field.

   The supported format for the destination is:

   `IP address[/mask]`

   When specifying a network as a destination, it is mandatory to use the "/" format.

   The mask must be a plain number specifying the number of binary 1s at the left side of the network mask (a mask of 24 specifies a network mask of `255.255.255.0`). For instance:
   - 192.168.1.5 specifies an IP address as the destination.
   - 192.168.1.0/24 specifies a network address as the destination.
3. Select the output link (interface) name in the corresponding *Link* drop-down menu.

   When left empty, the link is selected automatically according to the information already present in the routing table.
4. Define the IP address of the gateway used by the route in the corresponding *Gateway* field.
5. Click the **Submit & Apply** button to update the *Network* > *Status* web page.

   The current routes available are displayed in the *Network* > *Status* web page, *IPv4 Routes* section. This section identifies the entity that installed the route.

Table 67: IPv4 Routes Protocol

Protocol	Description
Dhcp	The route was installed dynamically by the DHCP protocol.
Static	The route was installed by the administrator of the unit.
Kernel	The route was installed by the operating system.
Other	The route was installed by another entity.

DHCPv4 Classless Static Route Option

Standards Supported	• RFC 3442: The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

You can define whether or not the Classless Static Route Option is enabled. Static routes can be configured through the Classless Static Route Option for DHCPv4 (option 121) defined in RFC 3442.

If a static route to 0.0.0.0/0 is received through option 121 while a default router is also specified (see "Default Gateway Configuration" on page 91 for more details), the route received through option 121 has priority.

The following values are available:

Table 68: DHCPv4 Classless Static Route Option Parameters

Parameter	Description
Request	The device requests the Classless Static Route Option 121.
None	Routes received from the DHCP server are ignored.

To define define whether or not the Classless Static Route Option is enabled:

1. In the *bniMIB*, locate the *DhcpClientGroup* folder.
2. Set the `dhcpClientClasslessStaticRouteOption` variable with the proper behaviour.

   You can also use the following line in the CLI or a configuration script:

   ```
   bni.dhcpClientClasslessStaticRouteOption="Value"
   ```

   where *Value* may be one of the following:

Table 69: DHCPv4 Classless Static Route Option Values

Value	Meaning
100	None
200	Request

Network Configuration Examples

The following are two examples of advanced IP routing that can be accomplished with the Aastra unit.

Forward Packets from the Lan1 Network to the Uplink Network with NAT

1. Create an IP routing rule so that the packets are routed ("Managing IP Routing" on page 113).
   - Source IP: Lan1/

     Remove this criterion if you want to forward all packets received on the *lan* link.
   - Source Link: lan[2]
   - Destination Network: Uplink
   - Click *Submit & Apply*.

2. The source link name may vary depending on the unit model you have.

2. Create a NAT rule so that the forwarded packets going on the *Uplink* network use the correct source IP address (“Creating/Editing a Source NAT Rule” on page 141).
   - Type: SNAT
   - Source IP: Lan1/
   - Protocol: All
   - New Address: Uplink
   - Click *Submit & Apply*.
3. Create a Network Firewall rule to let established or related packets go through the unit (if the default policy is not set to Accept) (“Managing the Network Firewall” on page 135).
   - Connection State: Established or Related
   - Action: Accept
4. Create a Network Firewall rule to let the packets pass from the *Lan1* network to the *Uplink* network (if the default policy is not set to Accept). All response packets will be accepted by the previous rule (“Managing the Network Firewall” on page 135).
   - Source IP: Lan1/

     Use additional rules or set the default policy to *Accept* if you want to forward packets received on the *lan* link with a source address that does not match the *Lan1* subnet.
   - Connection State: New
   - Action: Accept
   - Click *Submit & Apply*.

Configure Port Forwarding for a Web Server Located on the LAN

1. Make sure the IP Routing service is started (to activate IP forwarding).
2. Create a NAT rule (“Creating/Editing a Destination NAT Rule” on page 145).

   This will change the destination of an HTTP packet originally destined to the Aastra unit with the *IP:Port* of the Web server on the LAN side (to make sure the unit does not process the packet but forwards it on the *Lan1* network).
   - Type: DNat
   - Destination IP: Uplink
   - Destination Port: 8080
   - Protocol: TCP
   - New Address: 192.168.0.11:80 (IP:Port of the Web server on the LAN side)
   - Click *Submit & Apply*.
3. Create a NAT rule (“Creating/Editing a Source NAT Rule” on page 141).

   This will change the source IP address of the packet before it is sent on the *Lan1* network (to make sure the Web browser can reply correctly to the request).
   - Type: SNat
   - Destination IP: 192.168.0.11
   - Destination Port: 80
   - Protocol: TCP
   - New Address: Lan1
   - Click *Submit & Apply*.
4. Create a Network Firewall rule to let established or related packets go through the unit (if the default policy is not set to Accept) (“Managing the Network Firewall” on page 135).
   - Connection State: Established or Related
   - Action: Accept

5. Create a Network Firewall rule to let the packets pass from the *Uplink* network to the *Lan1* network (if the default policy is not set to Accept). All response packets will be allowed by the previous rule ("Managing the Network Firewall" on page 135).
    - Destination IP: 192.168.0.11
    - Destination Port: 80
    - Protocol: TCP
    - Action: Accept
    - Click *Submit & Apply*.

CHAPTER
17
Network Firewall Configuration

This chapter describes how to configure the network firewall parameters.

- Setting the default policy
- Creating/editing a firewall rule
- Moving a firewall rule
- Deleting a firewall rule
- Disabling the network firewall

Managing the Network Firewall

The network firewall allows dynamically creating and configuring rules to filter packets forwarded by the unit. Since this is a network firewall, rules only apply to packets forwarded by the unit. The traffic is analyzed and filtered by all the rules configured.

Note: The Aastra unit's network firewall settings do not support IPv6. See "IPv4 vs. IPv6 Availability" on page 85 for more details.

If no rule matches the incoming packet, the default policy is applied. A rule's priority is determined by its index in the table.

Rules using Network Names are automatically updated as the associated IP addresses and network mask are modified.

If the Network Firewall service is stopped, all forwarded traffic is accepted, this tab is greyed out and the parameters are not displayed. See "Chapter 4 - Services" on page 53 on information on how to start the service.

The maximum number of rules allowed in the configuration is 20.

Caution: Enabling the network firewall and adding rules has an impact on the Aastra unit's overall performance as the firewall requires additional processing. The more rules are enabled, the more overall performance is affected. Furthermore, Aastra recommends to use a 30 ms packetization time when the firewall is enabled (instead of a 20 ms ptime, for instance) in order to simultaneously use all the channels available on the unit.

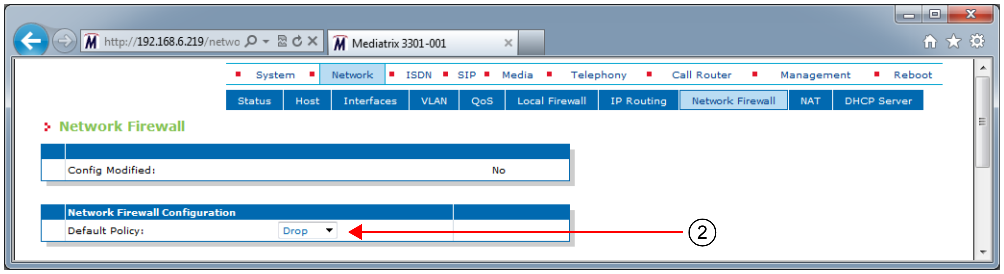
Setting the Default Policy

The default policy defines the action the Aastra unit must take when a forwarded packet does not match any rules.

▶ To set the default policy:

1. In the web interface, click the *Network* link, then the *Network Firewall* sub-link.

Figure 46: Network – Network Firewall Web Page



2. In the *Network Firewall Configuration* section, define the default policy in the *Default Policy* drop-down menu.

Table 70: Default Policy Parameters

Parameter	Description
Accept	Lets the packet through.
Drop	Drops the packet without any notification.

Setting the default policy to **Drop** or adding a rule automatically enables the network firewall. Enabling the network firewall may have a negative impact on performance.

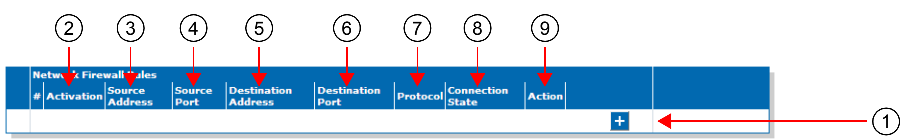
Creating/Editing a Network Firewall Rule

The web interface allows you to create a network firewall rule or modify the parameters of an existing one.

▶ To create or edit a network firewall rule:

1. In the *Network Firewall Rules* section of the *Network Firewall* page, do one of the following:
   - If you want to add a rule before an existing entry, locate the proper row in the table and click the + button of this row.
   - If you want to add a rule at the end of the existing rows, click the + button at the bottom right of the section.

Figure 47: Network Firewall Rules Section



Note: When you add a new rule, edit an existing rule or delete a rule, you can see a yellow **Yes** in the *Config Modified* section at the top of the window. It warns you that the configuration has been modified but not applied (i.e., the *Firewall* section of the *Status* page differs from the *Network Firewall* page). The *Network Firewall* page is a working area where you build up a network firewall configuration. While you work in this area, the configured parameters are saved but not applied (i.e., they are not used to filter packets). The yellow **Yes** flag warns you that the configuration has been modified but is not applied.

2. Set the required state for this rule in the corresponding *Activation* drop-down menu.

Table 71: Firewall Rule Activation Parameters

Parameter	Description
Enable	This rule is active in the firewall.
Disable	This rule is not in the firewall.

Only enabled rules may be applied to the firewall.

3. Enter the source address of the incoming packet in the corresponding *Source Address or Interface* field.

Use one of the following syntax:

Table 72: Source Address Syntax

Syntax	Description
`address[/mask]`	Network IP address (using `/mask`). The mask must be a plain number specifying the number of binary 1s at the left side of the network mask (a mask of 24 specifies a network mask of `255.255.255.0`). For instance: • 192.168.0.11 • 192.168.1.0/24
`networkInterfaceName/`	The value must already exist in the *Interface Configuration* table (see "Interfaces Configuration" on page 100 for more details). The interface name is case sensitive, hence it must be entered properly. If the specified network interface is disabled or removed, the rule is automatically disabled thus removed from the firewall. When the network interface is enabled or added back, the rule is automatically enabled and applied in the firewall. For instance: • Lan1/ (Lan1 network address) **Note:** It is mandatory to use the suffix "/" to indicate that the network address of this interface is used instead of the host address.

Leaving the default empty string matches any address.

4. Enter the source port of the incoming packet in the corresponding *Source Port* field.

You can enter a single port or a range of ports. This field supports the following syntax:

`port[-port]`

Leaving the default empty string means that no filtering is applied on the source port, thus matching any port.

This parameter is only effective when the *Protocol* drop-down menu is set to **TCP** or **UDP** (see Step 7).

5. Enter the destination address of the incoming packet in the corresponding *Destination Address or Interface* field.

Use one of the following syntax:

Table 73: Source Address Syntax

Syntax	Description
`address[/mask]`	Network IP address (using `/mask`). The mask must be a plain number specifying the number of binary 1s at the left side of the network mask (a mask of 24 specifies a network mask of `255.255.255.0`). For instance: • 192.168.0.11 • 192.168.1.0/24
`networkInterfaceName/`	The value must already exist in the *Interface Configuration* table (see “Interfaces Configuration” on page 100 for more details). The interface name is case sensitive, hence it must be entered properly. If the specified network interface is disabled or removed, the rule is automatically disabled thus removed from the firewall. When the network interface is enabled or added back, the rule is automatically enabled and applied in the firewall. For instance: • Lan1/ (Lan1 network address) **Note:** It is mandatory to use the suffix “/” to indicate that the network address of this interface is used instead of the host address.

Leaving the default empty string matches any address.

6. Enter the destination port of the incoming packet in the corresponding *Destination Port* field.

You can enter a single port or a range of ports. This field supports the following syntax:

`port[-port]`

Leaving the default empty string means that no filtering is applied on the destination port, thus matching any port.

This parameter is only effective when the *Protocol* drop-down menu is set to **TCP** or **UDP** (see Step 7).

7. Select the protocol of the incoming packet to filter in the corresponding *Protocol* drop-down menu.

Table 74: Firewall Rule Protocol Parameters

Parameter	Description
All	Matches packets using any protocols.
TCP	Matches only TCP packets.
UDP	Matches only UDP packets.
ICMP	Matches only ICMP packets.

8. Set the corresponding *Connection State* drop-down menu with the connection state associated with the incoming packet.

The connection state can be one of the following:

Table 75: Connection State Parameters

State	Description
All	Match packets in any state.
New	Match packets that are not part of an existing connection.

Table 75: Connection State Parameters (Continued)

State	Description
Established Or Related	Match packets that are part of an existing connection.

9. Select the action to take in the corresponding *Action* field.

Table 76: Network Firewall Rule Action Parameters

Parameter	Description
Accept	Lets the packet through.
Reject	Sends back an ICMP port unreachable in response to the matched packet. The packet is then dropped.
Drop	Drops the packet without any notification.

Note that if a connection is already established before creating a rule that rejects it, this connection stays active despite the rule applied.

10. Click the **Apply** button to activate the enabled rules.

The current enabled rules applied are displayed in the *Network* > *Status* web page, which contains the active configuration in the network firewall. You can also see that the yellow *Config Modified* **Yes** flag is cleared.

Note: You can revert back to the configuration displayed in the *Network* > *Status* web page at any time (including the disabled rules) by clicking the **Rollback** button at the bottom of the page. All modified settings in the *Network* > *Network Firewall* page will be lost.

Moving a Network Firewall Rule

The firewall rules sequence is very important because only one network firewall rule is applied on a packet. Rules priority is determined by their position in the table. If you want the unit to try to match one rule before another one, you must put that rule first.

▶ **To move a rule up or down:**

1. Either click the ^ or v arrow of the rule you want to move until the entry is properly located.

2. Click the **Apply** button to update the *Network* > *Status* web page.

Deleting a Network Firewall Rule

You can delete a rule from the table in the web interface.

▶ **To delete a rule entry:**

1. Click the − button of the rule you want to move.

2. Click the **Apply** button to update the *Network* > *Status* web page.

Disabling the Network Firewall

When the network firewall is enabled, it has an impact on the Aastra unit’s overall performance as the firewall requires additional processing. You can disable the firewall if you do not need it, thus not impacting performance. To disable the network firewall, you must stop the NFW service in the *System* > *Services* page. See “Chapter 4 - Services” on page 53 for more details on how to stop a service. All forwarded traffic is allowed when the network firewall service is stopped.

CHAPTER
18

NAT Configuration

This chapter describes how to configure the NAT parameters of the Aastra unit.

- Creating/editing a Source NAT
- Creating/editing a Destination NAT
- Moving a NAT rule
- Deleting a NAT rule

Introduction

Network Address Translation (NAT, also known as network masquerading or IP masquerading) rewrites the source and/or destination addresses/ports of IP packets as they pass through a router or firewall. It is most commonly used to connect multiple computers to the Internet (or any other IP network) by using one IP address. This allows home users and small businesses to cheaply and efficiently connect their network to the Internet. The basic purpose of NAT is to multiplex traffic from the internal network and present it to the Internet as if it was coming from a single computer having only one IP address.

The Aastra unit’s NAT service allows the dynamic creation and configuration of network address translation rules. Depending on some criteria, the packet matching the rule may see its source or destination address modified.

There are two types of NAT rules:

- ***Source rules***: They are applied on the source address of outgoing packets.
- ***Destination rules***: They are applied on the destination address of incoming packets.

A rule's priority is determined by its index in the Source NAT or Destination NAT tables.

If the NAT service is stopped, this tab is greyed out and the parameters are not displayed. See “Chapter 4 - Services” on page 53 on information on how to start the service.

The maximum number of rules allowed in the configuration is 10 of each Source NAT and Destination NAT.

Caution: Adding source or destination NAT rules has an impact on the Aastra unit’s overall performance as the NAT requires additional processing. The more rules are enabled, the more overall performance is affected. Furthermore, Aastra recommends to use a 30 ms packetization time when the NAT is enabled (instead of a 20 ms ptime, for instance) in order to simultaneously use all the channels available on the unit.

Partial Reset

When a partial reset is triggered, the configuration is rolled back if it was being modified.

A new rule is then automatically applied in the source and in the destination NAT tables to prevent incorrect rules from blocking access to the unit. If those rules are not the first priority, they are raised. If there are no rules in the tables, the new rules are not added since there are no rules to override.

Creating/Editing a Source NAT Rule

SNAT rules are executed after the routing decision, before the packet leaves the unit.

The web interface allows you to create a source NAT rule or modify the parameters of an existing one. The following parameters must all match to apply a SNAT rule to a packet:

- Source Address

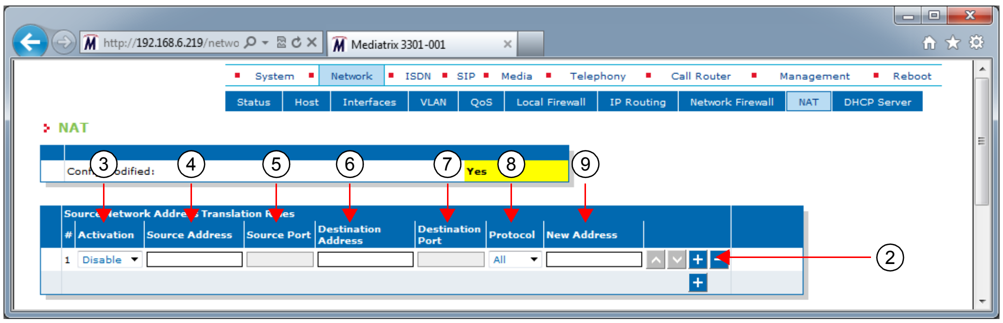
- Source Port
- Destination Address
- Destination Port
- Protocol

When the above parameters all match, then a new source IP address/port is applied to the packet.

To create or edit a source NAT rule:

1. In the web interface, click the *Network* link, then the *NAT* sub-link.

Figure 48: Source Network Address Translation Rules Section



2. In the *Source Network Address Translation Rules* section of the *NAT* page, do one of the following:

- If you want to add a rule before an existing entry, locate the proper row in the table and click the + button of this row.
- If you want to add a rule at the end of the existing rows, click the + button at the bottom right of the section.

> **Note:** When you add a new rule, edit an existing rule or delete a rule, you can see a yellow **Yes** in the *Config Modified* section at the top of the window. It warns you that the configuration has been modified but not applied (i.e., the *Network Address Translation* section of the *Status* page differs from the *NAT* page). The *NAT* page is a working area where you build up a NAT configuration. While you work in this area, the configured parameters are saved but not applied (i.e., they are not used in the NAT). The yellow **Yes** flag warns you that the configuration has been modified but is not applied.

3. Set the required state for this rule in the corresponding *Activation* drop-down menu.

Table 77: Source NAT Rule Activation Parameters

Parameter	Description
Enable	This SNAT rule is enabled.
Disable	This SNAT rule is disabled.

Only enabled rules may be applied to the Source NAT.

4. Enter the source address of the incoming packet in the corresponding *Source Address* field.

Use one of the following syntax:

Table 78: Source Address Syntax

Syntax	Description
`address[/mask]`	Can either be a network IP address (using `/mask`) or one of the host IP addresses. The mask must be a plain number specifying the number of binary 1s at the left side of the network mask (a mask of 24 specifies a network mask of `255.255.255.0`). For instance: • 192.168.0.11 • 192.168.1.0/24
`networkInterfaceName[/]`	The value must already exist in the *Interface Configuration* table (see “Interfaces Configuration” on page 100 for more details). The interface name is case sensitive, hence it must be entered properly. If the specified network interface is disabled or removed, the rule is automatically disabled thus removed from the NAT. When the network interface is enabled or added back, the rule is automatically enabled and applied in the NAT. For instance: • Lan1 (Lan1 IP address) • Lan1/ (Lan1 network address)

Leaving the default empty string matches any address.

5. Enter the source port of the incoming packet in the corresponding *Source Port* field.

You can enter a single port or a range of ports. This field supports the following syntax:

`port[-port]`

Leaving the default empty string means that no filtering is applied on the source port, thus matching any port.

This parameter is only effective when the *Protocol* drop-down menu is set to **TCP** or **UDP** (see Step 7).

6. Enter the destination address of the incoming packet in the corresponding *Destination Address* field.

Use one of the following syntax:

Table 79: Destination Address Syntax

Syntax	Description
`address[/mask]`	Can either be a network IP address (using `/mask`) or one of the host IP addresses. The mask must be a plain number specifying the number of binary 1's at the left side of the network mask (a mask of 24 specifies a network mask of `255.255.255.0`). For instance: • 192.168.0.11 • 192.168.1.0/24

Table 79: Destination Address Syntax (Continued)

Syntax	Description
`networkInterfaceName/`	The host address of this interface is used. The value must already exist in the *Interface Configuration* table (see “Interfaces Configuration” on page 100 for more details). The interface name is case sensitive, hence it must be entered properly. If the specified network interface is disabled or removed, the rule is automatically disabled thus removed from the NAT. When the network interface is enabled or added back, the rule is automatically enabled and applied in the Source NAT. For instance: • Lan1/ (Lan1 network address) **Note:** It is mandatory to use the suffix “/” to indicate that the network address of this interface is used instead of the host address.

Leaving the default empty string matches any address.

7. Enter the destination port of the incoming packet in the corresponding *Destination Port* field.

   You can enter a single port or a range of ports. This field supports the following format:

   `port[-port]`

   Leaving the default empty string means that no filtering is applied on the destination port, thus matching any port.

   This parameter is only effective when the *Protocol* drop-down menu is set to **TCP** or **UDP** (see Step 7).

8. Select the protocol of the incoming packet to NAT in the corresponding *Protocol* drop-down menu.

Table 80: Source NAT Rule Protocol Parameters

Parameter	Description
All	Matches packets using any protocols.
TCP	Matches only TCP packet.
UDP	Matches only UDP packets.
ICMP	Matches only ICMP packets.

9. Enter the new address applied to the source of the packet in the *New Address* field.

   Use the following syntax:

Table 81: New Address Syntax

Syntax	Description
`address[:port]`	Any IP address. When specifying a port number, it is mandatory to have the protocol set to TCP or UDP.

10. Click the **Apply** button to activate the enabled rules.

    The current enabled rules applied are displayed in the *Network > Status* web page, *Network Address Translation* section, which contains the active configuration in the NAT. You can also see that the yellow *Config Modified* **Yes** flag is cleared.

Note: You can revert back to the configuration displayed in the *Status* web page at any time (including the disabled rules) by clicking the **Rollback** button at the bottom of the page. All modified settings in the *NAT* page will be lost.

Creating/Editing a Destination NAT Rule

The web interface allows you to create a Destination NAT rule or modify the parameters of an existing one. This creates a rule that allows remote computers (e.g., public machines on the Internet) to connect to a specific computer within the private LAN, depending on the port used to connect. A destination NAT is also known as port forwarding or virtual server.

DNAT rules are executed before the routing decision, as the packet enters the unit. Therefore it is important to configure the Network Firewall ("Chapter 17 - Network Firewall Configuration" on page 135) with respect to the DNAT rules. An example of this would be port forwarding where the DNAT changes the routed address of a packet to a new IP address/port. The Network Firewall must also accept connection to this IP/port in order for the port forwarding to work.

The following parameters must all match to apply a DNAT rule to a packet:

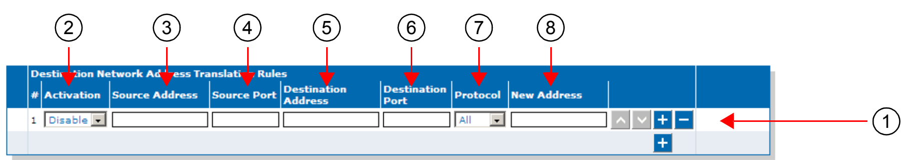
- Source Address
- Source Port
- Destination Address
- Destination Port
- Protocol

When the above parameters all match, then a new destination IP address/port is applied to the packet.

To create or edit a Destination NAT rule:

1. In the *Destination Network Address Translation Rules* section of the *NAT* page, do one of the following:
   - If you want to add a rule before an existing entry, locate the proper row in the table and click the + button of this row.
   - If you want to add a rule at the end of the existing rows, click the + button at the bottom right of the section.

Figure 49: Destination Network Address Translation Rules Section



Note: When you add a new rule, edit an existing rule, or delete a rule, you can see a yellow **Yes** in the *Config Modified* section at the top of the window. It warns you that the configuration has been modified but not applied (i.e., the *Network Address Translation* section of the *Status* page differs from the *NAT* page). The *NAT* page is a working area where you build up a NAT configuration. While you work in this area, the configured parameters are saved but not applied (i.e., they are not used in the NAT). The yellow **Yes** flag warns you that the configuration has been modified but is not applied.

2. Set the required state for this rule in the corresponding *Activation* drop-down menu.

Table 82: Destination NAT Rule Activation Parameters

Parameter	Description
Enable	This DNAT rule is enabled.
Disable	This DNAT rule is disabled.

Only enabled rules may be applied to the Destination NAT.

3. Enter the source address of the incoming packet in the corresponding *Source Address* field.

Use one of the following syntax:

Table 83: Source Address Syntax

Syntax	Description
`address[/mask]`	Can either be a network IP address (using `/mask`) or one of the host IP addresses. The mask must be a plain number specifying the number of binary 1's at the left side of the network mask (a mask of 24 specifies a network mask of `255.255.255.0`). For instance: • 192.168.0.11 • 192.168.1.0/24
`networkInterfaceName/`	The host address of this interface is used. The value must already exist in the *Interface Configuration* table (see "Interfaces Configuration" on page 100 for more details). The interface name is case sensitive, hence it must be entered properly. If the specified network interface is disabled or removed, the rule is automatically disabled thus removed from the NAT. When the network interface is enabled or added back, the rule is automatically enabled and applied in the Destination NAT. For instance: • Lan1/ (Lan1 network address) **Note:** It is mandatory to use the suffix "/" to indicate that the network address of this interface is used instead of the host address.

Leaving the default empty string matches any address.

4. Enter the source port of the incoming packet in the corresponding *Source Port* field.

You can enter a single port or a range of ports. This field supports the following format:

`port[-port]`

Leaving the default empty string means that no filtering is applied on the source port, thus matching any port.

This parameter is only effective when the *Protocol* drop-down menu is set to **TCP** or **UDP** (see Step 7).

5. Enter the destination address of the incoming packet in the corresponding *Destination Address* field.

Use one of the following syntax:

Table 84: Destination Address Syntax

Syntax	Description
`address[/mask]`	Can either be a network IP address (using `/mask`) or one of the host IP addresses. The mask must be a plain number specifying the number of binary 1's at the left side of the network mask (a mask of 24 specifies a network mask of `255.255.255.0`). For instance: • 192.168.0.11 • 192.168.1.0/24

Table 84: Destination Address Syntax (Continued)

Syntax	Description
`networkInterfaceName[/]`	The host address of this interface is used. The value must already exist in the *Interface Configuration* table (see “Interfaces Configuration” on page 100 for more details). The interface name is case sensitive, hence it must be entered properly. If the specified network interface is disabled or removed, the rule is automatically disabled thus removed from the NAT. When the network interface is enabled or added back, the rule is automatically enabled and applied in the Destination NAT. For instance: • Lan1 (Lan1 IP address) • Lan1/ (Lan1 network address)

Leaving the default empty string matches any address.

6. Enter the destination port of the incoming packet in the corresponding *Destination Port* field.

You can enter a single port or a range of ports. This field supports the following format:

`port[-port]`

Leaving the default empty string means that no filtering is applied on the destination port, thus matching any port.

This parameter is only effective when the *Protocol* drop-down menu is set to **TCP** or **UDP** (see Step 7).

7. Select the protocol of the incoming packet to NAT in the corresponding *Protocol* drop-down menu.

Table 85: Destination NAT Rule Protocol Parameters

Parameter	Description
All	Matches packets using any protocols.
TCP	Matches only TCP packets.
UDP	Matches only UDP packets.
ICMP	Matches only ICMP packets.

8. Enter the new address of the packet in the *New Address* field.

Use the following syntax:

Table 86: New Address Syntax

Syntax	Description
`address[:port]`	Any IP address. When specifying a port number, it is mandatory to have the protocol set to TCP or UDP.

9. Click the **Apply** button to activate the enabled rules.

The current enabled rules applied are displayed in the *Network > Status* web page, *Network Address Translation* section, which contains the active configuration in the NAT. You can also see that the yellow *Config Modified* **Yes** flag is cleared.

> **Note:** You can revert back to the configuration displayed in the *Network > Status* web page at any time (including the disabled rules) by clicking the **Rollback** button at the bottom of the page. All modified settings in the *Network > NAT* page will be lost.

Moving a NAT Rule

The NAT rules sequence is very important because only one SNAT rule or one DNAT rule is applied on a packet. Rules priority is determined by their position in the table. If you want the unit to try to match one rule before another one, you must put that rule first.

▶ **To move a rule up or down:**

1. Either click the ^ or v arrow of the rule you want to move until the entry is properly located.
2. Click the **Apply** button to update the *Network* > *Status* web page.

Deleting a NAT Rule

You can delete a rule from the table in the web interface.

▶ **To delete a rule entry:**

1. Click the − button of the rule you want to move.
2. Click the **Apply** button to update the *Network* > *Status* web page.

Disabling the NAT

When the NAT is enabled, it has an impact on the Aastra unit's overall performance as the NAT requires additional processing. You can disable the NAT if you do not need it, thus not impacting performance. To disable the NAT, you must stop the NAT service in the *System* > *Services* page. See "Chapter 4 - Services" on page 53 for more details on how to stop a service.

CHAPTER 19

DHCP Server Settings

This chapter describes how to configure the embedded DHCP server of the Aastra unit.

Standards Supported	• RFC 2131: Dynamic Host Configuration Protocol, section 2 (server side) • RFC 2132: DHCP Options and BOOTP Vendor Extensions (sections 3.3, 3.5, 3.8, 3.17, 8.3 and 8.5)

Introduction

The Aastra unit contains an embedded DHCP server that allocates IP addresses and provides leases to the various subnets that are configured. These subnets could have PCs or other IP devices connected to the unit's LAN Ethernet connectors. These devices could be any combination of switches, PCs, IP phones, etc.

If the DHCP service is stopped, this tab is greyed out and the parameters are not displayed. See "Chapter 4 - Services" on page 53 on information on how to start the service.

Note: The Aastra unit's DHCP server settings do not support IPv6. See "IPv4 vs. IPv6" on page 85 for more details.

Subnet Server

The DHCP server manages the hosts' network configuration on a given subnet. Each subnet can be seen as having a distinct DHCP server managing it, which is called a subnet server. To activate a subnet server for a given network interface, the name of that network interface and the name of the subnet configuration must match (the names are case sensitive). Only one subnet can be defined per network interface. The network interface can be a physical interface or a logical interface (e.g., sub-interface using VLAN).

Leases

In order to assign leases, the subnet server draws from an IP address pool (or subnet scope) defined by a start address and an end address. The subnet mask assigned to hosts is taken directly from the network interface. All hosts on the same subnet share the same configuration. The maximum number of hosts supported on a subnet is 254.

You can reserve IP addresses for specific hosts that are designated by their MAC address. Those addresses are then removed from the pool of IP addresses that can be leased. Once a lease is assigned, it is removed from the pool of IP addresses that can be leased for as long as the host keeps it.

Configuration Parameters

When an address is leased to a host, several network configuration parameters are sent to that host at the same time according to the options found in the DHCP request. You can modify the configuration source of a parameter. The following are the possible configuration sources:

Table 87: Parameter Configuration Sources

Source	Description
Static	The parameter is defined as a static parameter locally.
Automatic	The parameter is obtained from the network configured in the *Automatic Configuration Interface* drop-down menu of this subnet ("DHCP Basic Configuration" on page 137).

Table 87: Parameter Configuration Sources (Continued)

Source	Description
Host Configuration	The parameter is obtained from the host configuration.
Host Interface	The parameter is obtained from the network interface matching the subnet.

The following table lists the configuration parameters and their available configuration sources:

Table 88: Optional Parameter and Possible Configuration Sources

Parameter Name	Configuration Sources			
	Static	Automatic	Host Config	Host Interface
Domain Name	✓		✓	
Lease time	✓			
Default gateway	✓			✓
List of DNS servers	✓	✓	✓	
List of NTP servers	✓	✓	✓	
List of NBNS servers	✓			

Default vs. Specific Configurations

You can use two types of configuration:

- Default configurations that apply to all the subnets of the Aastra unit.
- Specific configurations that override the default configurations.

  You can define specific configurations for each subnet in your Aastra unit. For instance, you could define a lease time for all the subnets of the Aastra unit and use the specific configuration parameters to set a different value for one specific subnet.

The parameters available differ according to the subnet you have selected. The *Default* subnet has less parameters than the specific subnets available on the Aastra unit.

DHCP Basic Configuration

The basic configuration parameters are available only on the specific subnets configuration.

▶ **To set the DHCP server basic parameters:**

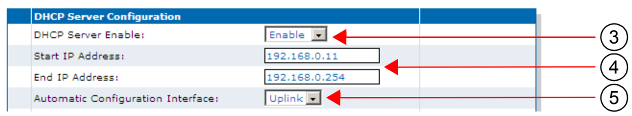
1. In the web interface, click the *Network* link, then the *DHCP Server* sub-link.

2. Select a specific subnet in the *Select Subnet* drop-down menu at the top of the window.

You have the choice between *Default* (applies to all subnets) and specific subnets.

3. In the *DHCP Server Configuration* section of the *DHCP Server* page, enable the DHCP server by selecting **Enable** in the *DHCP Server Enable* drop-down menu.

Figure 50: DHCP Server Configuration – General Parameters



4. Set the start and end IP addresses of the subnet range in the *Start IP Address* and *End IP Address* fields.

These are the addresses that the DHCP server offers to the subnets of the Aastra unit. The Aastra unit can offer up to 254 addresses. These addresses must be within the network interface's subnet or the subnet server will have an invalid configuration status.

5. Set the *Automatic Configuration Interface* drop-down menu with the network interface that provides the automatic configuration (e.g.: DNS servers, NTP server, etc.) to all parameters of this subnet that use the "Automatic" configuration source.

6. Click *Submit* if you do not need to set other parameters.

Lease Time (Option 51)

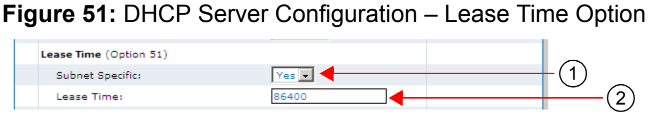
The Aastra unit DHCP server offers a lease time to its subnets. You can use a default lease time for all subnets or define a lease time specific to one or more subnets.

▶ **To set the DHCP server lease time parameters:**

1. In the *Lease Time (Option 51)* sub-section of the *DHCP Server Configuration* section, define whether or not you want to override the lease time set in the *Default* configuration in the *Subnet Specific* drop-down menu.

This menu is available only in the specific subnets configuration.

Figure 51: DHCP Server Configuration – Lease Time Option



2. Define the lease time (in seconds) given by the Aastra unit DHCP server in the *Lease Time* field.

3. Click *Submit* if you do not need to set other parameters.

Domain Name (Option 15)

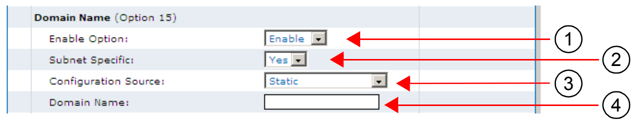
The Aastra unit DHCP server offers a domain name to its subnets. You can use a default domain name for all subnets or define a domain name specific to one or more subnets.

▶ **To set the DHCP server domain name parameters:**

1. In the *Domain Name (Option 15)* sub-section of the *DHCP Server Configuration* section, enable the domain name (option 15) by selecting **Enable** in the *Enable Option* drop-down menu.

   This menu is available only in the specific subnets configuration.

Figure 52: DHCP Server Configuration – Domain Name Option



2. Define whether or not you want to override the domain name parameters set in the *Default* configuration in the *Subnet Specific Value* drop-down menu.

   This menu is available only in the specific subnets configuration.

3. If the domain name option is enabled, select the configuration source of the domain name information in the *Configuration Source* drop-down menu.

Table 89: Domain Name Configuration Sources

Source	Description
Host Configuration	The domain name is the one used by the unit.
Static	You manually enter a domain name.

Static Configuration Source Only

4. If the configuration source is **Static**, enter the static default domain name for all subnets in the *Domain Name* field.

5. Click *Submit* if you do not need to set other parameters.

Default Gateway (Option 3)

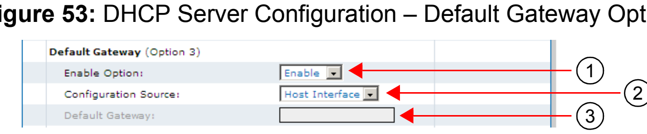
The Aastra unit DHCP server offers a default gateway (also called default router) to its subnets.

Note: The default gateway parameters are not available in the *Default* interface. You must access the specific subnets configuration to set its parameters.

▶ **To set the DHCP server default gateway parameters:**

1. In the *Default Gateway (Option 3)* sub-section of the *DHCP Server Configuration* section, enable the default gateway (option 3) by selecting **Enable** in the *Enable Option* drop-down menu

Figure 53: DHCP Server Configuration – Default Gateway Option



2. Select the configuration source of the default gateway information in the *Configuration Source* drop-down menu.

Table 90: Default Gateway Configuration Sources

Source	Description
Host Interface	The default gateway is the host address within the client's subnet.
Static	You manually enter the value.

Static Configuration Source Only

3. If the configuration source is **Static**, enter the default gateway host name or IP address of the subnet in the *Default Gateway* field.
4. Click *Submit* if you do not need to set other parameters.

DNS (Option 6)

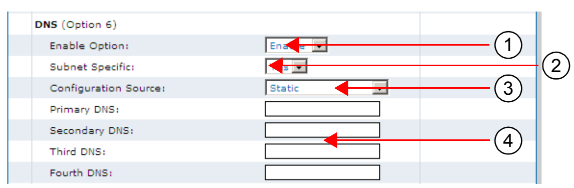
The Aastra unit DHCP server offers up to four DNS addresses to its subnets. You can use the default DNS addresses for all subnets or define static DNS addresses specific to one or more subnets.

▶ **To set the DHCP server DNS parameters:**

1. In the *DNS (Option 6)* sub-section of the *DHCP Server Configuration* section, enable the DNS servers (option 6) by selecting **Enable** in the *Enable Option* drop-down menu

   This menu is available only in the specific subnets configuration.

Figure 54: DHCP Server Configuration – DNS Option



2. Define whether or not you want to override the default values in the *Subnet Specific* drop-down menu.

   This menu is available only in the specific subnets configuration.

3. Select the configuration source of the DNS information in the *Configuration Source* drop-down menu.

Table 91: DNS Configuration Sources

Source	Description
Host Configuration	The DNS servers are obtained from the host configuration.
Automatic	The DNS servers are automatically obtained from the network configured in the *Automatic Configuration Interface* drop-down menu of this subnet (“DHCP Basic Configuration” on page 137).
Static	You manually enter the value.

Static Configuration Source Only

4. If the configuration source is **Static**, enter the static addresses of up to four DNS servers in the following fields:

- Primary DNS
- Secondary DNS
- Third DNS
- Fourth DNS

5. Click *Submit* if you do not need to set other parameters.

NTP (Option 42)

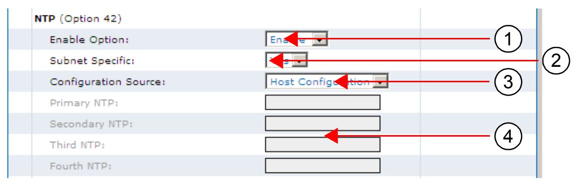
The Aastra unit DHCP server offers the addresses of up to four NTP (Network Time Protocol) servers to its subnets. You can use the default NTP addresses for all subnets or define static DNS addresses specific to one or more subnets.

▶ **To set the DHCP server NTP parameters:**

1. In the *NTP (Option 42)* sub-section of the *DHCP Server Configuration* section, enable the NTP servers (option 42) by selecting **Enable** in the *Enable Option* drop-down menu

This menu is available only in the specific subnets configuration.

Figure 55: DHCP Server Configuration – NTP Option



2. Define whether or not you want to override the default values in the *Subnet Specific* drop-down menu.

This menu is available only in the specific subnets configuration.

3. Select the configuration source of the NTP information in the *Configuration Source* drop-down menu.

Table 92: NTP Configuration Sources

Source	Description
Host Configuration	The NTP servers are obtained from the host configuration.
Automatic	The NTP servers are automatically obtained from the network configured in the *Automatic Configuration Interface* drop-down menu of this subnet (“DHCP Basic Configuration” on page 137).
Static	You manually enter the value.

Static Configuration Source Only

4. If the configuration source is **Static**, enter the static addresses of up to four NTP servers in the following fields:

- Primary NTP
- Secondary NTP
- Third NTP
- Fourth NTP

5. Click *Submit* if you do not need to set other parameters.

NBNS (Option 44)

The NetBIOS Name Server (NBNS) protocol, part of the NetBIOS over TCP/IP (NBT) family of protocols, is implemented in Windows systems as the Windows Internet Name Service (WINS). By design, NBNS allows network peers to assist in managing name conflicts.

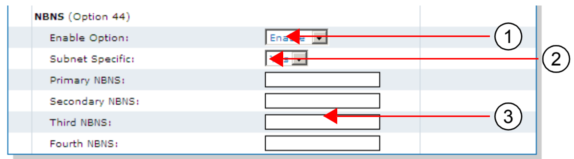
The Aastra unit DHCP server offers up to four NBNS addresses to its subnets. You can use the default NBNS addresses for all subnets or define static NBNS addresses specific to one or more subnets.

▶ **To set the DHCP server NBNS parameters:**

1. In the *NBNS (Option 44)* sub-section of the *DHCP Server Configuration* section, enable the NBNS servers (option 44) by selecting **Enable** in the *Enable Option* drop-down menu

This menu is available only in the specific subnets configuration.

Figure 56: DHCP Server – NBNS Option



2. Define whether or not you want to override the default values in the *Subnet Specific* drop-down menu.

This menu is available only in the specific subnets configuration.

3. Enter the static addresses of up to four NBNS servers in the following fields:

- Primary NBNS
- Secondary NBNS
- Third NBNS
- Fourth NBNS

4. Click *Submit* if you do not need to set other parameters.

DHCP Static Leases Configuration

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

The embedded DHCP server leases addresses to the hosts that request it. The address is assigned to a host for a configurable amount of time (as defined in "Lease Time (Option 51)" on page 137). The DHCP server can service all subnets on which it is enabled.

▶ **To define DHCP leases offered by the Aastra unit:**

1. In the web interface, click the *System* link, then the *DHCP Leases* sub-link.

2. In the *Static Leases Configuration* section, if applicable, delete an existing reserved IP address by selecting **Delete** in the *Action* drop-down next to an existing lease.

3. If applicable, add a new lease by entering the MAC address of the device and the IP address you want to reserve for it, then click **Submit**.

The static IP address is added to the *Static Leases Configuration* section, but not to the *Current Leases* section.

4. Click *Submit* if you do not need to set other parameters.

POTS Parameters

Page Left Intentionally Blank

C H A P T E R
20

POTS Configuration

This chapter describes how to configure the POTS (Plain Old Telephony System) line service, which allows you to configure the analog specification of each line, as well as gateways-specific parameters.

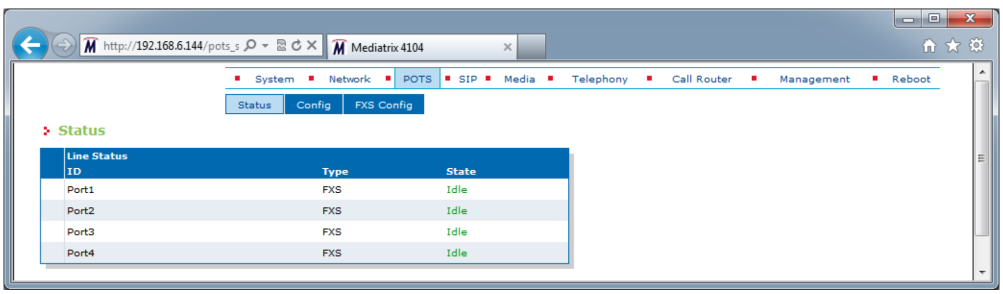
POTS Status

The POTS parameters are displayed in the *POTS / Status* page.

Line Status

The *Line Status* table lists the link state of the FXS lines.

Figure 57: POTS – Status Web Page



The *State* column may have one of the following values:

- **Idle**: The line is available
- **In Use**: The line is currently used
- **Disabled**: The line is disabled
- **Bypass**: The line is on bypass
- **Down**: The power of the line is down

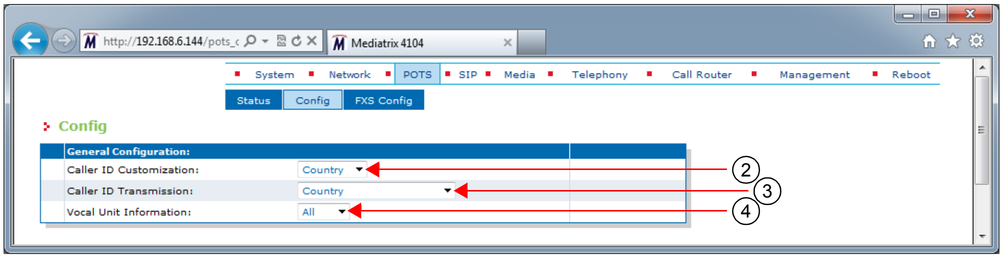
General POTS Configuration

The *General Configuration* section allows you to select the detection/generation method of caller ID.

▶ To configure the general POTS parameters:

1. In the web interface, click the *POTS* link, then the *Config* sub-link.

Figure 58: POTS Web Page



2. Select the detection/generation method of caller ID in the *Caller ID customization* drop-down menu.

   This allows selecting the detection/generation method of caller ID. See “Caller ID Information” on page 147 for more details.

Table 93: Caller ID Parameters

Parameter	Description
Country	Uses the default caller ID of the country defined in the *Country* section of the *Telephony* > *Misc* page (“Country Configuration” on page 451).
EtsiDtmf	ETSI 300 659-1 (DTMF string sent between the first and second ring).
EtsiFsk	ETSI 300 659-1 (FSK (V.21) sent between the first and second ring).

3. Select the caller ID transmission method in the *Caller ID Transmission* drop-down menu.

   It allows selecting the transmission type of the caller ID.

Table 94: Caller ID Transmission Parameters

Parameter	Description
Country	Uses the default caller ID of the country defined in the *Country* section of the *Telephony* > *Misc* page (“Country Configuration” on page 451).
First Ring	The caller ID is sent after the first ring.
Ring Pulse	The caller ID is sent between a brief ring pulse and the first ring.
Line Reversal Ring Pulse	The caller ID is sent between a brief ring pulse and the first ring on an inverted polarity line.
DT-AS	The caller ID is sent after the dual tone alerting state tone.
Line Reversal DT-AS	The caller ID is sent after the dual tone alerting state tone on an inverted polarity line.
No Ring Pulse	The caller ID is sent before the first ring.

4. Determine the type of vocal information that can be obtained by dialing a pre-defined digit map in the *Vocal Unit Information* drop-down menu.

   When entering special characters on your telephone pad, the Aastra unit talks back to you with relevant information.

Table 95: Caller ID Parameters

Parameter	Description
None	The vocal information feature is disabled.

Table 95: Caller ID Parameters (Continued)

Parameter	Description
All	Enable all vocal information digit maps.

To access the vocal unit information:

a. Take one of the telephones connected to the Aastra unit.

b. Dial one of the digits sequence on the keypad.

Table 96: Vocal Unit Information

Digits to Dial	Information Vocally Sent by the Aastra unit
*#*0	List of IP addresses of the Aastra unit (static or DHCP).
*#*1	MAC address of the Aastra unit.
*#*8	Firmware version number of the Aastra unit.

5. Click *Submit* if you do not need to set other parameters.

Caller ID Information

The caller ID is a generic name for the service provided by telephone utilities that supply information such as the telephone number or the name of the calling party to the called subscriber at the start of a call. In call waiting, the caller ID service supplies information about a second incoming caller to a subscriber already busy with a phone call. However, note that caller ID on call waiting is not supported by all caller ID-capable telephone displays.

In typical caller ID systems, the coded calling number information is sent from the central exchange to the called telephone. This information can be shown on a display of the subscriber telephone set. In this case, the caller ID information is usually displayed before the subscriber decides to answer the incoming call. If the line is connected to a computer, caller information can be used to search in databases and additional services can be offered.

The following basic caller ID features are supported:

- Date and Time
- Calling Line Identity
- Calling Party Name
- Visual Indicator (MWI)

Caller ID Generation

There are two methods used for sending caller ID information depending on the application and country-specific requirements:

- caller ID generation using DTMF signalling
- caller ID generation using Frequency Shift Keying (FSK)

Note: The Dgw v2.0 Application does not support ASCII special characters higher than 127.

The displayed caller ID for all countries may be up to 20 digits for numbers and 50 digits for names.

DTMF Signalling

The data transmission using DTMF signalling is performed during or before ringing depending on the country settings or endpoint configuration. The Aastra unit provides the calling line identity according to the following standards:

- Europe: ETSI 300 659-1 January 2001 (Annex B): Access and Terminals (AT); Analogue access to the Public Switched Telephone Network (PSTN); Subscriber line protocol over the local loop for display (and related) services; Part 1: On-hook data transmission.

FSK Generation

Different countries use different standards to send caller ID information. The Aastra unit is compatible with the following widely used standards:

- ETSI 300 659-1

Note: The compatibility of the Aastra unit is not limited to the above caller ID standards.

Continuous phase binary FSK modulation is used for coding that is compatible with:

- BELL 202
- ITU-T V.23

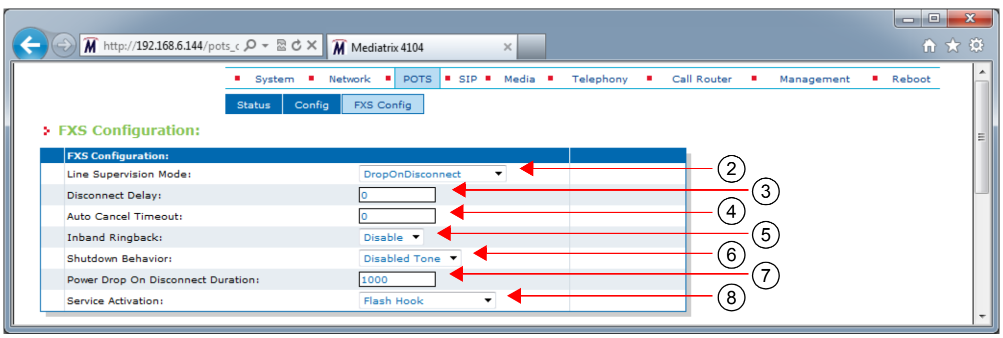
FXS Configuration

The *FXS Configuration* section allows you to define how a FXS endpoint behaves in certain conditions.

To configure the FXS parameters:

1. In the web interface, click the *POTS* link, then the *FXS Config* sub-link.

Figure 59: FXS Config Web Page



2. In the *FXS Configuration* section, set the *Line Supervision Mode* drop-down menu with the power drop and line polarity used to signal the state of a line.

   Power drop and polarity reversal are also called battery drop and battery reversal.

Table 97: Line Supervision Mode Parameters

Parameter	Description
None	Power drop or polarity reversal is not used to signal the state of the line.
DropOnDisconnect	Activates the Power Drop on Disconnect feature. A short power drop is made at the end of a call when the call is disconnected by the remote party. The drop duration can be configured in the *FXS Power Drop on Disconnect Duration* field (Step 5).

Table 97: Line Supervision Mode Parameters (Continued)

Parameter	Description
ReversalOnIdle	Activates the Polarity Reversal on Idle feature. The polarity of the line is initially in reversed state. The polarity of the line returns to the positive state when the user seizes the line or when the line rings for an incoming call. The polarity of the line is reversed again when the call is disconnected.
ReversalOnEstablished	Activates the Polarity Reversal on Established option. The polarity of the line is initially in the positive state. The polarity of the line is reversed when the call is established and returns to the positive state when the call is disconnected.

3. Set the *Disconnect Delay* field with the value used to determine whether or not call clearing occurs as soon as the called user is the first to hang up a received call.

   This parameter has no effect when you are acting as the calling party.

   If you set the value to **0**, the call is disconnected as soon as the called user hangs up the call.

   If the value is greater than 0, that value is the amount of time, in seconds, the unit waits after the called user hangs up before signalling the end of the call.

4. Set the *Auto Cancel Timeout* field with the time, in seconds, the endpoint rings before the call is automatically cancelled.

   Setting this variable to **0** disables the timeout. Calls will not be automatically cancelled and will ring until the party answers.

5. Set the *Inband Ringback* drop-down menu to define whether or not the FXS endpoint needs to generate a ringback for incoming ringing call.

Table 98: Inband Ringback Parameters

Parameter	Description
Disable	The FXS endpoint does not play local ringback to the remote party.
Enable	The FXS endpoint plays local ringback to the remote party via the negotiated media stream. The local ringback is generated only when the telephone is on-hook. The FXS ports never play the local ringback for the call waiting.

6. Set the *Shutdown Behavior* drop-down menu with the FXS endpoint behavior when it becomes shut down.

Table 99: FXS Shutdown Behavior Parameters

Parameter	Description
Disabled Tone	A disabled tone is played when the user picks up the telephone and the FXS endpoint is shut down.
Power Drop	The loop current is interrupted when the FXS endpoint is shut down and no tone is played when the user picks up the telephone.

A FXS endpoint becomes shut down when the operational state of the endpoint becomes *Disabled* and the *Shutdown Endpoint When Operational State is 'Disable' And Its Usage State Is 'idle-unusable'* parameter of the *SIP* > *Endpoints* page is set to **Enable**. See "Administration" on page 68 for more details.

This parameter is not used by FXS endpoints used for bypass when the *Activation* column of the *FXS Bypass* section is set to **Endpoint Disabled**. See "FXS Bypass" on page 167 for more details.

7. Set the *Power Drop on Disconnect Duration* field with the power drop duration, in milliseconds, that is made at the end of a call when the call is disconnected by the remote party.

This value only has an effect when the *Line Supervision Mode* drop-down menu is set to **DropOnDisconnect**.

8. Set the *Service Activation* drop-down menu with the method used by the user to activate supplementary services such as call hold, second call, call waiting, call transfer and conference call.

Table 100: Service Activation Parameters

Parameter	Description
Flash Hook	Service activation is performed by flash hook or hanging up.
Flash Hook And Digit	Service activation is performed by flash hook, flash hook followed by a digit or hanging up. The digit dialed has a different behaviour depending on the current call context: • One call active and one waiting call: Flash hook then dial the digit 2: Answer the waiting call. • One call active and one call on hold: Flash hook then dial the digit 1: Terminate the active call and recover the call on hold. Flash hook then dial the digit 2: Hold the active call and recover the call on hold. Flash hook then dial the digit 3: Enter the conference mode. Flash hook then dial the digit 4: Transfer the call on hold to the active call. When hanging up in this context, the telephone rings to notify the user there is still a call on hold. • In conference mode: Flash hook then dial the digit 2: Return to one active call and one call on hold. When hanging up in this context, all calls are finished.

9. Click *Submit* if you do not need to set other parameters.

FXS Country Customization

The *FXS Country Customization* section allows you to override the current default country parameters of certain features. Refer to “Appendix A - Country-Specific Parameters” on page 603 for the pre-defined values for a specific country.

▶ **To define the FXS country customization parameters:**

1. In the *FXS Country Configuration* section, select whether or not you want to override the current country parameters in the *Override Country Customization* drop down menu.

This allows overriding FXS related default country settings for the loop current and flash hook detection features.

Figure 60: FXS Country Customization Section

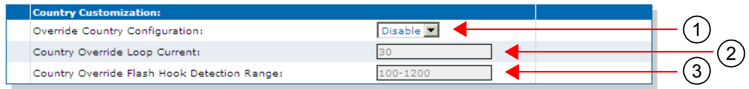


Table 101: Line Supervision Mode Parameters

Parameter	Description
Disable	The line uses the default country FXS settings.
Enable	The line uses the FXS country configuration set in the following steps.

2. Set the *Country Override Loop Current* field with the loop current generated by the FXS port in ma.

When a remote end-user goes on-hook, the Aastra unit signals the far end disconnect by performing a current loop drop (< 1 mA) on the analog line. This current loop drop, also referred to as “Power Denial” mode, is typically used for disconnect supervision on analog lines. The Aastra unit maintains a current drop for one second (this value cannot be configured), then a busy tone is generated to indicate the user to hang up. See the description for the *FXS Line Supervision Mode* drop-down menu in “FXS Configuration” on page 148 for more details.

When one of its analog lines goes off-hook, the Aastra unit controls the endpoint in a fixed loop current mode. When selecting a country (see “Country Configuration” on page 451 for more details), each country has a default loop current value. However, you can override this value and define your own loop current.

Note that the actual measured current may be different than the value you set, because it varies depending on the DC impedance.

3. Set the *Country Override Flash Hook Detection Range* field.

This is the range in which the hook switch must remain pressed to perform a flash hook.

When selecting a country (see “Country Configuration” on page 451 for more details), each country has a default minimum and maximum time value. However, you can override these values and define your own minimum and maximum time within which pressing and releasing the plunger is actually considered a flash hook.

The range consists of the minimal delay and maximal delay, in ms, separated by a “-”. The minimal value allowed is 10 ms and the maximum value allowed is 1200 ms. The space character is not allowed.

Flash hook can be described as quickly depressing and releasing the plunger in or the actual handset-cradle to create a signal indicating a change in the current telephone session. Services such as picking up a call waiting, second call, call on hold, and conference are triggered by the use of the flash hook.

A flash hook is detected when the hook switch is pressed for a shorter time than would be required to be interpreted as a hang-up.

Using the “flash” button that is present on many standard telephone handsets can also trigger a flash hook.

4. Click *Submit* if you do not need to set other parameters.

Calling Party Name of the Caller ID

Standards Supported	• ETSI EN 300659-3[a]

a. CLIR section

1. In the *potsMIB*, specify the Calling Party Name of the caller ID (CLIP) when the calling party is tagged as private in the `FxsCallerIdPrivateCallingPartyName` variable.

You can also use the following line in the CLI or a configuration script:

```
pots.FxsCallerIdPrivateCallingPartyName="Value"
```

Value may be any string of characters up to 50 characters.

- When empty, no Calling Party Name parameter is sent.
- When set to 'P', no Calling Party Name parameter is sent but a Reason for Absence or Caller Party Name parameter is sent with the value 0x50 (Private).

SIP Parameters

Page Left Intentionally Blank

C H A P T E R
21

SIP Gateways

This chapter describes how to add and remove SIP gateways in the Aastra unit.

SIP Gateways Configuration

Multiple SIP gateways may be used for a number of reasons, such as:

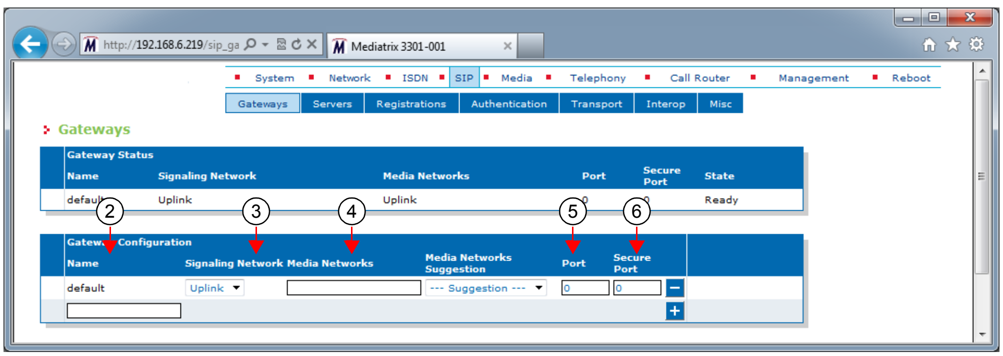
- Redirecting ISDN calls to different SIP servers depending on the call.
- Hunt calls across several gateways.

Adding a SIP gateway triggers a warning message if the total number of registrations configured reached the defined limit. See “Number of Registrations” on page 293 for more details.

To configure multiple SIP gateways:

1. In the web interface, click the *SIP* link, then the *Gateways* sub-link.

Figure 61: SIP – Gateways Web Page



You can add a new gateway by clicking the + button. The Aastra unit supports a maximum of 5 gateways.

You can delete an existing gateway by clicking the − button.

2. If you are adding a new gateway, enter its name in the *Name* field.

The Dgw v2.0 Application supports only alphanumeric characters, “-”, and “_”.

3. Select the network interface on which the gateway listens for incoming SIP traffic in the *Signaling Network* drop-down menu.

This value applies to all transports (e.g., UDP, TCP, etc.).

The LAN interface may be used as a SIP gateway to be bound on the LAN. However, there is no routing between the LAN and the uplink interface.

4. Define the list of networks (separated by ",") to use for the media (voice, fax, etc.) stream in the *Media Networks* field.

You can use the *Media Networks Suggestion* column’s drop-down menu to select between suggested values, if any.

The value must match one of the "InterarfaceName" values in the "NetworkInterfacesStatus" table of the BNI service. The order in the list defines the priority.

When the media stream is negotiated, the following rules apply:

- If the list of media networks is empty,the Aastra unit uses the IP address of the network defined in the *Signaling Network* drop-down menu.
- Only active networks are used.
- Only the first active network of an IP address family (IPv4, IPv6) is used. All subsequent networks of the same IP family are ignored.

Note: When generating an offer and multiple networks are available for the media, ANAT grouping (RFC 4091) is automatically enabled. When generating an answer, the ANAT grouping state is detected form the offer.

5. Set the SIP port on which the gateway listens for incoming unsecure SIP traffic in the *Port* field.

This is used only when the UDP and/or TCP transports are enabled.

If two or more SIP gateways use the same port, only the first SIP gateway starts correctly. The others are in error and not started. The SIP gateway is also in error and not started if the port is already used.

The default value is 0. If you set the port to 0, the default SIP port 5060 is used.

Note: The port “0” is the equivalent to the “well known port”, which is 5060 in SIP. Using 0 and 5060 is not the same. At the SIP packets level, if you set the port to **0**, it will not be present in the SIP packet. If you set the port to **5060**, it will be present in the SIP packet. For example: “23@test.com” if the port is 0 and “23@test.com:5060” if the port is 5060.

6. Set the SIP port on which the gateway listens for incoming secure SIP traffic in the *Secure Port* field.

This is used only when the TLS transport is enabled.

The default value is 0. If you set the port to 0, the default secure SIP port 5061 is used.

Note: The port “0” is the equivalent to the “well known port”, which is 5061 in SIP for TLS. Using 0 and 5061 is not the same. At the SIP packets level, if you set the port to **0**, it will not be present in the SIP packet. If you set the port to **5061**, it will be present in the SIP packet. For example: “23@test.com” if the port is 0 and “23@test.com:5061” if the port is 5061.

7. Click *Submit* if you do not need to set other parameters.

The state of the SIP gateways is displayed in the *SIP Gateway Status* section.

Table 102: SIP Gateway States

State	Description
Ready	The gateway is ready to make and receive calls.
Cannot start, port already in use	The gateway cannot open its IP port because the port is already used by another service. This generally occurs when the administrator adds a new gateway but forgets to configure a different IP port.
Network down	The SIP gateway is not started or the network interface on which the SIP gateway is associated does not have an IP address.
Restarting	The SIP gateway cannot make or receive calls while it is restarting.
Waiting for time synchronization	The gateway is started but it cannot open its SIP TLS port because the real-time clock is not synchronized. This generally occurs when the SNTP server is not set or is unreachable.
Server unreachable	The gateway is started but it cannot make and receive calls because the SIP server is unreachable. This state is only reported when a KeepAlive mechanism is used.

Table 102: SIP Gateway States (Continued)

State	Description
Unregistered	Indicates some registrations that are mandatory for this gateway failed. See “Unregistered User Behaviour” on page 297 for more details.

CHAPTER 22

SIP Servers

This chapter describes how to configure the SIP server parameters of the Aastra unit.

Standards Supported	• RFC 2543: SIP: Session Initiation Protocol • RFC 3261: The Session Initiation Protocol (SIP) • RFC 3903: Session Initiation Protocol (SIP) Extension for Event State Publication

It describes the following:

- How to define the SIP servers IP information.
- How to define the SIP gateways IP information.

Introduction

The Aastra unit uses the following types of servers:

Table 103: SIP Servers

Server	Description
Registrar Server	Accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles.
Proxy Server	An intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, which means its job is to ensure that a request is passed on to another entity that can further process the request. Proxies are also useful for enforcing policy and for firewall traversal. A proxy interprets, and, if necessary, rewrites parts of a request message before forwarding it.
Outbound Proxy Server	An intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. The outbound proxy receives all outbound traffic and forwards it. Incoming traffic may or may not go through the outbound proxy. The outbound proxy's address is never used in the SIP packets, it is only used as a physical network destination for the packets. When the outbound proxy is enabled, the proxy is still used to create the *To* and *From* headers, but the packets are physically sent to the outbound proxy.
Messaging Server Host	A Messaging system host is a server that accepts MWI SUBSCRIBE requests and places the information it receives in those requests into the location service for the domain it handles.

SIP Outbound Proxy (From RFC 3261)

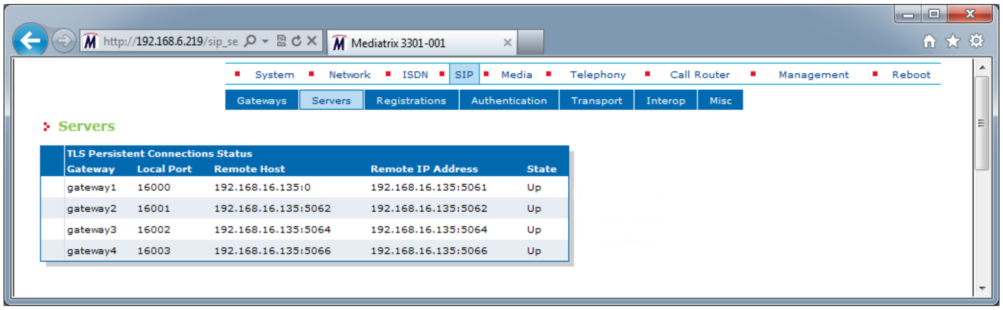
A proxy that receives requests from a client, even though it may not be the server resolved by the Request-URI. Typically, a user agent is manually configured with an outbound proxy.

When enabled, the initial route for all SIP requests contains the outbound proxy address, suffixed with the loose routing parameter "lr". The Request-URI still contains the home domain proxy address. Requests are directed to the first route (the outbound proxy).

TLS Persistent Connections Status

The TLS Persistent Connections Status table allows you to browse the status of the TLS persistent connections of the Aastra unit. These connections are associated with the SIP servers (outbound proxy, registrar and home domain proxy). Note that this section is not displayed if there is no information to show.

Figure 62: SIP – TLS Persistent Connections Status Section



The following information is available:

Table 104: TLS Persistent Connection Parameters

Parameter	Description
Gateway	The SIP gateway used to register.
Local Port	Local port used by the TLS persistent connection.
Remote Host	The remote host used to establish the TLS persistent connection. The remote host can be a host name or an IP address of the proxy, outbound proxy or registrar.
Remote IP Address	The resolved IP address of the remote host used to establish the TLS persistent connection.
Status	The current state of the TLS persistent connection. • Up: The TLS connection is established. • Down: The TLS connection is not established.

SIP Servers Configuration

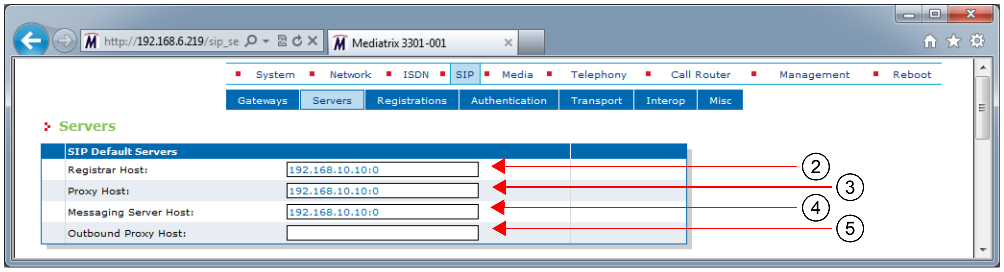
This section describes how to configure the IP address and port number of the SIP servers.

If any of the SIP servers parameters corresponds to a domain name that is bound to a SRV record, the corresponding port must be set to **0** for the unit to perform DNS requests of type SRV (as per RFC 3263). Otherwise, the unit will not use DNS SRV requests, but will rather use only requests of type A because it does not need to be specified which port to use.

▶ **To set the SIP servers configuration:**

1. In the web interface, click the *SIP* link, then the *Configuration* sub-link.

Figure 63: SIP – Servers Web Page



2. Enter the SIP registrar server static IP address or domain name and port number in the *Registrar Host* field.

   You must enter the information as `IP address:Port number`. For instance:
   `192.168.0.5:5060`

3. Enter the SIP Proxy server static IP address or domain name and port number in the *Proxy Host* field.

   You must enter the information as `IP address:Port number`. For instance:
   `192.168.0.5:5060`

4. Enter the SIP outbound proxy server static IP address or domain name and port number in the *Outbound Proxy Host* field.

   The outbound proxy is enabled if the IP address is valid (i.e., not 0.0.0.0:0). Setting the address to **0.0.0.0:0** or leaving the field empty disables the outbound proxy.

5. Enter the Messaging system host static IP address or domain name and port number in the *Messaging Server Host* field.

   If the host corresponds to a domain name that is bound to a SRV record, the port must be set to **0** for the unit to perform DNS SRV queries; otherwise only type A record lookups will be used.

   You can define whether or not an endpoint needs to subscribe to a messaging system in "Endpoints Registration" on page 289.

6. Click *Submit* if you do not need to set other parameters.

Multiple SIP Gateways

The Aastra unit allows you to have multiple SIP gateways (interfaces). You can configure each SIP gateway to register to a specific registrar. You can also configure each SIP gateway to send all requests to an outbound proxy. See "Chapter 24 - SIP Gateways" on page 277 for more details.

SIP Gateway Specific Registrar Servers

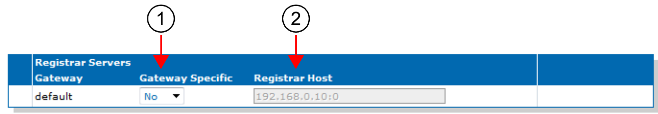
This section allows you to define whether the available SIP gateways use the default registrar server or rather use a specific registrar server.

▶ **To set specific registrars servers information:**

1. In the *Registrar Servers* section of the *Servers* page, select whether or not a SIP gateway uses a specific registrar server in the *Gateway Specific* drop-down menu.

   If you select **No**, the SIP gateway uses the server information as set in the *SIP Default Servers* section.

Figure 64: SIP Servers – Specific Registrar Section



2. Enter the IP address or domain name and port number of the registrar server currently used by the registration in the *Registrar Host* field.

You must enter the information as `IP address:Port number`. For instance:

`192.168.0.5:5060`

3. If you do not need to set other parameters, do one of the following:

- To save your settings without refreshing the registration, click *Submit*.
- To save your settings and refresh the registration now, click *Submit & Refresh Registration*.

SIP Gateway Specific Messaging Servers

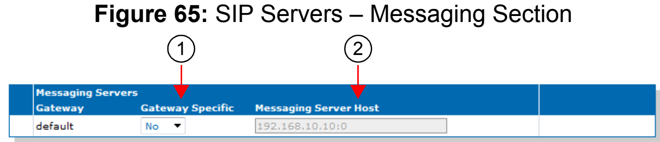
This section allows you to define whether the available SIP gateways use the default proxy and outbound proxy server or rather use specific servers.

▶ **To set specific proxy servers information:**

1. In the *Messaging Servers* section of the *Servers* page, select whether or not a SIP gateway uses a specific proxy and outbound proxy server in the *Gateway Specific* drop-down menu.

If you select **No**, the SIP gateway uses the server information as set in the *SIP Default Servers* and Messaging Subscription (“Messaging Subscription” on page 349) sections.

Figure 65: SIP Servers – Messaging Section



2. Enter the IP address or domain name and port number of the messaging server currently used by the registration in the *Proxy Host* field.

You must enter the information as `IP address:Port number`. For instance:

`192.168.0.5:5060`

3. Enter the IP address or domain name and port number of the outbound proxy server currently used by the registration in the *Outbound Proxy Host* field.

You must enter the information as `IP address:Port number`. For instance:

`192.168.0.5:5060`

The outbound proxy is enabled if the IP address is valid (i.e., not 0.0.0.0:0). Setting the address to **0.0.0.0:0** or leaving the field empty disables the outbound proxy.

4. If you do not need to set other parameters, do one of the following:

- To save your settings without refreshing the registration, click *Submit*.
- To save your settings and refresh the registration now, click *Submit & Refresh Registration*.

SIP Gateway Specific Proxy Servers

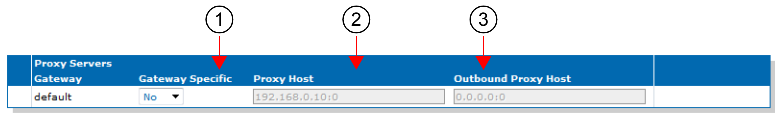
This section allows you to define whether the available SIP gateways use the default proxy and outbound proxy server or rather use specific servers.

▶ **To set specific proxy servers information:**

1. In the *Proxy Servers* section of the *Servers* page*,* select whether or not a SIP gateway uses a specific proxy and outbound proxy server in the *Gateway Specific* drop-down menu.

If you select **No**, the SIP gateway uses the server information as set in the *SIP Default Servers* section.

Figure 66: SIP Servers – Specific Proxy Section



2. Enter the IP address or domain name and port number of the proxy server currently used by the registration in the *Proxy Host* field.

You must enter the information as `IP address:Port number`. For instance:

`192.168.0.5:5060`

3. Enter the IP address or domain name and port number of the outbound proxy server currently used by the registration in the *Outbound Proxy Host* field.

You must enter the information as `IP address:Port number`. For instance:

`192.168.0.5:5060`

The outbound proxy is enabled if the IP address is valid (i.e., not 0.0.0.0:0). Setting the address to **0.0.0.0:0** or leaving the field empty disables the outbound proxy.

4. If you do not need to set other parameters, do one of the following:

- To save your settings without refreshing the registration, click *Submit*.
- To save your settings and refresh the registration now, click *Submit & Refresh Registration*.

Keep Alive

You can select the method used to perform the SIP keep alive mechanism. With this mechanism, the Aastra unit sends messages periodically to the server to ensure that it can still be reached.

▶ **To use the SIP keep alive mechanism:**

1. In the *Keep Alive* section of the *Servers* page, select the keep alive method to use in the *Keep Alive Method* drop-down menu.

Figure 67: Keep Alive Section

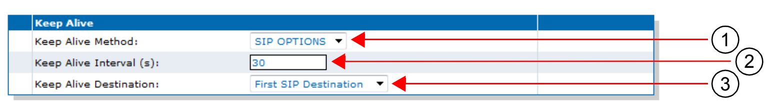


Table 105: Keep Alive Parameters

Parameter	Description
None	No keep alive is performed.

Table 105: Keep Alive Parameters (Continued)

Parameter	Description
SipOptions	SIP OPTIONS are sent periodically for each gateway to the corresponding server. Any response received from the server means that it can be reached. No additional processing is performed on the response. If no response is received after the retransmission timer expires (configurable via the *Transmission Timeout* field in "SIP Interop" on page 312), the gateway considers the server as unreachable. In this case, any call attempt through the gateway is refused. SIP OPTIONS are still sent when the server cannot be reached and as soon as it can be reached again, new calls are allowed.
Ping	A Ping is sent periodically for each gateway to the corresponding server. The response received from the server means that it is reachable. If no response is received after the retransmission timer expires (configurable via the *Transmission Timeout* field in "SIP Interop" on page 312), the gateway considers the server as unreachable. In this case, any call attempt through the gateway is refused. The Pings are still sent when the server is unreachable and as soon as it becomes reachable again, new calls are allowed.

2. Set the interval, in seconds, at which SIP Keep Alive requests using SIP OPTIONS or Ping are sent to verify the server status in the *Keep Alive Interval* field.
3. Select the behaviour of the device when performing the keep alive action in the *Keep Alive Destination* drop-down menu.

Table 106: SIP Keep Alive Destination Parameters

Parameter	Description
First SIP Destination	Performs the keep alive action through the first SIP destination. This corresponds to the outbound proxy host when specified, otherwise it is the proxy host.
Alternate Destination	Performs the keep alive action through the alternate destination target (see "SIP Gateway Specific Keep Alive Destinations" on page 164 for more details).

4. Click *Submit* if you do not need to set other parameters.

SIP Gateway Specific Keep Alive Destinations

This section allows you to override the default Keep Alive destination alternate target when the *Keep Alive Destination* drop-down menu is set to **Alternate Destination** (see "Keep Alive" on page 163 for more details).

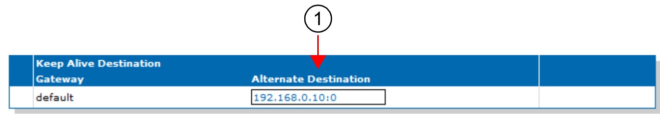
▶ **To set specific keep alive destinations:**

1. In the *Keep Alive Destinations* section of the *Servers* page, set the Alternate destination target server FQDN and port for a specific SIP gateway in the *default* field.

   You must enter the information as `IP address:Port number`. For instance:

   `192.168.0.5:5060`

Figure 68: SIP Servers – Specific Keep alive Targets



2. Click *Submit* if you do not need to set other parameters.

Outbound Proxy Loose Router Configuration

Standards Supported	• RFC 3261: SIP: Session Initiation Protocol, section 6 • RFC 2543: SIP: Session Initiation Protocol

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

You can specify the type of routing of the outbound proxy configured in “SIP Servers Configuration” on page 160.

You can use two types of configuration:

- Default configurations that apply to all the endpoints of the Aastra unit.
- Specific configurations that override the default configurations.

  You can define specific configurations for each endpoint in your Aastra unit. For instance, you could enable a codec for all the endpoints of the Aastra unit and use the specific configuration parameters to disable this same codec on one specific endpoint.

Using one or more specific parameter usually requires that you enable an override variable and set the specific configuration you want to apply.

The following types are available:

Table 107: Outbound Proxy Router Status

Type	Description
LooseRouter	This is the most current method for SIP routing, as per RFC 3261, and will become the standard behaviour once RFC 3261 compliance is achieved. See “Introduction” on page 159 for details.
StrictRouter	Pre-RFC 3261, RFC 2543 compatible SIP routing. The initial route for all SIP requests contains the home domain proxy address (the Request-URI). Requests are directed to the outbound proxy. In other words, the Request-URI is constructed as usual, using the home domain proxy and the user name, but is used in the route set. The Request-URI is filled with the outbound proxy address.

Loose Router

A proxy is said to be loose routing if it follows the procedures defined in the *RFC 3261* specification (section 6) for processing of the *Route* header field. These procedures separate the destination of the request (present in the Request-URI) from the set of proxies that need to be visited along the way (present in the *Route* header field). A proxy compliant to these mechanisms is also known as a loose router.

Table 107: Outbound Proxy Router Status (Continued)

Type	Description
NoRouteHeader	Removes the route header from all SIP packets sent to an outbound proxy. This does not modify persistent TLS connection headers. **Note:** The Router header will not be removed from the SIP packets if the unit is configured to use the TLS Fallback feature. This feature requires the information of the SIP Outbound Proxy in the SIP packet to work correctly.

▶ **To set the outbound proxy router status:**

1. In the *sipEpMIB*, set the `defaultProxyOutboundType` variable to the proper value.

   You can also use the following line in the CLI or a configuration script:

   ```
   sipEp.defaultProxyOutboundType="Value"
   ```

   where *Value* may be one of the following:

   Table 108: Outbound Proxy Router Values

Value	Meaning
100	LooseRouter
200	StrictRouter
300	NoRouteHeader

2. If you want to set a different routing type for one or more SIP gateways, set the following variables:

   - `gwSpecificproxyEnableConfig` variable for the specific SIP gateway you want to configure to **enable**.
   - `gwSpecificProxyOutboundType` variable for the specific SIP gateway you want to configure to the proper value.

   You can also use the following lines in the CLI or a configuration script:

   ```
   sipEp.gwSpecificProxy.EnableConfig[GatewayName="default"]="1"
   sipEp.gwSpecificProxy.OutboundType[GatewayName="Specific_Gateway"]="Value"
   ```

   where:

   - *Specific_Gateway* is the name of the SIP gateway you want to configure.
   - *Value* is the refresh router status as defined in Step 1.

CHAPTER

23

SIP Registration

This chapter describes how to configure the registration parameters of the Aastra unit.

Standards Supported	• RFC 2543: SIP: Session Initiation Protocol • RFC 3261: The Session Initiation Protocol (SIP) • RFC 3863: Presence Information Data Format (PIDF) • RFC 3903: Session Initiation Protocol (SIP) Extension for Event State Publication

Endpoints Registration

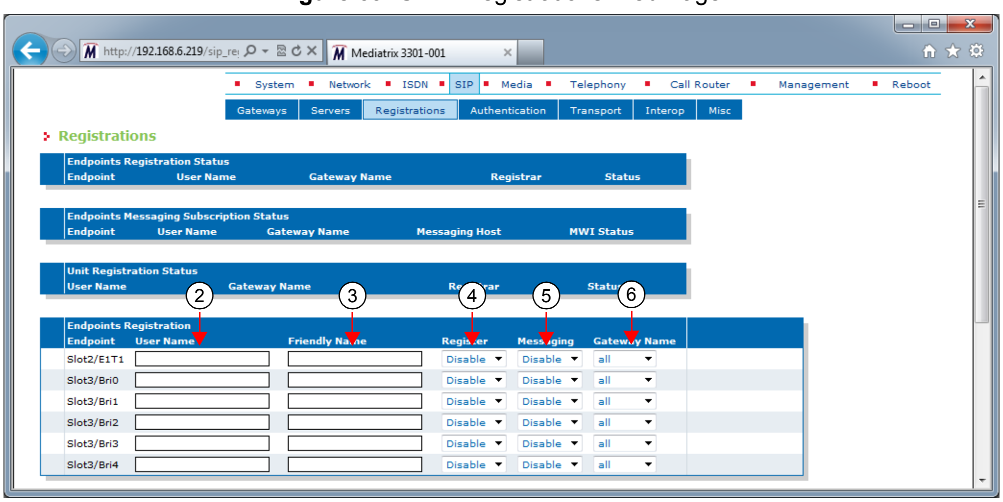
Each endpoint of the Aastra unit has its own registration information. You can set information for each endpoint such as its telephone number and friendly name.

Adding an endpoint registration triggers a warning message if the total number of registrations configured reached the defined limit. See "Number of Registrations" on page 171 for more details.

▶ **To set endpoints registration information:**

1. In the web interface, click the *SIP* link, then the *Registrations* sub-link.

Figure 69: SIP – Registrations Web Page



2. In the *Endpoints Registration and Subscription* section of the *Registrations* page, enter a user name for each endpoint in the *User Name* column.

The user name (such as a telephone number) uniquely identifies this endpoint in the domain. It is used to create the *Contact* and *From* headers. The *From* header carries the permanent location (IP address, home domain) where the endpoint is located. The *Contact* header carries the current location (IP address) where the endpoint can be reached.

Contacts are registered to the registrar. This enables callers to be redirected to the endpoint's current location.

3. Enter another name for each endpoint in the *Friendly Name* column.

This is a friendly name for the endpoint. It contains a descriptive version of the URI and is intended to be displayed to a user interface.

4. Define whether or not the endpoint registration needs to register to the registrar in the *Register* column.

An endpoint configured to register (set to **Enable**) will become unavailable for calls from or to SIP when not registered.

You can define the behaviour of an endpoint when it becomes unavailable in the *defaultRegistrationUnregisteredBehavior* MIB variable.

5. Define whether or not the endpoint needs to subscribe to a messaging system in the *Messaging* drop-down menu.

The current state of the subscription is displayed in the *Endpoints Messaging Subscription Status* table.

Table 109: MWI Subscription State

State	Description
Unsubscribed	The unit/endpoint is not subscribed and never tries to subscribe. This case occurs if the network interface used by the SIP gateway is not up or the unit/ endpoint is locked.
Subscribing	The subscription is currently trying to subscribe.
Subscribed	The subscription is successfully subscribed.
Refreshing	The subscription is trying to refresh.
Unreachable	The last subscription attempt failed because the messaging server is unreachable.
AuthFailed	The last subscription attempt failed because authentication was not successful.
Rejected	The last subscription attempt failed because the messaging server rejects the subscription.
ConfigError	The last subscription attempt failed because it was badly configured. Check if the username and the messaging host are not empty.
InvalidResponse	The received 200 OK response contact does not match the contact of the messaging server, or the 200 OK response for an unsubscribe contains a contact.

You can enter the address of the Messaging server in “SIP Servers Configuration” on page 282.

6. Select on which SIP gateway the user configuration is applied in the *Gateway Name* drop-down menu.

You must have SIP gateways already defined. See “Chapter 24 - SIP Gateways” on page 277 for more details. If you select **all**, the configuration applies to all gateways available.

7. If you do not need to set other parameters, do one of the following:

- To save your settings without refreshing the registration, click *Submit*.
- To save your settings and refresh the registration now, click *Submit & Refresh*.

Contact Domain

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

You can set the host part of the SIP contact field. If an empty string is specified, the listening IP address is used.

▶ **To set the contact domain:**

1. In the *sipEpMIB*, define the host part of the SIP contact field in the `userAgentDomain` variable.

   You can also use the following line in the CLI or a configuration script:

   `sipEp.userAgentDomain=[value]`

Unit Registration

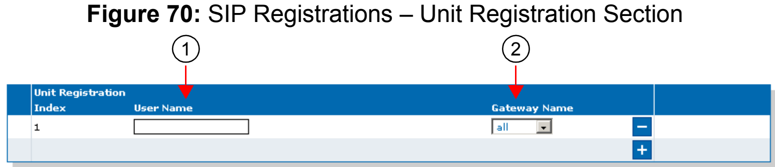
Unit registration is used to register a contact not directly related to endpoints. This is generally used to indicate to a registrar the IP location of the Aastra unit when it is used as a gateway.

Adding a unit registration triggers a warning message if the total number of registrations configured reached the defined limit. See “Number of Registrations” on page 171 for more details.

▶ **To set unit registration information:**

1. In the *Unit Registration* section of the *Registrations* page*,* enter a user name in the *User Name* column.

   Figure 70: SIP Registrations – Unit Registration Section

   The user name (such as a telephone number) uniquely identifies this user in the domain.

   You can add a new user by clicking the + button.

   You can delete an existing user by clicking the − button.

2. Select on which SIP gateway the user configuration is applied in the *Gateway Name* drop-down menu.

   You must have SIP gateways already defined. See “Chapter 24 - SIP Gateways” on page 277 for more details. If you select **all**, the configuration applies to all gateways available.

3. If you do not need to set other parameters, do one of the following:
   - To save your settings without refreshing the registration, click *Submit*.
   - To save your settings and refresh the registration now, click *Submit & Refresh*.

Registration Configuration

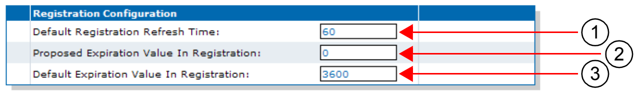
This section allows you to define registration refresh parameters.

See “Additional Registration Refresh Parameters” on page 172 for more registration parameters.

▶ To set the registration configuration:

1. In the *Registration Configuration* section of the *Registrations* page*,* set the *Default Registration Refresh Time* field with the time, in seconds, at which a registered unit begins updating its registration before the registration expiration.

Figure 71: SIP Registrations – Registration Configuration Section



In SIP, a registration is valid for a period of time defined by the registrar. Once a unit is registered, the SIP protocol requires the User Agent to refresh this registration before the registration expires. Typically, this re-registration must be completed before the ongoing registration expires, so that the User Agent's registration state does not change (i.e., remains 'registered').

For instance, if the parameter is set to 43 and the registration lasts one hour, the unit will send new REGISTER requests 59 minutes and 17 seconds after receiving the registration acknowledgement (43 seconds before the unit becomes unregistered).

> **Note:** Normally, the Aastra unit cannot make or receive calls until the REGISTER has completed successfully. Because the timeout for a SIP transaction in UDP is 32 seconds, it is possible to have an ongoing re-REGISTER transaction at the same moment that the registration itself expires. This could happen if the *Default Registration Refresh Time* field is set to a value lower than 32.
>
> In that case, the user agent becomes unregistered, and will become registered again only when the re-REGISTER request is answered with a positive response from the server. See “Gateway Specific Registration Retry Time” on page 174 for a workaround if the unit cannot make calls during that period.

Setting this parameter to 0 means that the User Agent will fall into the 'unregistered' state BEFORE sending the re-REGISTER requests.

This value MUST be lower than the value of the "expires" of the contact in the 200 OK response to the REGISTER, otherwise the unit rapidly sends REGISTER requests continuously.

You can also set a different registration refresh time for one or more SIP gateways by using the MIB parameters of the Aastra unit. See “Registration Refresh” on page 172 for more details.

2. Set the *Proposed Expiration Value In Registration* field with the suggested expiration delay, in seconds, of a contact in the REGISTER request.

The SIP protocol allows an entity to specify the “expires” parameter of a contact in a REGISTER request. The server can return this “expires” parameter in the 200 OK response or select another “expires”. In the REGISTER request, the “expires” is a suggestion the entity makes.

The “expires” parameter indicates how long, in seconds, the user agent would like the binding to be valid.

Available values are from 1 s to 86,400 s (one day).

This value does not modify the delay before a re-REGISTER.

- The delay is the “expires” of the contact in the 200 OK response to the REGISTER request minus the value set in the *Default Registration Refresh Time* field.
- If the “expires” of the contact in the 200 OK response to the REGISTER is not present or not properly formatted, then the delay is the default registration proposed expiration value minus the value set in the *Default Registration Refresh Time* field.

Setting the parameter to **0** disables the expiration suggestion.

You can also set a different expiration delay for one or more SIP gateways by using the MIB parameters of the Aastra unit. See “Registration Expiration” on page 173 for more details.

3. Set the *Default Expiration Value in Registration* field with the default registration expiration, in seconds.

This value is used when the contact in a registration response contains no “expires” or the “expires” is badly formatted. In this case, the delay before a re-REGISTER is the value set in this field minus the value set in the *Default Registration Refresh Time* field (Step 1).

You can also set a different expiration value in registration for one or more SIP gateways by using the MIB parameters of the Aastra unit. See “Expiration Value in Registration” on page 173 for more details.

4. If you do not need to set other parameters, do one of the following:

- To save your settings without refreshing the registration, click *Submit*.
- To save your settings and refresh the registration now, click *Submit & Refresh*.

Number of Registrations

The Aastra unit limits the total number of registrations to 100. The total number of registrations is the sum of all the endpoints and gateways (“SIP Gateways Configuration” on page 277) pairs. The Aastra unit supports a maximum of 5 gateways. An endpoint configured with "All" gateways generates as many pairs as the number of gateways. In a setup with 3 gateways, one endpoint configured with "All" as the gateway name counts for 3 in the total number of registrations.

The registrations are enabled gateway by gateway until the limit is reached. Endpoints Registrations are used first, then Unit Registrations. The remaining registrations are not registered and do not appear in the status table. If you click the **Submit And Refresh** button and the configured number of registrations exceeds the defined limit, a warning is displayed on the web interface (as well as in the CLI and SNMP interfaces) and a syslog notify (Level Error) is sent.

Adding a gateway or an endpoint triggers a warning message if the total number of registrations configured reached the defined limit.

Let’s suppose for instance that we have the current SIP Gateways configuration and the following SIP Registration configuration:

Figure 72: Example, Gateway Configuration

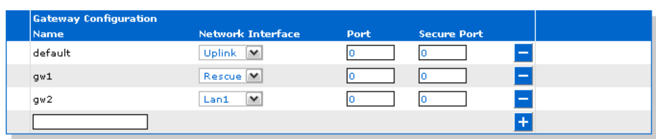
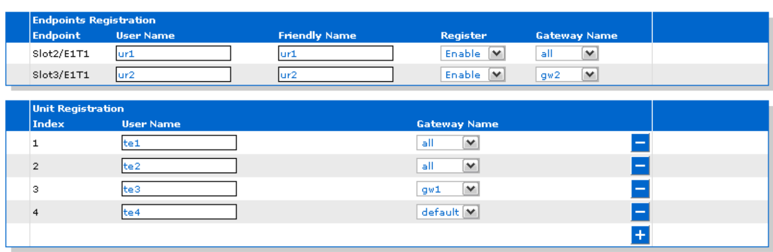


Figure 73: Example, Registrations Configuration



The following table describes how to compute the total number of registrations for this example:

Table 110: Number of Registrations Example

Parameter	Setting	Nb of Registrations
Endpoint Registration 1 in Figure 73	*Gateway Name* set to **all**[a]	3
Endpoint Registration 2 in Figure 73	*Gateway Name* set to **gw2**	1
Unit Registration 1 in Figure 73	*Gateway Name* set to **all**	3
Unit Registration 2 in Figure 73	*Gateway Name* set to **all**	3
Unit Registration 3 in Figure 73	*Gateway Name* set to **gw1**	1
Unit Registration 4 in Figure 73	*Gateway Name* set to **default**	1

Table 110: Number of Registrations Example (Continued)

Parameter	Setting	Nb of Registrations
Total Number of registrations		12

a. When the Gateway Name is set to all, this must be multiplied by the number of gateways set in Figure 72. In this example, there are 3 gateways set.

Additional Registration Refresh Parameters

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

Default Registration Retry Time

You can configure the interval in seconds (s) on which a failed registration is retried.

This variable defines the time, relative to the failure of the registration, at which the device retries the registration.

To specify the default registration retry time value:

1. In the *sipEpMIB*, locate the *registrationGroup* folder.
2. Set the `DefaultRegistrationRetryTime` variable with the desired interval value.

   You can also use the following line in the CLI or a configuration script:

   `sipEp.DefaultRegistrationRetryTime="Value"`

   where *Value* may be between 1 and 86400 seconds.

Default vs. Specific Configurations

You can use two types of configuration:

- Default configurations that apply to all the endpoints of the Aastra unit.
- Specific configurations that override the default configurations.

  You can define specific configurations for each endpoint in your Aastra unit. For instance, you could enable a codec for all the endpoints of the Aastra unit and use the specific configuration parameters to disable this same codec on one specific endpoint.

Using one or more specific parameter usually requires that you enable an override variable and set the specific configuration you want to apply.

Registration Refresh

You can set the default registration refresh time in the web page (“Registration Configuration” on page 169), but you can also set a different registration refresh time for one or more SIP gateways.

To set registration refresh parameters:

1. In the *sipEpMIB*, locate the *registrationGroup* folder.
2. If you want to set a different registration refresh time for one or more SIP gateways, set the following variables:

   - `gwSpecificRegistrationEnableConfig` variable for the specific SIP gateway you want to configure to **enable**.

- `gwSpecificRegistrationRefreshTime` variable for the specific SIP gateway you want to configure to the proper value.

You can also use the following lines in the CLI or a configuration script:

```
sipEp.gwSpecificRegistration.EnableConfig[GatewayName="Specific_Gateway"]="1"
sipEp.gwSpecificRegistration.RefreshTime[GatewayName="Specific_Gateway"]="Value"
```

where:

- *Specific_Gateway* is the name of the SIP gateway you want to configure.
- *Value* is the refresh time value.

Registration Expiration

You can set the default registration proposed expiration value in the web page ("Registration Configuration" on page 169), but you can also set a different registration refresh time for one or more SIP gateways.

▶ **To configure the registration expiration:**

1. In the *sipEpMIB*, locate the *registrationGroup* folder.
2. If you want to set a different registration refresh time for one or more SIP gateways, set the following variables:
   - `gwSpecificRegistrationEnableConfig` variable for the specific SIP gateway you want to configure to **enable**.
   - `gwSpecificRegistrationProposedExpirationValue` variable for the specific SIP gateway you want to configure to the proper value.

   You can also use the following lines in the CLI or a configuration script:

```
sipEp.gwSpecificRegistration.EnableConfig[GatewayName="Specific_Gateway"]="1"
sipEp.gwSpecificRegistration.ProposedExpirationValue[GatewayName="Specific_Gatew
ay"]="Value"
```

   where:

   - *Specific_Gateway* is the name of the SIP gateway you want to configure.
   - *Value* is the expiration delay value.

   This value does not modify the time before a re-REGISTER.

   - The delay is the "expires" of the contact in the 200 OK response to the REGISTER request minus the value set in the `gwSpecificRegistrationRefreshTime` parameter.
   - If the "expires" of the contact in the 200 OK response to the REGISTER is not present or not properly formatted, then the delay is the default registration proposed expiration value minus the value set in the `gwSpecificRegistrationRefreshTime` parameter.

Expiration Value in Registration

You can set the default expiration value in registration in the web page ("Registration Configuration" on page 169), but you can also set a different expiration value in registration for one or more SIP gateways.

This value is used when the contact in a registration response contains no "expires" or the "expires" is badly formatted. In this case, the delay before a re-REGISTER is the value set in this field minus the value set in the in the 'RefreshTime' variable ("Registration Refresh" on page 172).

▶ **To configure the expiration value in registration for a specific gateway:**

1. In the *sipEpMIB*, locate the *registrationGroup* folder.
2. To set a different expiration value in registration for one or more SIP gateways, set the following variables:
   - `gwSpecificRegistrationEnableConfig` variable for the specific SIP gateway you want to configure to **enable**.
   - `gwSpecificRegistrationExpirationValue` variable for the specific SIP gateway you want to configure to the proper value.

You can also use the following lines in the CLI or a configuration script:

3. To set a different expiration value in registration for one or more SIP gateways, put the following lines in the configuration script:

```
sipEp.gwSpecificRegistration.EnableConfig[GatewayName="Specific_Gateway"]="1"
sipEp.gwSpecificRegistration.ExpirationValue[GatewayName="Specific_Gateway"]="Va
lue"
```

where:

- *Specific_Gateway* is the name of the SIP gateway you want to configure.
- *Value* is the expiration value in registration value.

Gateway Specific Registration Retry Time

You can set a different Registration Retry Time for one or more SIP gateways.

This variable defines the time, relative to the failure of the registration, at which the SIP gateway retries the registration.

▶ **To specify the registration retry time value for a specific gateway:**

1. In the *sipEpMIB*, locate the *registrationGroup* folder.
2. To set a different registration retry time for one or more SIP gateways, set the following variables:
   - `gwSpecificRegistrationEnableConfig` variable for the specific SIP gateway you want to configure to enable.
   - `gwSpecificRegistrationRetryTime` variable for the specific SIP gateway you want to configure to the proper value.

   You can also use the following line in the CLI or a configuration script:
3. To set a different expiration value in registration for one or more SIP gateways, put the following lines in the configuration script:

```
sipEp.gwSpecificRegistration.EnableConfig[GatewayName="Specific_Gateway"]="1"
sipEp.gwSpecificRegistrationRetryTime[GatewayName="Specific_Gateway"]="Value"
```

where:

- *Specific_Gateway* is the name of the SIP gateway you want to configure.
- *Value* is the expiration value in registration retry time.

Unregistered Endpoint Behaviour

You can specify whether an endpoint should remain enabled or not when not registered. This is useful if you want your users to be able to make calls even if the endpoint is not registered with a SIP server.

The following values are supported:

Table 111: Unregistered Endpoint Behaviour Parameters

Value	Description
disablePort	When the endpoint is not registered, it is disabled. The user cannot make or receive calls. Picking up the handset yields a fast busy tone, and incoming INVITEs receive a “403 Forbidden” response.
enablePort	When the endpoint is not registered, it is still enabled. The user can receive and initiate outgoing calls. Note that because the endpoint is not registered with a registrar, its public address is not available to the outside world; the endpoint will most likely be unreachable except through direct IP calling.

▶ **To specify unregistered endpoint behaviour:**

1. In the *sipEpMIB*, locate the *registrationGroup* folder.

2. Set the `defaultRegistrationUnregisteredBehavior` variable.

You can also use the following line in the CLI or a configuration script:

```
sipEp.defaultRegistrationUnregisteredBehavior="Value"
```

where *Value* may be as follows:.

Table 112: Unregistered Endpoint Behaviour Values

Value	Meaning
0	disablePort
1	enablePort

3. If you want to set a different behaviour for one or more SIP gateways, set the following variables:

- `gwSpecificRegistrationEnableConfig` variable for the specific SIP gateway you want to configure to **enable**.
- `gwSpecificRegistrationUnregisteredBehavior` variable for the specific SIP gateway you want to configure to the proper value.

You can also use the following lines in the CLI or a configuration script:

```
sipEp.gwSpecificRegistration.EnableConfig[GatewayName="Specific_Gateway"]="1"
sipEp.gwSpecificRegistration.UnregisteredBehavior[GatewayName="Specific_Gateway"
]="Value"
```

where:

- *Specific_Gateway* is the name of the SIP gateway you want to configure.
- *Value* is one of the values described in Step 2.

Unregistered User Behaviour

You can specify whether the SIP gateway state should be affected or not by the unit registrations state.

The following values are supported:

Table 113: Unregistered User Behaviour Parameters

Value	Description
NoEffect	The unit registrations state has no effect on the SIP gateway state.
DisableGateway	The SIP gateway goes in the 'unregistered' state when all unit registrations are not in the 'registered' state. The 'unregistered' state indicates some registrations that are mandatory for this gateway failed.

▶ **To specify unregistered user behaviour:**

1. In the *sipEpMIB*, locate the *registrationGroup* folder.

2. Set the `defaultUserRegistrationUnregisteredBehavior` variable.

You can also use the following line in the CLI or a configuration script:

```
sipEp.defaultUserRegistrationUnregisteredBehavior="Value"
```

where *Value* may be as follows:.

Table 114: Unregistered User Behaviour Values

Value	Meaning
100	NoEffect

Table 114: Unregistered User Behaviour Values (Continued)

Value	Meaning
200	DisableGateway

Behaviour on Initial-Registration Reception

You can configure the behaviour of the Aastra unit upon reception of a 380 or 504 carrying an XML body with a specified 'initial-registration' action.

The following values are supported:

Table 115: Behaviour on Initial-Registration Reception Parameters

Value	Description
NoRegistration	No registration refresh are sent upon reception of the message.
EndpointRegistration	Registration refresh of the endpoint associated with the call is sent upon reception of the message.
UnitRegistration	Registration refresh of all the usernames configured as 'unit registration' are sent upon reception of the message.
UnitAndEndpointRegistration	Registration refresh of the endpoint associated with the call and of all the usernames configured as 'unit registration' are sent upon reception of the message.

▶ **To specify the behaviour on Initial-Registration reception:**

1. In the *sipEpMIB*, locate the *registrationGroup* folder.
2. Set the `behaviorOnInitialRegistrationReception` variable with the proper behaviour.

   You can also use the following line in the CLI or a configuration script:

   `sipEp.behaviorOnInitialRegistrationReception="Value"`

   where *Value* may be as follows:.

   Table 116: Behaviour on Initial-Registration Reception Values

Value	Meaning
100	NoRegistration
200	EndpointRegistration
300	UnitRegistration
400	UnitAndEndpointRegistration

   If the registration(s) succeed, then the call is re-attempted.

   If the registration(s) fail, then the call is terminated.
3. Set the `registrationDelayOnInitialRegistrationReception` variable with the registration delay, in milliseconds, on Initial-Registration Reception.

   This variable configures the time interval between the unregistration confirmation (or final response) and the registration attempt that follows.

   This variable is only used when `behaviorOnInitialRegistrationReception` is configured to a value other than 'NoRegistration'.

Note: This variable only applies on registration refresh triggered by the `behaviorOnInitialRegistrationReception` feature.

You can also use the following line in the CLI or a configuration script:

```
sipEp.registrationDelayOnInitialRegistrationReception="Value"
```

Registration Delay Value

The quality of calls may be altered if a large quantity of registrations, more than 100, is requested at the same time. To avoid this situation, you can configure the maximum number of seconds that the system uses to apply a random algorithm, which is used to determine a delay before requesting a user registration or an endpoint registration.

When the value is **0**, the request registration is done immediately.

> **Note:** The random algorithm applies individually to all registrations, meaning registrations order may not follow their corresponding index.

▶ **To specify the registration delay value:**

1. In the *sipEpMIB*, set the `interopRegistrationDelayValue` variable with the proper delay value.

   You can also use the following line in the CLI or a configuration script:

   ```
   sipEp.interopRegistrationDelayValue="Value"
   ```

   where *Value* may be between 0 and 600 seconds.

SIP User Agent Header

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

The *User-Agent* header field contains information about the user agent client originating the request. For instance, the information of the *User-Agent* header could be something like the following:

```
User-Agent: Softphone Beta1.5
```

You can specify whether or not the Aastra unit sends this information when establishing a communication.

▶ **To enable sending the SIP User Agent header:**

1. In the *sipEpMIB*, set the `interopSendUAHeaderEnable` variable to **enable**.

   You can also use the following line in the CLI or a configuration script:

   ```
   sipEp.interopSendUaHeaderEnable="1"
   ```

CHAPTER 24

SIP Authentication

This chapter describes how to configure authentication parameters of the Aastra unit.

Standards Supported	• Basic and Digest authentication as per RFC 3261

Caution: The *SIP* > *Authentication* page is not accessible if you have the User or Observer access right. See "Users" on page 591 for more details.

Authentication Configuration

Authentication information allows you to add some level of security to the Aastra unit endpoints by setting user names and passwords.

You can add four types of authentication information:

Table 117: Authentication Information

Authentication	Description
endpoint-specific	Applies only to challenges received for SIP requests related to a specific endpoint. For instance, the registration associated with the endpoint in the user agent table or the INVITE sent to initiate a call from the endpoint. You can define several user names and passwords for each endpoint of the Aastra unit. An endpoint can thus register with several different realms.
gateway-specific	Applies only to challenges received for SIP requests on a specific SIP gateway. You can define several user names and passwords for each endpoint of the Aastra unit. An endpoint can thus register with several different realms.
unit	Applies to all challenges received for SIP dialog. You can define several user names and passwords for the Aastra unit. These user names and passwords apply to all endpoints of the unit.
user name-specific	Applies only to challenges for a context that uses a specific user name.

The *Authentication* table may have between 20 and 100 rows. Each of these rows can either be associated with the unit, a specific gateway, a specific endpoint, or a specific user name. If you have less than 20 rows, the Aastra unit automatically adds new rows up to the minimum of 20.

When a challenge occurs (either 401 or 407), the first entry in the *Authentication* table that matches the user name/password request is used to reply to the challenge. You can configure the use name and password in the web interface. The order of the tried entries in the *Authentication* table is from the first row to the last row.

The challenge matches an authentication entry if the realm of the challenge matches the realm specified in the *Realm* field or if the *Validate Realm* field is set to **disable**. For each entry matching certain criteria (described below), the challenge is replied with the entry's user name and password. If no entry matches the criteria, the authentication fails. To match the authentication request, the entry must also meet one of the following criteria:

- The challenge needs to be for a SIP request related to the endpoint specified in the *Endpoint* column if the corresponding *Apply To* column is set to **Endpoint**.
- The challenge needs to be for a SIP request performed on the SIP gateway specified in the *Gateway* column if the corresponding *Apply To* column is set to **Gateway**.

- The challenge needs to be for a context that uses the user name specified in the *User Name* field if the corresponding *Apply To* column is set to **Usename**. The user name associated with a context is:
  - the user name of the FROM if the context sent the original SIP request, or
  - the user name of the request URI if the context received the original SIP request
- The challenge applies to a unit if the corresponding *Apply To* column is set to **Unit**.

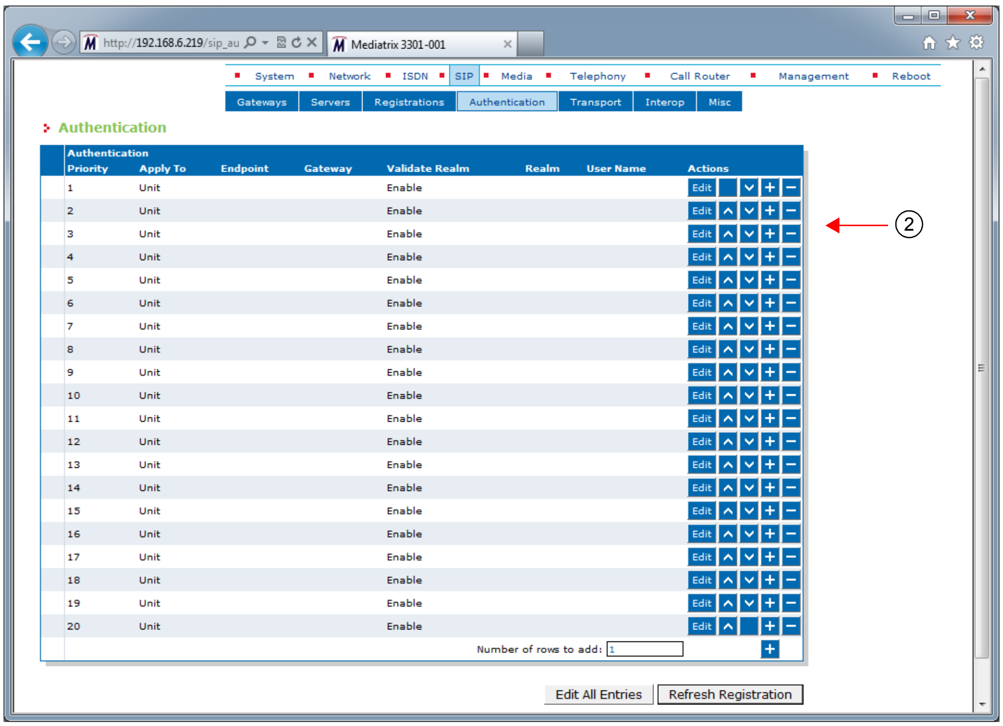
Creating/Editing an Authentication Entry

The web interface allows you to create authentication entries or modify the parameters of an existing one.

▶ To create or edit SIP authentication parameters:

1. In the web interface, click the *SIP* link, then the *Authentication* sub-link.

Figure 74: SIP Configuration – Authentication Web Page



2. Do one of the following:

- If you want to add an authentication entry before an existing entry, locate the proper row in the table and click the + button of this row.
- If you want to add an authentication entry at the end of the existing rows, click the + button at the bottom right of the *Authentication* section.
- If you want to add several authentication entries at the same time, enter the number of entries you want to add in the *Number of rows to add* at the bottom of the page.
- If you want to edit a single authentication entry, locate the proper row in the table and click the Edit button.
- If you want to edit a several authentication entries of the current page at the same time, click the *Edit All Entries* button at the bottom of the page.

This brings you to the proper *Authentication* panel.

Table 118: Authentication Panel – Single Entry

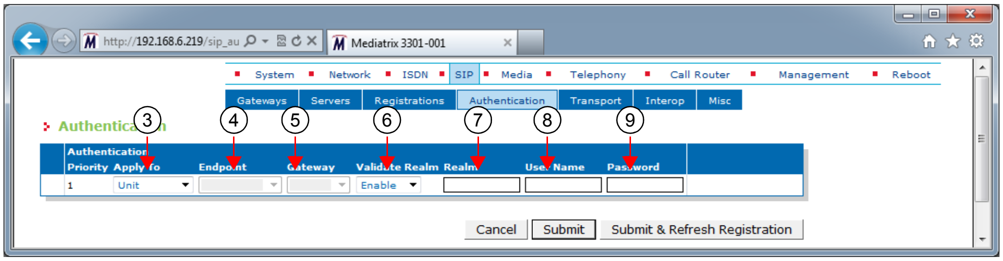
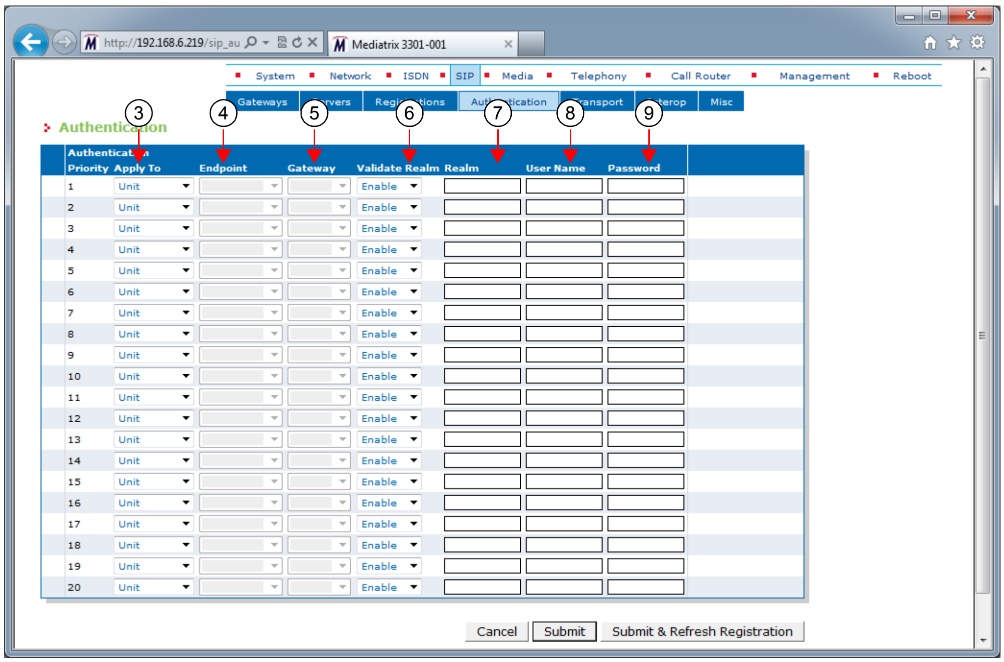


Table 119: Authentication Panel – Page



3. Select which criterion to use for matching an authentication request with an authentication entry in the *Apply to* column.

Table 120: Authentication Entity

Parameter	Description
Unit	The authentication entry is used on all challenges.
Endpoint	The authentication entry used for all challenges related to a specific endpoint.
Gateway	The authentication entry is used for all challenges related to a specific SIP gateway.
Username	The authentication entry is used for all challenges related to a specific user name. Only the username part is used if the value has the format 'username@domain'.

4. Enter a string that identifies an endpoint in other tables in the *Endpoint* column.

This field is available only if you have selected the **Endpoint** entity in the previous step for the specific row.

5. Enter a string that identifies a SIP gateway in other tables in the *Gateway* column.

This field is available only if you have selected the **Gateway** entity in the *Apply to* column for the specific row.

6. Select whether or not the current credentials are valid for any realm in the corresponding *Validate Realm* drop-down menu.

Table 121: Realm Authentication Parameters

Parameter	Description
Disable	The current credentials are valid for any realm. The corresponding *Realm* field is read-only and cannot be modified.
Enable	The credentials are used only for a specific realm set in the corresponding *Realm* field.

7. Enter a realm for each authentication row in the *Realm* column.

When authentication information is required from users, the realm identifies who requested it.

8. Enter a string that uniquely identifies this endpoint in the realm in the *User Name* column.

9. Enter a user password in the *Password* column.

10. If you do not need to set other parameters, do one of the following:

- To save your settings without refreshing the registration, click *Submit*.
- To save your settings and refresh the registration now, click *Submit & Refresh Registration*.

Moving an Authentication Entry

The order of the tried entries in the *Authentication* table is from the first row to the last row. The rows sequence is thus very important. If you want the unit to try to match one row before another one, you must put that row first.

▶ **To move an authentication entry up or down:**

1. Either click the  or  arrow of the row you want to move until the entry is properly located.

Deleting an Authentication Entry

You can delete an authentication row from the table in the web interface.

▶ **To delete an authentication entry:**

1. Click the  button of the row you want to delete.

C H A P T E R
25

SIP Transport Parameters

This chapter describes the SIP transport parameters you can set.

SIP Transport Type

Standards Supported	• RFC 2246: The TLS Protocol Version 1.0 • RFC 3261: SIP, Session Initiation Protocol

You can globally set the transport type for all the endpoints of the Aastra unit to either UDP (User Datagram Protocol), TCP (Transmission Control Protocol), or TLS (Transport Layer Security).

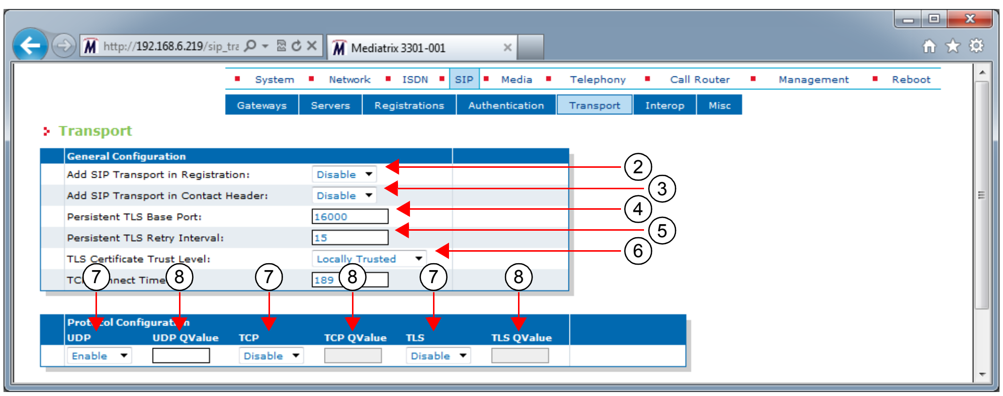
The Aastra unit will include its supported transports in its registrations.

Please note that RFC 3261 states the implementations must be able to handle messages up to the maximum datagram packet size. For UDP, this size is 65,535 bytes, including IP and UDP headers. However, the maximum datagram packet size the Aastra unit supports for a SIP request or response is 5120 bytes excluding the IP and UDP headers. This should be enough, as a packet is rarely bigger than 2500 bytes.

▶ **To set the SIP transport type parameters:**

1. In the web interface, click the *SIP* link, then the *Transport* sub-link.

Figure 75: SIP Configuration – Transport Web Page



2. In the *General Configuration* section, enable or disable the transport registration in the *Add SIP Transport in Registration* drop-down menu.

   When enabled, the Aastra unit includes its supported transports in its registrations. It registers with one contact for each transport that is currently enabled. Each of these contacts contains a “transport” parameter.

This is especially useful for a system where there are no SRV records configured to use a predefined transport order for receiving requests. When sending a request, the unit either follows the SRV configuration, or, if not available, any transport parameter received from a redirection or from a configured SIP URL.

> **Note:** If the Aastra unit has the following configuration:
> - the *Add SIP Transport in Registration* drop-down menu is set to **Disable**
> - the UDP transport type is disabled
> - the TCP transport type is enabled
>
> The unit will not work properly unless the SIP server uses the TCP transport type by default.
>
> This is also true if the Aastra unit has the TCP transport disabled and the UDP transport enabled. In this case, the unit will not work properly unless the SIP server uses the UDP transport protocol by default.

3. Indicate whether or not the unit must include its supported transport in the *Contact* header in the *Add SIP Transport in Contact Header* drop-down menu.

The supported transports are included in all SIP messages that have the *Contact* header, except for the REGISTER message.

Available values are *Enable* and *Disable*. If you set the menu to **Enable**, the Aastra unit will send SIP messages with the "transport" parameter in the *Contact* header set to:

- *transport=tcp* when TCP is enabled and UDP is disabled
- *transport=udp* when UDP is enabled and TCP disabled
- no transport parameter when both TCP and UDP are enabled
- *transport=tls* when secure transport (TLS) is selected

4. Define the base port used to establish TLS persistent connections with SIP servers when the TLS transport is enabled in the *Persistent TLS Base Port* field.

5. Set the time interval, in seconds, before retrying the establishment of a TLS persistent connection in the *Persistent TLS Retry Interval* field.

This is the interval that the Aastra unit waits before retrying periodically to establish a TLS persistent connection using a single IP address or a FQDN. This timer is started when a TLS persistent connection goes down or fails to connect to the destination. The TLS persistent connect timeout applies only to TLS persistent connections.

When the destination is a single IP address and the TLS persistent connection goes down or fails to establish, the timer is started. When the timer expires, the Aastra unit attempts to re-establish the TLS persistent connection.

When the destination is a FQDN and the TLS persistent connection goes down or fails to establish with the higher priority target received from a DNS answer, the timer is started and the lower priority targets are attempted. When the timer expires, a new DNS request is sent and depending on the DNS answer, the Aastra unit retries to establish the TLS persistent connection with the higher priority target. The timer is unique for all TLS persistent connections using the same FQDN. This means that the timer is not restarted when a connection using a lower priority target fails while a connection using a higher priority target has already failed.

6. In the *TLS Trusted Certificate Level* field, define how a peer certificate is considered trusted for a TLS connection.

Table 122: Certificate Trust Level for TLS Connections Parameters

Parameter	Description
Locally Trusted	A certificate is considered trusted when the certificate authority (CA) that signed the peer certificate is present in the Others Certificates table (see "Chapter 46 - Certificates Management" on page 557 for more details). The certificate revocation status is not verified.

Table 122: Certificate Trust Level for TLS Connections Parameters (Continued)

Parameter	Description
OCSP Optional	A certificate is considered trusted when it is locally trusted and is not revoked by its certificate authority (CA). The certificate revocation status is queried using the Online Certificate Status Protocol (OCSP). If the OCSP server is not available or the verification status is unknown, the certificate is considered trusted.
OCSP Mandatory	A certificate is considered trusted when it is locally trusted and is not revoked by its certificate authority (CA). The certificate revocation status is queried using the Online Certificate Status Protocol (OCSP). If the OCSP server is not available or the verification status is unknown, the certificate is considered not trusted.

7. Set the *TCP Connect Timeout* field with the maximum time, in seconds, the unit should try to establish a TCP connection to SIP hosts.

This timeout value is useful to have a faster detection of unreachable remote hosts. This timer can also affect the TLS connection establishment time.

8. In the *Protocol Configuration* section, enable or disable the UDP, TCP, and TLS transport type to use in their corresponding drop-down menu.

UDP and TCP are mutually exclusive with TLS. Activating TLS automatically disables these unsecure protocols.

The successful configuration of a secure transport requires a little more than the activation of the TLS protocol itself. You need to:

- synchronize the time in the unit (see “Time Configuration” on page 94 & “SNTP Configuration” on page 93 for more details).
- install the security certificates used to authenticate the server to which you will connect (see “Chapter 46 - Certificates Management” on page 557 for more details).
- Use secure media (see “Security” on page 201 for more details).
- configure the unit so that a “transport=tls” parameter is added to the *Contact* header of your SIP requests (see Step 3).

Caution: If you have enabled Secure RTP (SRTP) on at least one line, it is acceptable to have the secure SIP transport (TLS) disabled for testing purposes. However, you must never use this configuration in a production environment, since an attacker could easily break it. Enabling TLS for SIP Transport is strongly recommended and is usually mandatory for security interoperability with third-party equipment.

9. Set the priority order of each transport type in the corresponding *QValue* field.

A qvalue parameter is added to each contact. The qvalue gives each transport a weight, indicating the degree of preference for that transport. A higher value means higher preference.

The format of the qvalue string must follow the RFC 3261 ABNF (a floating point value between 0.000 and 1.000). If you specify an empty string, no qvalue is set in the contacts.

10. Click *Submit* if you do not need to set other parameters.

Additional Transport Parameters

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

UDP Source Port Behaviour

You can configure whether or not the Aastra unit always uses the same local port (the port on which it is listening for incoming packets) when sending SIP traffic over UDP. This is called symmetric UDP source port. Symmetric UDP ports are sometimes needed to traverse NAT/Firewall devices.

When changing this setting, all destinations are automatically sent out of the penalty box, when applicable.

The following parameters are available:

Table 123: UDP Source Port Parameters

Parameter	Description
disable	The SIP signalling over UDP uses a randomly-generated originating port. ICMP errors are processed correctly.
enable	The SIP signalling sent over UDP originates from the same port as the port on which the user agent is listening. ICMP messages are not processed, which means that unreachable targets will take longer to detect.

► **To set the UDP source port behaviour:**

1. In the *sipEpMIB*, set whether or not the unit uses the symmetric source port feature in the `interopSymmetricUdpSourcePortEnable` variable.

   You can also use the following line in the CLI or a configuration script:

   ```
   sipEp.interopSymmetricUdpSourcePortEnable="Value"
   ```

   where *Value* may be as follows:

   Table 124: UDP Source Port Values

Value	Meaning
0	disable
1	enable

2. Restart the *SipEp* service by accessing the *scmMIB* and setting the `serviceCommandsRestart` variable for the *SipEp* service to **restart**.

   You can also use the following line in the CLI or a configuration script:

   ```
   scm.serviceCommands.Restart[Name=SipEp]="10"
   ```

TLS Client Authentication

When acting as a TLS server, it is customary not to request from the clients that they authenticate themselves via the TLS protocol. However, if mutual authentication is required between client and server, you can set the Aastra unit so that it requests client authentication when acting as a TLS server.

The following parameters are available:

Table 125: TLS Client Authentication Parameters

Parameter	Description
disable	The Aastra unit does not require TLS clients to provide their host certificate for the connection to be allowed. This is the default value.
enable	The TLS clients must provide their host certificate for the connection to be allowed. In this case, the level of security used to validate the host certificate is **TrustedCertificate**, whatever the value set in the *Certificate Validation* drop-down menu of the *TLS Interop* section (*SIP > Interop* web page). See "TLS Interop" on page 318 for more details.

▶ **To set TLS client authentication:**

1. In the *sipEpMIB*, set whether or not the Aastra unit requests client authentication when acting as a TLS server in the `interopTlsClientAuthenticationEnable` variable.

You can also use the following line in the CLI or a configuration script:

`sipEp.interopTlsClientAuthenticationEnable="Value"`

where *Value* may be as follows:

Table 126: TLS Client Authentication Values

Value	Meaning
0	disable
1	enable

Force DNS NAPTR In TLS

The Aastra unit allows you to force a DNS NAPTR request when the SIP transport is TLS.

This variable only applies to calls over TLS when the *Supported DNS Queries* drop-down menu of the *SIP > Misc* page is set to **NAPTR** (see "DNS Configuration" on page 348 for more details).

The following parameters are available:

Table 127: Force DNS NAPTR in TLS Parameters

Parameter	Description
disable	The DNS SRV request is sent directly with the SIP transport in SIP URI as recommended in RFC 3263, section 4.1.
enable	A DNS NAPTR request is sent to obtain the DNS record associated with SIP over TLS. An SRV request is performed afterward. If no SIP over TLS entry is returned, the call fails.

▶ **To force DNS NAPTR in TLS:**

1. In the *sipEpMIB*, set whether or not to force a DNS NAPTR request in the `InteropForceDnsNaptrInTls` variable.

You can also use the following line in the CLI or a configuration script:

`sipEp.interopForceDnsNaptrInTls="Value"`

where *Value* may be as follows:

Table 128: Force DNS NAPTR in TLS Values

Value	Meaning
0	disable
1	enable

CHAPTER 26

Interop Parameters

This chapter describes the interop parameters that allow the Aastra unit to properly work, communicate, or connect with specific IP devices.

Standards Supported	• draft-ietf-sipping-realtimefax-00 • ITU-T Recommendation T.38, section D.2.3 • RFC 3264: An Offer/Answer Model with the Session Description Protocol (SDP) • RFC 3515: The Session Initiation Protocol (SIP) Refer Method

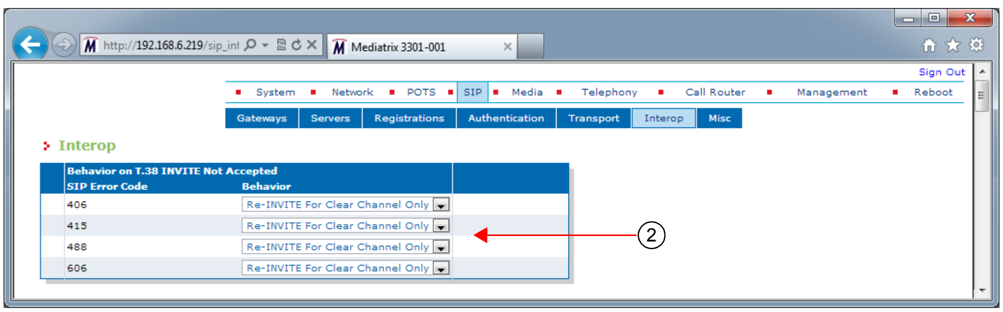
Behavior on T.38 INVITE Not Accepted

This section describes the unit's behaviour after receiving an error to a SIP INVITE for T.38 fax.

▶ **To set the T.38 interop parameters:**

1. In the web interface, click the *SIP* link, then the *Interop* sub-link.

Figure 76: SIP – Interop Web Page



2. In the *Behavior on T.38 INVITE Not Accepted* section, for each of 406, 415, 488, and 606 SIP code, set the behaviour after receiving the code in the error response to an INVITE for T.38 fax in the corresponding *Behavior* drop-down menu.

Table 129: Behavior on T.38 INVITE Not Accepted Parameters

Behavior	Description
Drop Call	The call is dropped by sending a BYE.
ReInviteForClearChannelOnly	A re-INVITE is sent with audio codecs that support clear channel faxes.
Re-Establish Audio	A re-INVITE is sent to re-establish the audio path. Also, fax detection is disabled for the remainder of the call.
UsePreviousMediaNegotiation	No re-INVITE is sent and the audio codec from the last successful negotiation is used. For the remainder of the call, T.38 is disabled and fax detection may trigger a switch to a clear channel codec that was available in the last successful negotiation.

3. Click *Submit* if you do not need to set other parameters.

SIP Interop

Standards Supported	• RFC 3261: SIP: Session Initiation Protocol

This section describes the SIP interop parameters of the Aastra unit

▶ **To set the SIP interop parameters:**

1. In the *SIP Interop* section of the *Interop* page, set whether or not the “x-Siemens-Call-Type” header is added to the SIP packets sent by the unit in the *Secure Header* drop-down header.

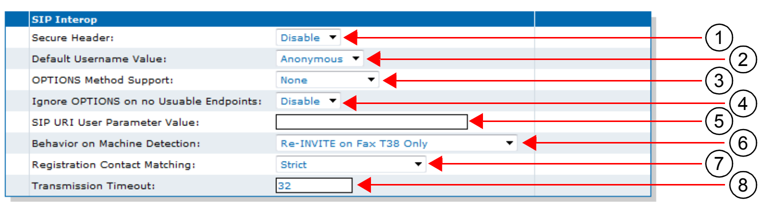
You can set the Aastra unit so that it triggers the addition of the “x-Siemens-Call-Type” header to the SIP packets sent by the unit when secure transport is in use.

The following parameters are available:

Table 130: Secure Transport Header Parameters

Parameter	Description
disable	The “x-Siemens-Call-Type” header is not added to the SIP packets sent by the unit.
enable	The “x-Siemens-Call-Type” header is added to the SIP packets sent by the unit, and assigned the value “ST-secure”, as soon as secure transport and secure payload are being used. If secure transport or secure payload are not used, the header is not added.

Figure 77: SIP Interop Section



2. Select the username to use when the username is empty or undefined in the *Default Username Value* drop-down menu.

Table 131: Default Username Value

Parameter	Description
Anonymous	Sets the username to “anonymous”.
Host	Sets the username to the same value as the host.

3. Define the behaviour of the Aastra unit when answering a SIP OPTIONS request in the *OPTIONS Method Support* drop-down menu.

Table 132: OPTIONS Method Support Parameters

Parameter	Description
None	The Aastra unit responds with an error 405 Method not allowed.
AlwaysOK	The Aastra unit responds with a 200 OK regardless of the content of the OPTIONS request.

4. Define whether or not the SIP OPTIONS requests should be ignored when all endpoints are unusable in the *Ignore OPTONS on no usable endpoints* drop-down menu.

Table 133: Ignore SIP Options Parameters

Parameter	Description
Enable	The unit ignores SIP OPTIONS requests when all endpoints are unusable. When at least one endpoint is usable, then the SIP OPTIONS requests are answered as configured in the *OPTIONS Method Support* drop-down menu (see Step 10).
Disable	The SIP OPTIONS requests are answered as configured in the *OPTIONS Method Support* drop-down menu (see Step 10) regardless of the state of the endpoints.

Note that this feature may be influenced by whether or not you have enabled the *Monitor Link State* parameter. For more information:

- ISDN PRI interface: “PRI Configuration” on page 184
- ISDN BRI interface: “BRI Configuration” on page 195
- R2 PRI interface: “R2 Channel Associated Signaling” on page 224

5. Set the value of the user parameter in SIP URIs sent by the unit in the *SIP URI User Parameter Value* field.

If you leave the field empty, the parameter is not added.

E.g : sip:1234@domain.com;user=InteropSipUriUserParameterValue

Note that when the *Map Plus To TON International* drop-down menu is set to **Enable**, the parameter's value might be overwritten (“Misc Interop” on page 196).

6. Set the *Behavior On Machine Detection* drop-down menu with the SIP device’s behavior when a machine (fax or modem) is detected during a call.

Table 134: Behavior on Machine Detection Parameters

Parameter	Description
Re-INVITE On Fax T38 Only	A SIP re-INVITE is sent only on a fax detection and T.38 is enabled.
Re-INVITE On No Negotiated Data Codec	A SIP re-INVITE is sent on a fax or modem detection if no data codec was previously negotiated in the original SDP negotiation. In the case where at least one data codec was previously negotiated in the SDP negotiation, the device switches silently to a data codec without sending a SIP re-INVITE. Note sthat if there is no data codec enabled on the device, no SIP re-INVITE is sent and the call is dropped by sending a BYE.
Re-INVITE Unconditional	A SIP re-INVITE is sent with data codecs upon detection of a fax or modem even if a data codec was negotiated in the initial offer-answer. The T.38 codec is offered if it is enabled and a fax is detected.

See “Data Codec Selection Procedure” on page 221 for more details on the procedure the Aastra unit follows when selecting data codec.

7. Set the *Registration Contact Matching* field with the matching behaviour for the contact header received in positive responses to REGISTER requests sent by the unit.

Table 135: Registration Contact Matching Parameters

Parameter	Description
Strict	Matches the complete contact's SIP URI including any URI parameters, if any, as per RFC 3261 sections '10.2.4 Refreshing Bindings' and '19.1.4 URI Comparison'. The contact's SIP URI of a 2XX positive response MUST match the contact's SIP URI of the REGISTER request.
IgnoreUriParams	Matches the username and the host port part of the contact's SIP URI. All URI parameters are ignored.

8. Set the *Transmission Timeout* field with the time to wait for a response or an ACK before considering a transaction timed out.

This corresponds to timers B, F and H for all transport protocols and timer J for UDP. These timers are defined in section A of RFC 3261.

This timeout affects the number of retransmissions. Retransmissions continue to follow the timing guidelines described in RFC 3261.

If a DNS SRV answer contains more than one entry, the Aastra unit will try these entries if the entry initially selected does not work. You can configure the maximum time, in seconds, to spend waiting for answers to messages, from a single source. Retransmissions still follow the algorithm proposed in RFC 3261, but the total wait time can be overridden by using this feature.

For example, if you are using DNS SRV and more than one entry are present, this timeout is the time it takes before trying the second entry.

Available values are from 1 to 32 seconds.

9. Click *Submit* if you do not need to set other parameters.

SDP Interop

Standards Supported	• RFC 3264: An Offer/Answer Model with Session Description Protocol (SDP)

This section describes the SDP interop parameters of the Aastra unit.

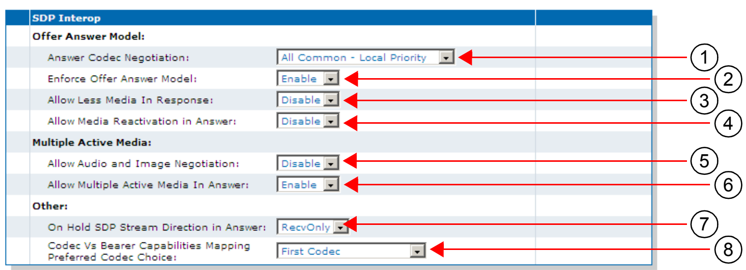
▶ To set the SDP interop parameters:

1. In the *SDP Interop* section of the *Interop* page, *Offer Answer Model* part, select the codec negotiation rule when generating a SDP answer in the *Answer Codec Negotiation* drop-down menu.

Table 136: Answer Codec Negotiation Parameters

Parameter	Description
All Common - Local Priority	When generating an answer to an offered session, all common codecs are listed in the local order of priority. The local priority is defined for each codec in the *Telephony > CODECS* page – by clicking the Edit button of each codec and looking in the *Voice Priority* and *Data Priority* fields. See "Chapter 14 - Voice & Fax Codecs Configuration" on page 181 for more details.
First Common - Local Priority	When generating an answer to an offered session, only the first common codec with the higher local priority is listed. The local priority is defined for each codec in the *Telephony > CODECS* page – by clicking the Edit button of each codec and looking in the *Voice Priority* and *Data Priority* fields. See "Chapter 14 - Voice & Fax Codecs Configuration" on page 181 for more details.
All Common - Peer Priority	When generating an answer to an offered session, all common codecs are listed. The codecs order is the same as in the peer offer.
First Common - Peer Priority	When generating an answer to an offered session, only the first common codec is listed. The codecs order is the same as in the peer offer.

Figure 78: SDP Interop Section



2. Select whether or not the Aastra unit requires strict adherence to RFC 3264 when receiving an answer from the peer when negotiating capabilities for the establishment of a media session in the *Enforce Offer Answer Model* drop-down menu.

The following values are available:

Table 137: Offer/Answer Model Parameters

Parameter	Description
Disable	The peer can freely: • Send back a brand new list of codecs or add new ones to the offered list. • Add new media lines. As long as at least one codec sent back was present in the initial offer, the call is allowed to go on. Any media line added by the peer is simply ignored.

Table 137: Offer/Answer Model Parameters

Parameter	Description
Enable	The following guidelines from the Offer-Answer Model must be strictly followed. An answer must: • Include at least one codec from the list that the Aastra unit sent in the offer. • Contain the same number of media lines that the unit put in its offer. Otherwise, the answer is rejected and the unit ends the call. This is the default value.

3. Define the behaviour of the Aastra unit when receiving less media announcements in the response than in the offer in the *Allow Less Media In Response* drop-down menu.

   The following values are available:

Table 138: Less Media Announcements Parameters

Parameter	Description
Disable	The Aastra unit rejects the response with less media announcements than in the offer.
Enable	The Aastra unit tries to find matching media when the response contains less media announcement than in the offer. This is a deviation from the Offer/ Answer model.

4. Define the behaviour of the Aastra unit when receiving a SDP answer activating a media that had been previously deactivated in the offer in the *Allow Media Reactivation in Answer* drop-down menu.

Table 139: Media Reactivation Parameters

Parameter	Description
Enable	A media reactivated in an incoming answer is ignored. This behaviour goes against the SDP Offer/Answer model described by IETF RFC 3264.
Disable	A media reactivated in an incoming answer ends the current media negotiation and the call. This behaviour follows the SDP Offer/Answer model described by IETF RFC 3264.

5. In the Multiple Active Media part, define the behaviour of the Aastra unit when offering media or answering to a media offer with audio and image negotiation in the *Allow Audio and Image Negotiation* drop-down menu.

Table 140: Audio and Image Negotiation Parameters

Parameter	Description
Enable	The unit offers audio and image media simultaneously in outgoing SDP offers and transits to T.38 mode upon reception of a T.38 packet. Also, when the unit answers positively to a SDP offer with audio and image, it transits to T.38 mode upon reception of a T.38 packet.
Disable	Outgoing offers never include image and audio simultaneously. Incoming offers with audio and image media with a non-zero port are considered as offering only audio.

6. Define the behaviour of the Aastra unit when answering a request offering more than one active media in the *Allow Multiple Active Media in Answer* drop-down menu.

Figure 79: Allow Multiple Active Media in Answer

Parameter	Description
disable	The answer contains only one active media. The media specified as active in the answer is the top-most matching one in the offer. Other media are set to inactive.
enable	Each matching active media in the offer is specified as active in the answer. Other media are set to inactive

7. In the *Other* part, define how to set the direction attribute and the connection address in the SDP when answering a hold offer with the direction attribute “sendonly” in the *On Hold SDP Stream Direction in Answer* drop-down menu.

   The following parameters are supported:

Table 141: “sendonly” Direction Attribute

Parameter	Description
inactive	The stream is marked as inactive and if the stream uses IPv4, the connection address is set to '0.0.0.0'.
revconly	If the stream is currently active or receive only, it is marked as recvonly and the connection address is set to the IP address of the unit. If the stream is currently send only or inactive, it is marked as inactive and if the stream uses IPv4, the connection address is set to '0.0.0.0'. This method is in conformance with RFC 3264.

   In both cases, no direction attribute is present in the SDP if the `interopSdpDirectionAttributeEnable` variable is set to **disable** (see “Direction Attribute” on page 199 for more details.

8. Click *Submit* if you do not need to set other parameters.

> **Note:** If you are experiencing media negotiation problems (because the Aastra unit sends a BYE after receiving a 200 OK), try to set the *Enforce Offer Answer Model* value to **Disable** and the *Allow Less Media In Response* value to **Enable**.

TLS Interop

This section describes the TLS interop parameters of the Aastra unit.

▶ **To set the TLS interop parameters:**

1. In the *TLS Interop* section of the *Interop* page, select the level of security used to validate the TLS server certificate when the unit is acting as a TLS client in the *Certificate Validation* drop-down menu.

Figure 80: TLS Interop Section

> **Note:** This parameter has no effect on the TLS client authentication when the unit is acting as a TLS server (see the *interopTlsClientAuthenticationEnable* variable in “TLS Client Authentication” on page 308).

The following values are available:

Table 142: TLS Certificate Validation Parameters

Parameter	Description
No Validation	No validation of the peer certificate is performed. All TLS connections are accepted without any verification. Note that at least one certificate must be returned by the peer even if no validation is made. This option provides no security and should be restricted to a lab use only.
Trusted Certificate	Allows a TLS connection only if the peer certificate is trusted. A certificate is considered trusted when the certificate authority (CA) that signed the peer certificate is present in the *Management* > *Certificates* page ("Chapter 46 - Certificates Management" on page 557). This option provides a minimum level of security and should be restricted to a lab use only.
Dns Srv Response	Allows a TLS connection if the peer certificate is trusted and contains a known host name. A known host name can be the FQDN or IP address configured as the SIP server, or can also be returned by a DNS SRV request. In this case, the match is performed against the DNS response name. If it matches either one of the Subject Alternate Name (SAN) or Common Name (CN) in the peer certificate, the connection is allowed. This option provides an acceptable level of security, but not as good as *Host Name*.
HostName	Allows a TLS connection if the peer certificate is trusted and contains a known host name. A known host name can only be the FQDN or IP address configured as the SIP server. If it matches either one of the Subject Alternate Name (SAN) or Common Name (CN) in the peer certificate, the connection is allowed. This option provides the highest level of security.

2. Click *Submit* if you do not need to set other parameters.

Misc Interop

This section describes miscellaneous interop parameters of the Aastra unit.

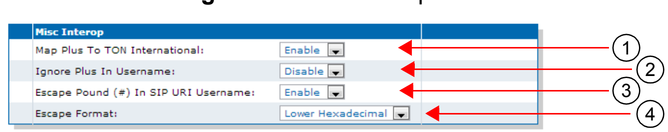
▶ **To set the Misc interop parameters:**

1. In the *Misc Interop* section of the *Interop* page, select whether or not the Aastra unit enables the mapping between the "+" prefix of the user name and the "type of number" property in the *Map Plus To TON International* drop-down menu.

When enabled, the service has the following behaviour:

- For a call to SIP, the Aastra unit prefixes the user name with '+' if the call has the call property "type of number" set to **international**. The unit also adds the "user" parameter with the value "phone" to the SIP URI. For instance: sip:1234@domain.com;user=phone.
- For a call from SIP, the Aastra unit sets the call property "type of number" to **international** if the user name has the prefix '+'.

Figure 81: Misc Interop Section



2. Define the *Ignore Plus in Username* drop-down menu as to whether or not the plus (+) character is ignored when attempting to match a challenge username with usernames in the Authentication table.

Table 143: Ignore Plus (+) Character in Username Parameters

Parameter	Description
Enable	The plus (+) character is ignored when attempting to match a username in the authentication table.
Disable	The plus (+) character is not ignored when attempting to match a username in the authentication table.

3. Select whether or not the pound character (#) must be escaped in the username part of a SIP URI in the *Escape Pound (#) in SIP URI Username* drop-down menu.

Table 144: Escape Pound Parameters

Parameter	Description
Enable	The Pound character (#) is escaped in the username part of a SIP URI.
Disable	The Pound character (#) is not escaped in the username part of a SIP URI. Note that RFC 3261 specifies that the pound character (#) needs to be escaped in the username part of a SIP URI.

4. Select the format of the escaped characters to be used in all SIP headers in the *Escape Format* drop-down menu.

Table 145: Escape Format Parameters

Parameter	Description
Lower Hexadecimal	Escaped characters are displayed in a lowercase hexadecimals format.
Upper Hexadecimal	Escaped characters are displayed in a uppercase hexadecimals format.

5. Click *Submit* if you do not need to set other parameters.

Additional Interop Parameters

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

The interop parameters allow the Aastra unit to properly work, communicate, or connect with specific IP devices.

Call Waiting Private Number Criteria for SIP INFO

You can specify the call waiting criteria, in the form of a regular expression, that defines a private number received in a SIP INFO.

▶ **To set the Call Waiting Private Number Criteria:**

1. In the *sipEpMIB*, set the Call Waiting Private Number Criteria in the `InteropCallWaitingSipInfoPrivateNumberCriteria` variable.

   You can also use the following line in the CLI or a configuration script:

   `sipEp.interopCallWaitingSipInfoPrivateNumberCriteria="Value"`

   For example, the value "(Anonymous|anonymous)" would define a calling number that is either "Anonymous" or "anonymous" as private. The regular expression symbols to match the beginning and end of the number are implicit and do not need to be specified. See "Regular Expressions" on page 463 for more details.

   The variable is effective only if the *Default Hook-Flash Processing* parameter of the *SIP > Misc* page is set to **TransmitUsingSignalingProtocol** (see "General Configuration" on page 417 for more details).

Max-Forwards Header

Standards Supported	• RFC 3261: SIP: Session Initiation Protocol

Max-Forwards serves to limit the number of hops a request can make on the way to its destination. It consists of an integer that is decremented by one at each hop. If the Max-Forwards value reaches 0 before the request reaches its destination, it is rejected with a "483 (Too Many Hops)" error response. The *Max-Forwards* SIP header is always present and the default value is 70.

Direction Attributes in a Media Stream

The Aastra unit allows you to define various direction attributes pertaining to the media stream.

When Putting a Call on Hold

Standards Supported	• RFC 3264: An Offer/Answer Model with Session Description Protocol (SDP)

The Aastra unit can provide the direction attribute and the meaning of the connection address "0.0.0.0" sent in the SDP when an endpoint is put on hold.

The following parameters are supported:

Table 146: Direction Attributes

Parameter	Description
inactive	The stream is put on hold by marking it as *inactive*. This is the default value. This setting should be used for backward compatibility issues.
sendonly	The stream is put on hold by marking it as *sendonly*. This method allows the Aastra unit to be in conformance with RFC 3264.

▶ **To define the direction attribute when putting a call on hold:**

1. In the *sipEpMIB*, set the `interopOnHoldSdpStreamDirection` variable to the proper value.

   You can also use the following line in the CLI or a configuration script:

   `sipEp.interopOnHoldSdpStreamDirection="Value"`

   where *Value* may be as follows:

Table 147: Direction Attributes Values

Value	Meaning
100	inactive

Table 147: Direction Attributes Values (Continued)

Value	Meaning
200	sendonly

This configuration has no effect if the `interopSdpDirectionAttributeEnable` variable is set to **disable** (see “Direction Attribute” on page 199 for more details).

Direction Attribute

Standards Supported	• RFC 2543: SIP: Session Initiation Protocol • RFC 3264: An Offer/Answer Model with Session Description Protocol (SDP)

You can define if the SDP direction attribute is supported by the unit.

This variable applies only when the negotiated media uses an IPv4 address. The application always behaves as if this variable is set to Enable for media using an IPv6 address.

The following parameters are supported:

Table 148: SDP Direction Attribute

Parameter	Description
disable	No direction attribute is present in the SDP sent by the Aastra unit. The Aastra unit ignores any direction attribute found in the SDP received from the peer. The method to put a session on hold is in conformance with RFC 2543.
enable	The Aastra unit always sends the direction attribute in the SDP of an initiated call. For all other SDP messages sent by the unit, refer to “Enable/Disable SDP Detect Peer Direction Attribute Support” on page 199. If present in the SDP, the direction attribute is preferred over the connection address to transmit session modification information. This method is in conformance with RFC 3264.

▶ **To define if the direction attribute is present:**

1. In the *sipEpMIB*, set the `interopSdpDirectionAttributeEnable` variable to the proper value.

   You can also use the following line in the CLI or a configuration script:

   ```
   sipEp.interopSdpDirectionAttributeEnable="Value"
   ```

   where *Value* may be as follows:

Table 149: SDP Direction Attribute

Value	Meaning
0	disable
1	enable

Enable/Disable SDP Detect Peer Direction Attribute Support

You can define if the SDP direction attribute support should be autodetected in the SDP received from the peer.

This variable is used only when the negotiated media uses an IPv4 address and when the `interopSdpDirectionAttributeEnable` is enabled (see “Direction Attribute” on page 199 for more details). The application always behaves as if this variable is set to 'Disable' for media using an IPv6 address.

The following parameters are supported:

Table 150: SDP Detect Peer Direction Attribute Parameters

Parameter	Description
disable	The Aastra unit always sends the direction attribute in the SDP without autodetection of peer support.
enable	The initial handshake determines if the peer supports the direction attribute. The direction attribute will be present when the peer supports it.

▶ **To define if the SDP detect peer direction attribute is enabled or disabled:**

1. In the *sipEpMIB*, set the `interopSdpDetectPeerDirectionAttributeSupportEnable` variable to the proper value.

You can also use the following line in the CLI or a configuration script:

```
sipEp.interopSdpDetectPeerDirectionAttributeSupportEnable="Value"
```

where *Value* may be as follows:

Table 151: SDP Detect Peer Direction Attribute Values

Value	Meaning
0	disable
1	enable

On Hold SDP Connection Address

You can define the value of the connection address sent in the SDP when an endpoint is on hold and no longer listening to media packets.

This variable is used only when the negotiated media uses an IPv4 address. The application always behaves as if this variable is set to 'MediaAddress' for media using an IPv6 address.

The following parameters are supported:

Table 152: On Hold SDP Connection Address Parameters

Parameter	Description
HoldAddress	The connection address sent in the SDP is '0.0.0.0' if the media uses an IPv4 address. This method is described by RFC 2543.
MediaAddress	The connection address sent in the SDP is the listening address.

▶ **To define the on hold SDP connection address:**

1. In the *sipEpMIB*, set the `interopOnHoldSdpConnectionAddress` variable to the proper value.

You can also use the following line in the CLI or a configuration script:

```
sipEp.interopOnHoldSdpConnectionAddress="Value"
```

where *Value* may be as follows:

Table 153: On Hold SDP Connection Address Values

Value	Meaning
100	HoldAddress
200	MediaAddress

Answering a Hold Offer with the Direction Attribute “sendonly”

Standards Supported	• RFC 3264: An Offer/Answer Model with Session Description Protocol (SDP)

You can define how to set the direction attribute in the SDP when answering a hold offer with the direction attribute 'sendonly'.

The following parameters are supported:

Table 154: “sendonly” Direction Attribute

Parameter	Description
inactive	The stream is marked as inactive and if the stream uses an IPv4 address, the connection address is set according to the *InteropOnHoldSdpConnectionAddress* variable (“On Hold SDP Connection Address” on page 200).
revconly	If the stream is currently active or receive only, it is marked as recvonly and the connection address is set to the IP address of the unit. If the stream is currently send only or inactive, it is marked as inactive and the connection address is set according to the *InteropOnHoldSdpConnectionAddress* variable (“On Hold SDP Connection Address” on page 200). This method is in conformance with RFC 3264.

▶ **To define the behaviour with the “sendonly” direction attribute:**

1. In the *sipEpMIB*, set the `InteropOnHoldAnswerSdpStreamDirection` variable to the proper value.

You can also use the following line in the CLI or a configuration script:

```
sipEp.interopOnHoldAnswerSdpStreamDirection="Value"
```

where *Value* may be as follows:

Table 155: “sendonly” Direction Attribute

Value	Meaning
100	inactive
200	Recvonly

In both cases, no direction attribute is present in the SDP if the `interopSdpDirectionAttributeEnable` variable is set to **disable** (see “Direction Attribute” on page 199 for more details.

SDP Direction Attribute Level

Standards Supported	• RFC 3264: An Offer/Answer Model with Session Description Protocol (SDP)

You can define the preferred location where the stream direction attribute is set.

The following parameters are supported:

Table 156: SDP Direction Attribute Level

Parameter	Description
MediaOrSessionLevel	If every media have the same direction, the stream direction attribute is only present at session level. Otherwise, the stream direction attribute is only present at media level.

Table 156: SDP Direction Attribute Level (Continued)

Parameter	Description
MediaAndSessionLevel	If every media have the same direction, the stream direction attribute is present both at session level and media level. Otherwise, the stream direction attribute is only present at media level.

▶ **To define the SDP direction attribute level:**

1. In the *sipEpMIB*, set the `InteropSdpDirectionAttributeLevel` variable to the proper value.

   You can also use the following line in the CLI or a configuration script:

   `sipEp.InteropSdpDirectionAttributeLevel="Value"`

   where *Value* may be as follows:

Table 157: SDP Direction Attribute Level

Value	Meaning
100	MediaOrSessionLevel
200	MediaAndSessionLevel

Local Ring Behaviour on Provisional Response

You can set the Aastra unit so that it starts or not the local ring upon receiving a “18x Provisional” response without SDP.

This setting does not affect the behaviour when the “18x Provisional” response contains SDP, which allows establishing an early media session before the call is answered.

This variable does not affect the behaviour in case the '18x Provisional' response contains SDP, in which case the media stream, if present, is played.

The following parameters are supported:

Figure 82: Local Ring Behaviour

Parameter	Description
Disable	The local ring is not started on a '18x Provisional' response without SDP, with one exception: the '180 Ringing' without SDP will start the local ring if the media stream is not already established.
LocalRingWhenNoEstablishedMediaStream	: The local ring is started on any '18x Provisional' response without SDP if the media stream is not already established.
LocalRingAlways	The local ring is always started on any '18x Provisional' response without SDP.

▶ **To define the local ring behaviour on provisional response:**

1. In the *sipEpMIB*, set the `interopLocalRingOnProvisionalResponse` variable to the proper value.

   You can also use the following line in the CLI or a configuration script:

   `sipEp.interopLocalRingOnProvisionalResponse="Value"`

   where *Value* may be as follows:

Figure 83: Local Ring Values

Value	Meaning
0	disable
1	LocalRingWhenNoEstablishedMediaStream

Figure 83: Local Ring Values (Continued)

Value	Meaning
2	LocalRingAlways

Session ID and Session Version Number in the Origin Field of the SDP

You can define the maximum length of the session ID and the session version number in the origin line (o=) of the SDP. This allows the Aastra unit to be compatible with 3rd party vendor equipment.

The following parameters are supported:

Table 158: Maximum Length Parameters

Length	Description
max-32bits	The session ID and the session version number are represented with a 32 bit integer. They have a maximum length of 10 digits.
max-64bits	The session ID and the session version number are represented with a 64 bit integer. They have a maximum length of 20 digits. This is the default value.

► **To set the maximum length of the session ID and the session version number:**

1. In the *sipEpMIB*, set the `interopSdpOriginLineSessionIDAndVersionMaxLength` variable with the proper length.

You can also use the following line in the CLI or a configuration script:

```
sipEp.interopSdpOriginLineSessionIdAndVersionMaxLength="Value"
```

where *Value* may be as follows:

Table 159: Maximum Length Values

Value	Meaning
100	max-32bits
200	max-64bits

Register Home Domain Override

By default, the address-of-record in the “To” header uses the value set in the *Proxy Host* field of the *SIP/ Configuration* page for the host/port part. See “SIP Servers Configuration” on page 282 for more details. You can override this value if required.

► **To override the register home domain value:**

1. In the *sipEpMIB*, set the `interopRegisterHomeDomainOverride` variable with the override home domain value.

You can also use the following line in the CLI or a configuration script:

```
sipEp.interopRegisterHomeDomainOverride="IP_Address"
```

The address of record in the register will use this string instead of the home domain proxy. If the variable is empty, the value of the *Proxy Host* field is used.

The host is also overridden in the *From* and *Call-Id* headers since they match the *To* header.

DNS SRV Record Lock

Standards Supported	• RFC 3263 - Session Initiation Protocol (SIP): Locating SIP Servers

You can configure the Aastra unit to always use the same DNS SRV record for a SIP call ID. As a result, a call or registration always uses the same destination until the destination is unreachable or the unit receives a different DNS SRV result.

The following parameters are supported:

Table 160: DNS SRV Record Lock Parameters

Length	Description
disable	The behaviour follows RFC 3263.
enable	All messages during a call or registration use the same SRV record.

To enable the DNS SRV record lock feature:

1. In the *sipEpMIB*, set the `interopLockDnsSrvRecordPerCallEnable` variable to **enable**.

   You can also use the following line in the CLI or a configuration script:

   `sipEp.interopLockDnsSrvRecordPerCallEnable="Value"`

   where *Value* may be as follows:

Figure 84: DNS SRV Record Lock Values

Value	Meaning
0	disable
1	enable

Listening for Early RTP

You can set the Aastra unit so that it listens for RTP before the reception of a response with SDP. This feature only applies to calls initiated from analog endpoints (FXS/FXO) with non-secure RTP.

The following parameters are supported:

Table 161: Early RTP Parameters

Length	Description
enable	The RTP port is opened after the initial INVITE has been sent, without waiting for a provisional or final response with SDP to be received. No local ring is generated. This conforms to section 5.1 of RFC 3264.
disable	The RTP port is opened only after a response with SDP is received.

STOP **Warning:** Do not enable this feature unless the server supports early RTP (or early media). Failing so prevents any ringing to be heard for outgoing calls.

To enable the Early RTP feature:

1. In the *sipEpMIB*, set the `InteropListenForEarlyRtpEnable` variable to **enable**.

   You can also use the following line in the CLI or a configuration script:

   `sipEp.InteropListenForEarlyRtpEnable="Value"`

where *Value* may be as follows:

Figure 85: Early RTP Values

Value	Meaning
0	disable
1	enable

Resolve Route Header

The Aastra unit has a parameter that allows you to resolve the FQDN in the top-most route header of outgoing packets.

The following parameters are supported:

Table 162: Resolve Route Header Parameters

Length	Description
enable	The FQDN in the top-most route header is replaced by the IP address of the packet's destination if the FQDN matches the gateway's configured outbound proxy.
disable	The route header is not modified.

► **To resolve the route header:**

1. In the *sipEpMIB*, set the `InteropResolveRouteHeaderEnable` variable with the proper value.

You can also use the following line in the CLI or a configuration script:

`sipEp.interopResolveRouteHeaderEnable="Value"`

where *Value* may be as follows:

Figure 86: Resolve Route Header Values

Value	Meaning
0	disable
1	enable

ACK Branch Matching

You can configure the method used to match incoming ACK SIP packets.

The following parameters are supported:

Table 163: ACK Branch Matching Parameters

Parameter	Description
Rfc3261	Follows the method described in RFC 3261 (section 8.1.1.7). The branch value in the topmost via of the ACK request to a 2XX response MUST be different than the one of the INVITE.
Rfc3261WithoutAck	Follows the method described in RFC 3261 (section 8.1.1.7) but enables the handling of ACK requests (for 2XX responses) that have the same branch value in the topmost via as the INVITE.

► **To set ACK branch matching:**

1. In the *sipEpMIB*, set the `interopAckBranchMatching` variable with the proper value.

You can also use the following line in the CLI or a configuration script:

`sipEp.interopAckBranchMatching="Value"`

where *Value* may be as follows:

Figure 87: ACK Branch Matching Values

Value	Meaning
100	Rfc3261
200	Rfc3261WithoutAck

Ignore Require Header

You can define whether or not the Require Header must be ignored when processing the incoming SIP Client requests (INVITE, re-INVITE, Bye, etc.).

The following parameters are supported:

Table 164: Ignore Require Header Parameters

Parameter	Description
Enable	The Require Header is ignored and no validation about these options-tags is performed.
Disable	The Require Header options-tags are validated and, when an option-tag is not supported, a 420 (Bad Extension) response is sent. The supported options-tags are: • * 100rel • * replaces • * timer

► **To set whether or not to ignore the Require header:**

1. In the *sipEpMIB*, set the `interopIgnoreRequireHeaderEnable` variable with the proper value.

   You can also use the following line in the CLI or a configuration script:

   `sipEp.interopIgnoreRequireHeaderEnable="Value"`

   where *Value* may be as follows:

Figure 88: Ignore Require Header Values

Value	Meaning
0	disable
1	enable

Ringing Response Code

You can define the response code sent back when the endpoint starts ringing.

The following parameters are supported:

Table 165: Ringing Response Code Parameters

Parameter	Description
Send180Ringing	Sends out a '180 Ringing' response without a body.
Send183WithSdp	Returns a '183 Session Progress' packet with SDP (needed if the endpoint is required to generate ringback on connection).

▶ **To set the ringing response code:**

1. In the *sipEpMIB*, set the `InteropRingingResponseCode` variable with the proper value.

You can also use the following line in the CLI or a configuration script:

`sipEp.InteropRingingResponseCode="Value"`

where *Value* may be as follows:

Figure 89: Ringing Response Code Values

Value	Meaning
100	Send180Ringing
200	Send183WithSdp

Reject Code for No Resource

You can define the rejection code used when all lines of the group are unavailable.

The following parameters are supported:

Table 166: Reject Code for No Resource Parameters

Parameter	Description
TemporarilyUnavailable	The '480 Temporarily Unavailable' rejection code is used.
BusyHere	The '486 Busy Here' rejection code is used.

▶ **To set the reject code:**

1. In the *sipEpMIB*, set the `InteropRejectCodeForNoRessource` variable with the proper value.

You can also use the following line in the CLI or a configuration script:

`sipEp.InteropRejectCodeForNoRessource="Value"`

where *Value* may be as follows:

Figure 90: Reject Code Values

Value	Meaning
100	TemporarilyUnavailable
200	BusyHere

Reject Code for Unsupported SDP Offer

You can define the rejection code used when an offer is received with invalid or unsupported SDP Offer. RFC 3261 recommends using the error code 488 'Not Acceptable Here'.

The following parameters are supported:

Table 167: Reject Code for Unsupported SDP Offer Parameters

Parameter	Description
UnsupportedMediaType	The SIP error code 415 'Unsupported Media Type' is returned if the Content-Type is invalid; the payload is missing or the SDP content is invalid.
NotAcceptableHere	The SIP error code 488 'Not Acceptable Here' is returned if the SDP content is invalid.

▶ **To set the reject code:**

1. In the *sipEpMIB*, set the `InteropRejectCodeForUnsupportedSdpOffer` variable with the proper value.

You can also use the following line in the CLI or a configuration script:

```
sipEp.InteropRejectCodeForUnsupportedSdpOffer="Value"
```

where *Value* may be as follows:

Figure 91: Reject Code Values

Value	Meaning
415	UnsupportedMediaType
488	NotAcceptableHere

SIP User-Agent Header Format

You can define the text to display in the SIP *User-Agent* header. You can use macros to include information specific to the unit.

You can also define the same information in the HTTP User-Agent header. See "HTTP User-Agent Header Format" on page 42 for more details.

▶ **To set the SIP User-Agent header format:**

1. In the *sipEpMIB*, set the *User-Agent* header format in the `interopUaHeaderFormat` variable.

You can also use the following line in the CLI or a configuration script:

```
sipEp.interopUaHeaderFormat="Value"
```

where *Value* may contain any text, as well as one or more of the following macros:

Table 168: Macros Supported

Macro	Description
%version%	Application version.
%mac%	MAC address.
%product%	Product name.
%profile%	Profile.
%%	Insert the % character.

For instance, the default value is:

```
%product%/v%version% %profile%
```

SIP INFO Without Content Answer

You can define the response of the Aastra unit to a received SIP INFO with no message body for an existing call.

RFC 2976 recommends that a 200 OK response MUST be sent for an INFO request with no message body if the INFO request was successfully received for an existing call.

The following parameters are supported:

Table 169: Reject Code for Unsupported SDP Offer Parameters

Parameter	Description
UnsupportedMediaType	The unit responds with the SIP error code 415 'Unsupported Media Type'.
Ok	The unit responds with a 200 OK.

▶ **To define the SIP INFO Without Content Answer behaviour:**

1. In the *sipEpMIB*, set the `interopSipInfoWithoutContentAnswer` variable with the proper behaviour.

You can also use the following line in the CLI or a configuration script:

`sipEp.interopSipInfoWithoutContentAnswer="Value"`

where *Value* may be as follows:

Table 170: SIP INFO Values

Value	Meaning
200	Ok
415	UnsupportedMediaType

Unsupported Content-Type

You can define the behaviour of the Aastra unit upon reception of a SIP packet containing multiple unsupported Content-Type in the payload.

The following parameters are supported:

Table 171: Unsupported Content-Type Parameters

Parameter	Description
Reject	Unsupported Content-Type are rejected.
Allow	Unsupported Content-Type are allowed and ignored if at least one Content-Type is supported.
Ignore	Unsupported Content-Type are ignored.

Note: When ignored, unsupported Content-Type are treated as if they were not present in the packet.

▶ **To define the unsupported Content-Type behaviour:**

1. In the *sipEpMIB*, set the `interopUnsupportedContentType` variable with the proper behaviour.

You can also use the following line in the CLI or a configuration script:

`sipEp.interopUnsupportedContentType="Value"`

where *Value* may be as follows:

Table 172: Unsupported Content-Type Values

Value	Meaning
100	Reject
200	Allow
300	Ignore

CHAPTER

27

Miscellaneous SIP Parameters

This chapter describes miscellaneous SIP parameters you can set:

- SIP penalty box parameters
- How to override the default mapping of error causes defined in RFC 3398.
- Additional Headers
- PRACK
- Session Refresh
- SIP Gateway Configuration
- SIAastraP Blind Transfer Method
- Diversion Configuration
- DNS Configuration
- Event Handling Configuration
- Messaging Subscription

SIP Penalty Box

The penalty box feature is used when a given host FQDN resolves to a non-responding address. When the address times out, it is put into the penalty box for a given amount of time. During that time, the address in question is considered as "non-responding" for all requests.

This feature is most useful when using DNS requests returning multiple or varying server addresses. It makes sure that, when a host is down, users wait a minimal amount of time before trying a secondary host.

When enabled, this feature takes effect immediately on the next call attempt.

The penalty box feature is applied only when using UDP or TCP connections established with a FQDN. A similar penalty box feature for the TLS persistent connections is available via the *TLS Persistent Retry Interval* parameter. See "SIP Transport Type" on page 305 for more details.

Penalty Box vs Transport Types

Aastra recommends to use this feature with care when supporting multiple transports (see "Chapter 28 - SIP Transport Parameters" on page 305 for more details) or you may experience unwanted behaviours.

When the Aastra unit must send a packet, it retrieves the destination from the packet. If the destination address does not specify a transport to use and does not have a DNS SRV entry that configures which transport to use, then the Aastra unit tries all transports it supports, starting with UDP. If this fails, it tries with TCP. The unit begins with UDP because all SIP implementations must support this transport, while the mandatory support of TCP was only introduced in RFC 3261.

> **Note:** It is not the destination itself that is placed in the penalty box, but the combination of address, port and transport. When a host is in the penalty box, it is never used to try to connect to a remote host unless it is the last choice for the Aastra unit and there are no more options to try after this host.

Let's say for instance that the Aastra unit supports both the UDP and TCP transports. It tries to reach endpoint "B" for which the destination address does not specify a transport and there is no DNS SRV entry to specify which transports to use in which order. It turns out that this endpoint "B" is also down. In this case, the Aastra unit first tries to contact endpoint "B" via UDP. After a timeout period, UDP is placed in the penalty box and the unit then tries to contact endpoint "B" via TCP. This fails as well and TCP is also placed in the penalty box.

Now, let’s assume endpoint “B” comes back to life and the Aastra unit tries again to contact it before UDP and TCP are released from the penalty box. First, the unit tries UDP, but it is currently in the penalty box and there is another transport left to try. The Aastra unit skips over UDP and tries the next target, which is TCP. Again, TCP is still in the penalty box, but this time, it is the last target the Aastra unit can try, so penalty box or not, TCP is used all the same to try to contact endpoint “B”.

There is a problem if endpoint “B” only supports UDP (RFC 2543-based implementation). Endpoint “B” is up, but the Aastra unit still cannot contact it: with UDP and TCP in the penalty box, the unit only tries to contact endpoint “B” via its last choice, which is TCP.

The same scenario would not have any problem if the penalty box feature was disabled. Another option is to disable TCP in the Aastra unit, which makes UDP the only possible choice for the unit and forces to use UDP even if it is in the penalty box.

You must fully understand the above problem before configuring this feature. Mixing endpoints that do not support the same set of transports with this feature enabled can lead to the above problems, so it is suggested to either properly configure SRV records for the hosts that can be reached or be sure that all hosts on the network support the same transport set before enabling this feature.

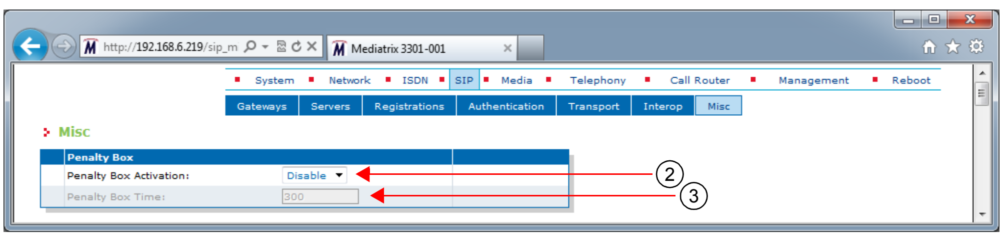
Penalty Box Configuration

The following steps describe how to configure the penalty box feature.

▶ **To set the SIP penalty box parameters:**

1. In the web interface, click the *SIP* link, then the *Misc* sub-link.

Figure 92: SIP Configuration – Misc Web Page



2. In the *Penalty Box* section, enable the SIP penalty box feature by selecting **Enable** in the *Penalty Box Activation* drop-down menu.

The penalty box is always “active”. This means that even if the feature is disabled, IP addresses are marked as invalid, but they are still tried. This has the advantage that when the feature is enabled, IP addresses that were already marked as invalid are instantly put into the penalty box.

3. Set the amount of time, in seconds, that a host spends in the penalty box in the *Penalty Box Time* field.

Changing the value does not affect IP addresses that are already in the penalty box. It only affects new entries in the penalty box.

4. Click *Submit* if you do not need to set other parameters.

Error Mapping

Standards Supported	• RFC 3398: Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping[a]

a. Only the ISDN to SIP error mapping is supported.

You can override the default mapping of error causes defined in RFC 3398.The web interface offers two sections:

- The *SIP To Cause Error Mapping* section allows you to override the default mapping for SIP code to ISDN cause.

- The *Cause To SIP Error Mapping* section allows you to override the default mapping for ISDN cause to SIP code.

The following standard SIP codes are available:

400: Bad Request	414: Request-URI too long	485: Ambiguous
401: Unauthorized	415: Unsupported media type	486: Busy here
402: Payment required	416: Unsupported URI Scheme	500: Server internal error
403: Forbidden	420: Bad extension	501: Not implemented
404: Not found	421: Extension Required	502: Bad gateway
405: Method not allowed	423: Interval Too Brief	503: Service unavailable
406: Not acceptable	480: Temporarily unavailable	504: Server time-out
407: Proxy authentication required	481: Call/Transaction Does not Exist	504: Version Not Supported
		513: Message Too Large
408: Request timeout	482: Loop Detected	600: Busy everywhere
410: Gone	483: Too many hops	603: Decline
413: Request Entity too long	484: Address incomplete	604: Does not exist anywhere

You can also map any other custom code between 400 and 699.

The following standard ISDN cause numbers specified in Q.931 are available:

Normal event:

1: Unassigned (unallocated) number.

2: No route to specified transit network.

3: No route to destination.

6: Channel unacceptable.

7: Call awarded and being delivered in an established channel.

17: User busy.

18: No user responding.

19: User alerting, no answer.

20: Subscriber absent.

21: Call rejected.

22: Number changed.

23: Redirection to new destination.

26: Non-selected user clearing.

27: Destination out of order.

28: Invalid number format (incomplete number).

29: Facility rejected.

30: Response to STATUS ENQUIRY.

31: Normal, unspecified.

Resource unavailable:

34: No circuit/channel available.

38: Network out of order.

41: Temporary failure.

42: Switching equipment congestion.

43: Access information discarded.

44: Requested circuit/channel not available.

47: Resource unavailable, unspecified.

Service or option not available:

55: Incoming calls barred within CUG.

57: Bearer capability not authorized.

58: Bearer capability not presently available.

63: Service or option not available, unspecified.

Service or option not implemented:

65: Bearer capability not implemented.

66: Channel type not implemented.

69: Requested facility not implemented.

70: Only restricted digital information bearer.

79: Service or option not implemented, unspecified.

Invalid Message

81: Invalid call reference value.

82: Identified channel does not exist.

83: A suspended call exists, but this call identity does not.

84: Call identity in use.

85: No call suspended.

86: Call having the requested call identity has been cleared.

87: user not member of CUG.

88: Incompatible destination.

91: Invalid transit network selection.

95: Invalid message, unspecified.

Protocol error

96: Mandatory information element is missing.

97: Message type non-existent or not implemented.

98: Message not compatible with call state or message type non-existent or not implemented.

99: Information element non-existent or not implemented.

100: Invalid information element contents.

101: Message not compatible with call state.

102: Recovery on time expiry.

111: Protocol error, unspecified.

Interworking

127: Interworking, unspecified

You can also map any other custom code between 1 and 127.

SIP to Cause Error Mapping

This section describes how to override the default mapping of ISDN error causes.

▶ **To override the default mapping of ISDN error causes:**

1. In the *SIP To Cause Error Mapping* section of the *Misc* page, click the button to add a new row.

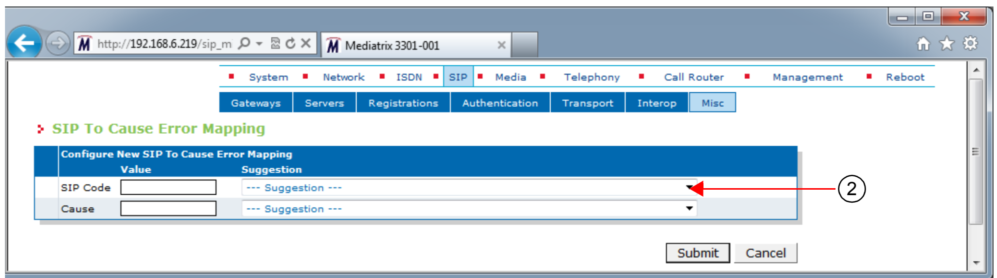
Figure 93: SIP To Cause Error Mapping Section

This brings you to the *Configure New SIP To Cause Error Mapping* panel.

2. Enter the SIP code in the *SIP Code* field, then the corresponding ISDN cause number in the *Cause* column.

You can use the *Suggestion* column's drop-down menu to select between available code values.

Figure 94: Configure New SIP To Cause Error Mapping Panel



3. Click *Submit*.

This brings you back to the main *Misc* web page.

You can delete an existing row by clicking the button.

You can modify the *Cause* value by typing a new code in the field. See "SIP To Cause Default Error Mapping" on page 215 for the default mappings as per RFC 3398.

4. Click *Submit* if you do not need to set other parameters.

SIP To Cause Default Error Mapping

Table 173 lists the default mappings as per RFC 3398.

Table 173: SIP To Cause Default Error Mapping

SIP Response Received		Cause Value	
400	Bad Request	41	Temporary Failure
401	Unauthorized	21	Call rejected
402	Payment required	21	Call rejected
403	Forbidden	21	Call rejected
404	Not found	1	Unallocated number
405	Method not allowed	63	Service or option unavailable
406	Not acceptable	79	Service/option not implemented
407	Proxy authentication required	21	Call rejected
408	Request timeout	102	Recovery on timer expiry
410	Gone	22	Number changed (w/o diagnostic)
413	Request Entity too long	127	Interworking
414	Request-URI too long	127	Interworking

Table 173: SIP To Cause Default Error Mapping (Continued)

SIP Response Received		Cause Value	
415	Unsupported media type	79	Service/option not implemented
416	Unsupported URI Scheme	127	Interworking
420	Bad extension	127	Interworking
421	Extension Required	127	Interworking
423	Interval Too Brief	127	Interworking
480	Temporarily unavailable	18	No user responding
481	Call/Transaction Does not Exist	41	Temporary Failure
482	Loop Detected	25	Exchange - routing error
483	Too many hops	25	Exchange - routing error
484	Address incomplete	28	Invalid Number Format
485	Ambiguous	1	Unallocated number
486	Busy here	17	User busy
500	Server internal error	41	Temporary failure
501	Not implemented	79	Not implemented, unspecified
502	Bad gateway	38	Network out of order
503	Service unavailable	41	Temporary failure
504	Server time-out	102	Recovery on timer expiry
504	Version Not Supported	127	Interworking
513	Message Too Large	127	Interworking
600	Busy everywhere	17	User busy
603	Decline	21	Call rejected
604	Does not exist anywhere	1	Unallocated number

Cause to SIP Error Mapping

This section describes how to override the default mapping of SIP codes.

▶ **To override the default mapping of SIP codes:**

1. In the *Cause To SIP Error Mapping* section of the *Misc* page, click the + button to add a new row.

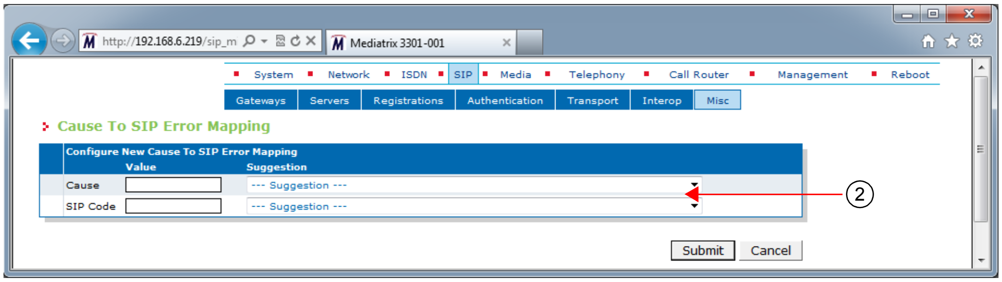
Figure 95: Cause To SIP Error Mapping Section

This brings you to the *Configure New Cause To SIP Error Mapping* panel.

2. Enter the ISDN cause number in the *Cause* column, then the corresponding SIP code in the *SIP Code* field.

You can use the *Suggestion* column's drop-down menu to select between available code values.

Figure 96: Configure New Cause To SIP Error Mapping Panel



3. Click *Submit*.

This brings you back to the main *Misc* web page.

You can delete an existing row by clicking the − button.

You can modify the *SIP Code* value by typing a new code in the field. See "Cause To SIP Default Error Mapping" on page 217 for the default mappings as per RFC 3398.

4. Click *Submit* if you do not need to set other parameters.

Cause To SIP Default Error Mapping

Table 174 lists the default mappings as per RFC 3398.

Table 174: Cause To SIP Default Error Mapping

ISUP Cause Value		SIP Response	
Normal Event			
1	unallocated number	404	Not Found
2	no route to network	404	Not Found
3	no route to destination	404	Not Found
16	normal call clearing	---	BYE or CANCEL
17	user busy	486	Busy Here
18	no user responding	408	Request Timeout
19	no answer from the user	480	Temporarily unavailable
20	subscriber absent	480	Temporarily unavailable
21	call rejected	403	Forbidden
22	number changed (w/o diagnostic)	410	Gone
22	number changed (w/ diagnostic)	301	Moved Permanently
23	redirection to new destination	410	Gone
26	non-selected user clearing	404	Not Found
27	destination out of order	502	Bad Gateway
28	address incomplete	484	Address incomplete
29	facility rejected	501	Not implemented
31	normal unspecified	480	Temporarily unavailable
Resource Unavailable			
34	no circuit available	503	Service unavailable
38	network out of order	503	Service unavailable

Table 174: Cause To SIP Default Error Mapping (Continued)

ISUP Cause Value		SIP Response	
41	temporary failure	503	Service unavailable
42	switching equipment congestion	503	Service unavailable
47	resource unavailable	503	Service unavailable
Service or Option not Available			
55	incoming calls barred within CUG	403	Forbidden
57	bearer capability not authorized	403	Forbidden
58	bearer capability not presently available	503	Service unavailable
Service or Option not Implemented			
65	bearer capability not implemented	488	Not Acceptable Here
70	only restricted digital available	488	Not Acceptable Here
79	service or option not implemented	501	Not implemented
Invalid message			
87	user not member of CUG	403	Forbidden
88	incompatible destination	503	Service unavailable
Protocol error			
102	recovery of timer expiry	504	Gateway timeout
111	protocol error	500	Server internal error
Interworking			
127	interworking unspecified	500	Server internal error

Additional Headers

You can define whether or not the Aastra unit uses additional SIP headers.

▶ **To use additional SIP headers:**

1. In the *Additional Headers* section of the *Misc* page, select the method to use in the *Reason Header Support* drop-down menu.

Figure 97: Reason Header Section

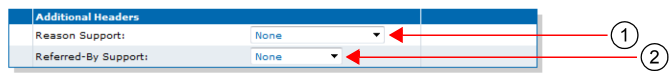


Table 175: Reason Header Support Parameters

Parameter	Description
None	Silently ignores any incoming reason headers and does not send the reason header.
SendQ850	Silently ignores incoming reason codes and sends the SIP reason code when the original Q.850 code is available. The reason code sent is not affected by the entries in the Error Mapping SIP To Cause table.
ReceiveQ850	Uses the incoming Q.850 reason cause header. When received, the reason code supersedes any entrie s in the Error Mapping SIP To Cause table.
SendReceiveQ850	Uses the incoming Q.850 reason cause header and sends the SIP reason code when the original Q.850 code is available. When received, the reason code supersedes any entries in the Error Mapping SIP To Cause table. The reason code sent is not affected by the entries in the Error Mapping SIP To Cause table.

2. Select how the Referred-By header is used when participating in a transfer in the *Referred-By Support* drop-down menu.

Table 176: Referred-By Support Parameters

Parameter	Description
None	When acting as the transferor (sending the REFER), the REFER does not contain a Referred-By header. When acting as the transferee (receiving the REFER and sending the INVITE to the target), the Referred-By header is not copied from the REFER to the INVITE.
HeaderOnly	When acting as the transferor (sending the REFER), the Referred-By header contains the SIP URI of the transferor. When acting as the transferee (receiving the REFER and sending the INVITE to the target), the Referred-By header is copied from the REFER to the INVITE.

3. Click *Submit* if you do not need to set other parameters.

4. Set the interval, in seconds, at which SIP Keep Alive requests using SIP OPTIONS or Ping are sent to verify the server status in the *Keep Alive Interval* field.

PRACK

Standards Supported	• RFC 3262: Reliability of Provisional Responses in the Session Initiation Protocol (SIP) • RFC 3311: The Session Initiation Protocol (SIP) UPDATE Method[a]

a. Only support receiving UPDATE. Sending an UPDATE is not supported.

The Aastra unit supports reliable provisional responses (PRACK) as per RFC 3262. You can define this support when acting as a user agent client and when acting as a user agent server.

The Aastra unit supports the UPDATE as per RFC 3311; however, its support is limited to reception.

▶ To define the PRACK support:

1. In the *PRACK* section of the *Misc* page, define the support of RFC 3262 (PRACK) when acting as a user agent server in the *UAS PRACK Support* drop-down menu.

Figure 98: PRACK Section

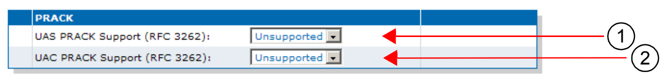


Table 177: PRACK User Agent Server Parameters

Parameter	Description
Unsupported	The option tag “100rel” is ignored if present in the *Supported* or *Required* header of received initial INVITEs and provisional responses are not sent reliably as per RFC 3261.
Supported	If the option tag “100rel” is present in the *Supported* or *Required* header of initial received INVITEs, provisional responses are sent reliably as per RFC 3262 by adding the option tag “100rel” to the *Require* header.

Receiving an UPDATE request to negotiate “early media” is supported only if you have selected **Supported**.

2. Define the support of RFC 3262 (PRACK) when acting as user agent client in the *UAC PRACK Support* drop-down menu.

Table 178: PRACK User Agent Client Parameters

Parameter	Description
Unsupported	The option tag “100rel” is not added in the *Supported* or *Required* header of sent INVITEs as per RFC 3261. If the provisional response contains a *Require* header field with the option tag “100rel”, the indication is ignored and no PRACK are sent.
Supported	The option tag “100rel” is added to the *Supported* header of sent initial INVITEs as per RFC 3262. If the received provisional response contains a *Require* header field with the option tag “100rel”, the response is sent reliably using the PRACK method.

Table 178: PRACK User Agent Client Parameters (Continued)

Parameter	Description
Required	The option tag “100rel” is added to the *Require* header of sent initial INVITEs as per RFC 3262. If the received provisional response contains a *Require* header field with the option tag “100rel”, the response is sent reliably using the PRACK method.

3. Click *Submit* if you do not need to set other parameters.

Forked Provisional Responses Behaviour

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

You can configure the unit's behaviour when receiving forked provisional answers. This configuration has no effect if the *UAC PRACK Support* drop-down menu is set to a value other than **Unsupported**.

The following values are supported:

Table 179: Forked Provisional Responses Behaviour Parameters

Value	Description
InterpretFirst	Only the first provisional answer is interpreted. Following responses do not change the state of the call and the SDP is ignored if present.
InterpretAll	Each forked provisional response received by the unit is interpreted replacing the previous one. If the response contains SDP, it replaces previous answers if any.

► **To set the forked provisional responses behaviour:**

1. In the *sipEpMIB*, define the behaviour in the `interopForkedProvisionalResponsesBehavior` variable.

   You can also use the following line in the CLI or a configuration script:

   `sipEp.interopForkedProvisionalResponsesBehavior=[value]`

   where *Value* may be as follows:.

Table 180: Forked Provisional Responses Behaviour Values

Value	Meaning
100	InterpretFirst
200	InterpretAll

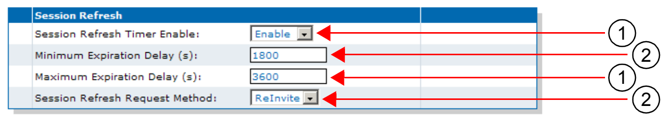
Session Refresh

This section allows you to define session refresh and session timers parameters. Session timers apply to the whole unit.

To set Session Refresh information:

1. In the *Session Refresh* section of the *Misc* page, define whether to enable or disable the session expiration services in the *Session Refresh Timer Enable* drop-down menu.

Figure 99: Session Refresh Section



Disabling this service is not recommended since it will make 'dead' calls impossible to detect.

See “Background Information” on page 222 for more details.

2. Set the session timer minimum expiration delay, in seconds, in the *Minimum Expiration Delay (s)* field.

This is the minimum value, in seconds, for the periodical session refreshes. It must be equal to or smaller than the maximum value. This value is reflected in the *Min-SE* header.

The *Min-SE* value is a threshold under which proxies and user agents on the signalling path are not allowed to go. Increasing the minimum helps to reduce network traffic, but also makes “dead” calls longer to detect.

3. Set the session timer maximum expiration delay, in seconds, in the *Maximum Expiration Delay (s)* field.

This is the suggested maximum time, in seconds, for the periodical session refreshes. It must be equal to or greater than the minimum value. This value is reflected in the *Session-Expires* header.

Increasing the maximum helps to reduce network traffic, but also makes “dead” calls longer to detect.

Note: When the *Maximum Expiration Delay* value is lower than the *Minimum Expiration Delay* value, the minimum and maximum expiration delay values in INVITE packets are the same as the value set in the *Minimum Expiration Delay* field.

4. Select the method used for sending Session Refresh Requests in the *Use UPDATE for Session Refresh* parameter.

Table 181: UPDATE for Session Refresh Parameters

Parameter	Description
ReInvite	Session Refresh Requests are sent with the INVITE method.
Update	Session Refresh Requests are sent with the UPDATE method.

Session Refresh Requests can be received via both methods, regardless of how this parameter is configured.

5. Click *Submit* if you do not need to set other parameters.

Background Information

The following explains how the session timers are used.

What is the session timer extension?

The session timer extension allows detecting the premature end of a call caused by a network problem or a peer’s failure by resending a refresh request at every *n* seconds. This refresh request is either an reINVITE or an UPDATE, according to the configuration of the *Session Refresh Request Method* parameter (see “PRACK” on page 220).

A successful response (200 OK) to this refresh request indicates that the peer is still alive and reachable. A timeout to this refresh request may mean that there are problems in the signalling path or that the peer is no longer available. In that case, the call is shut down by using normal SIP means.

SDP in Session Timer reINVITEs or UPDATEs

The reINVITE is sent with the last SDP that was negotiated. Receiving a session timer reINVITE should not modify the connection characteristics.

If the reINVITE method is used, it is sent with the last SDP that was negotiated. Reception of a session timer reINVITE should not modify the connection characteristics. If the UPDATE method is used, it is sent without any SDP offer. REMPLACER

Relation Between Minimum and Maximum Values

A user agent that receives a *Session-Expires* header whose value is smaller than the minimum it is willing to accept replies a “422 Timer too low” to the INVITE and terminates the call. The phone does not ring.

It is up to the caller to decide what to do when it receives a 422 to its INVITE. The Aastra unit will automatically retry the INVITE, with a *Session-Expires* value equal to the minimum value that the user agent server was ready to accept (located in the *Min-SE* header). This means that the maximum value as set in the Aastra unit might not be followed. This has the advantageous effect of establishing the call even if the two endpoints have conflicting values. The Aastra unit will also keep retrying as long as it gets 422 answers with different *Min-SE* values.

Who Refreshes the Session?

Sending a session timer reINVITE or UPDATE is referred to as refreshing the session. Normally, the user agent server that receives the INVITE has the last word on who refreshes. The Aastra unit always lets the user agent client (caller) perform the refreshes if the caller supports session timers. In the case where the caller does not support session timers, the Aastra unit assumes the role of the refresher.

SIP Gateway Configuration

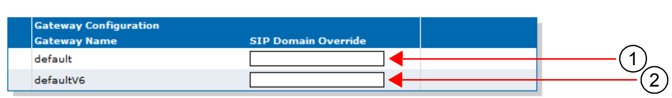
You can define whether or not to override the SIP domain used.

► **To set the SIP domain override:**

1. In the *SIP Gateway Configuration* section of the *Misc* page, define whether or not to override the SIP domain used in the *SIP Domain* field.

   If not empty, the address of record uses this string instead of the home domain proxy (*Proxy Host* field of the *Servers* sub-page – *SIP Default Servers* section (“SIP Servers Configuration” on page 282).

Figure 100: SIP Gateway Configuration Section



2. Click *Submit* if you do not need to set other parameters.

SIP Blind Transfer Method

You can set the SIP transfer method when an endpoint is acting as the transferor in a blind transfer scenario.

▶ **To set the SIP blind transfer method:**

1. In the *SIP Transfer* section of the *Misc* page, set the Blind Transfer Method.

Figure 101: SIP Transfer Section

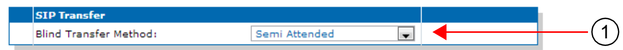


Table 182: SIP Blind Transfer Method Parameters

Parameter	Description
Semi Attended	When blind transfer is invoked by the transferor, the device sends immediately a REFER (it does not wait for the reception of the 200OK response). This allows the call transfer to be executed before the transfer-target answers. The transferee and the target are then connected together early and the transferee can hear the ringback from the target until the target answers.
Semi Attended Confirmed	When blind transfer is invoked by the transferor, the device waits for reception of the 200 OK from the transfer-target before sending a REFER to the transferee.
Semi Attended Cancelled	This method is similar to the Semi Attended Transfer method except that the INVITE sent to the transfer-target is cancelled when the blind transfer is invoked before receiving a 200OK (INVITE). In case where the transferor receives a 200OK (INVITE) from the transfer-target before receiving of a 487 Request Terminated, the transfer stays ongoing and it behaves as a Semi Attended Confirmed Transfer.

2. Click *Submit* if you do not need to set other parameters.

Diversion Configuration

You can define call diversion parameters.

Note: The Diversion feature is not available in the NI2 and QSIG signalling protocols. See “PRI Configuration” on page 184 for more details on how to configure the signalling protocol.

▶ **To set the call diversion parameters:**

1. In the *Diversion* section of the *Misc* page, set the *Methcd* drop-down menu with the SIP method used to receive/send call diversion information in an INVITE.

The gateways available are those defined in “SIP Gateways Configuration” on page 277.

Figure 102: Diversion Configuration Section

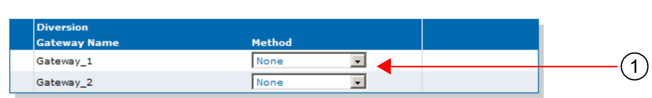


Table 183: Diversion Parameters

Parameter	Description
None	No diversion information is sent in SIP messages.

Table 183: Diversion Parameters (Continued)

Parameter	Description
Diversion Header	The SIP gateway supports the SIP header 'Diversion' (RFC 5806) in received and sent INVITEs, as well as in 302 messages.

2. Click *Submit* if you do not need to set other parameters.

DNS Configuration

You can define DNS-related parameters.

▶ **To set the DNS-related parameters:**

1. In the *DNS* section of the *Misc* page, set the *Supported DNS Queries* drop-down menu with the type of DNS queries that the SipEp service supports and uses.

Figure 103: DNS Configuration Section

Table 184: DNS Parameters

Parameter	Description
Address	Sends only Address requests (type A).
SRV	Sends a Service request (type SRV) first and then Address requests (type A) if needed.
NAPTR	Sends a Naming Authority Pointer request (type NAPTR) first and then Service requests (type SRV) or Address requests (type A) as needed.

2. Click *Submit* if you do not need to set other parameters.

Event Handling Configuration

The Aastra unit supports receiving event handling Notifications to start a remote reboot or a sync of configuration for specific endpoint(s). The event handling Notifications "reboot" or "check-sync" is not specified in an Allow-Events header. The Aastra unit supports the Notify without subscription.

It is recommended to use these event handling notifications only when the SIP transport is secure (TLS) or when the firewall filters the requests sent to the unit.

▶ **To set the event handling parameters:**

1. In the *Event Handling* section of the *Misc* page, set the *Reboot* column of each available gateway to define whether or not the SIP gateway can start a remote reboot via a SIP NOTIFY Event.

   This specifies whether a remote reboot via a SIP NOTIFY message event is supported or not for a specific SIP gateway.

Figure 104: Event Handling Parameters

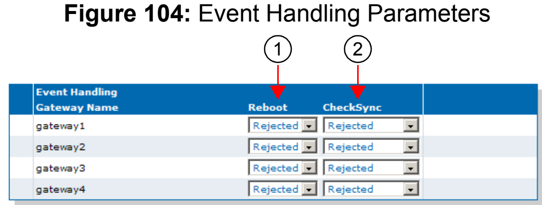


Table 185: Reboot Event Handling Parameters

Parameter	Description
Rejected	The "reboot" notification is rejected on reception.

Table 185: Reboot Event Handling Parameters (Continued)

Parameter	Description
Restart	When receiving a "reboot" notification, a restart of the unit is done.

2. Set the CheckSync column of each available gateway to define whether or not the SIP gateway can transfer and run a configuration file via a SIP NOTIFY Event.

   This specifies whether a transfer script via a SIP NOTIFY message event is supported or not for a specific SIP gateway.

Table 186: CheckSync Event Handling Parameters

Parameter	Description
Rejected	The "check-sync" notification is rejected on reception.
TransferScript	When receiving a "check-sync" notification, the Conf.ConfiguredScriptsTransferAndRun command is executed.

3. Click *Submit* if you do not need to set other parameters.

Messaging Subscription

The Aastra unit allows you to add the username in the Request-URI of SUBSCRIBEs it sends.

▶ **To set the messaging subscription:**

1. In the *Messaging Subscription* section of the *Misc* page, set the *Username in Request-URI* drop-down menu, set whether or not the unit adds the username in the request URI of MWI SUBSCRIBE requests.

Figure 105: Messaging Subscription Parameters

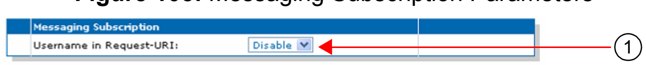


Table 187: Messaging Subscription Parameters

Parameter	Description
Enable	The unit adds the username in the Request-URI of sent MWI SUBSCRIBE requests.
Disable	No username in Request-URI of MWI SUBSCRIBE requests sent by the unit.

2. Click *Submit* if you do not need to set other parameters.

AastraMedia Parameters

Page Left Intentionally Blank

CHAPTER
28

Voice & Fax Codecs Configuration

This chapter describes the voice and fax codec configuration parameters.

- Codec descriptions.
- How to enable and disable the codecs.
- How to set the individual codecs' parameters.

Standards Supported	• RFC 3550: RTP: A Transport Protocol for Real-Time Applications • RFC 3551: RTP Profile for Audio and Video Conferences with Minimal Control

Codec Descriptions

The Aastra unit supports several voice and fax codecs. It also supports unicast applications, but not multicast ones. All voice transport is done over UDP.

All the endpoints of the Aastra unit can simultaneously use the same codec (for instance, G.711 PCMA), or a mix of any of the supported codecs. Set and enable these codecs for **each** endpoint.

Table 188: Codecs Comparison

	Compression	Voice Quality
G.711	None	Excellent
G.723.1[a]	Highest	Good
G.726	Medium	Fair
G.729a/ab	High	Fair/Good

a. This codec is not available on the Aastra Series models.

G.711 A-Law and µ-Law

Standards Supported	• ITU-T Recommendation G.711

The audio data is encoded as 8 bits per sample, after logarithmic scaling.

Table 189: G.711 Features

Feature	Description
Packetization time	Range of 10 ms to 30 ms with increments of 10 ms. See "G.711 Codec Parameters" on page 237 for more details. For the reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).
Voice Activity Detection (VAD)	Two levels of detection are available: transparent or conservative. See "Generic Voice Activity Detection (VAD)" on page 237 for more details.

Table 189: G.711 Features (Continued)

Feature	Description
Comfort noise	Uses custom comfort noise as defined in *RFC 3389*.
Available for voice	Yes
Available for fax	Yes
Available for modem	Yes

G.723.1

Standards Supported	• ITU-T Recommendation G.723.1[a]

a. This codec is not available on the Aastra Series models.

Dual-rate speech coder for multimedia communications transmitting at 5.3 kbit/s and 6.3 kbit/s. This Recommendation specifies a coded representation that can be used to compress the speech signal component of multi-media services at a very low bit rate. The audio is encoded in 30 ms frames.

A G.723.1 frame can be one of three sizes: 24 octets (6.3 kb/s frame), 20 octets (5.3 kb/s frame), or 4 octets. These 4-octet frames are called SID frames (Silence Insertion Descriptor) and are used to specify comfort noise parameters.

Table 190: G.723.1 Features

Feature	Description
Packetization time	Range of 30 ms to 60 ms with increments of 30 ms. See "G.723 Codec Parameters" on page 239 for more details. For the reception, the range is extended from 30 ms to 120 ms with increments of 30 ms only if the stream is not encrypted (SRTP).
Voice Activity Detection (VAD)	Supports the annex A, which is the built-in support of VAD in G.723.1.
Payload type	4
Available for voice	Yes
Available for fax	No
Available for modem	No

G.726

Standards Supported	• ITU-T Recommendation G.726: 40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM)

Algorithm recommended for conversion of a single 64 kbit/s A-law or U-law PCM channel encoded at 8000 samples/s to and from a 40, 32, 24, or 16 kbit/s channel. The conversion is applied to the PCM stream using an Adaptive Differential Pulse Code Modulation (ADPCM) transcoding technique.

Table 191: G.726 Features

Feature	Description
Packetization time	Range of 10 ms to 30 ms with increments of 10 ms. See "G.726 Codecs Parameters" on page 240 for more details. For the reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).
Voice Activity Detection (VAD)	Two levels of detection are available: transparent or conservative. See "Generic Voice Activity Detection (VAD)" on page 237 for more details.

Table 191: G.726 Features (Continued)

Feature	Description
Comfort noise	Uses custom comfort noise as defined in *RFC 3389*.
Payload type	Configurable as per "G.726 Codecs Parameters" on page 240.
Available for voice	Yes
Available for fax	Yes (32 kbps and 40 kbps)
Available for modem	Yes (32 kbps and 40 kbps)

G.729

Standards Supported	• ITU-T Recommendation G.729

Coding of speech at 8 kbit/s using conjugate structure-algebraic code excited linear prediction (CS-ACELP). For all data rates, the sampling frequency (and RTP timestamp clock rate) is 8000 Hz.

A voice activity detector (VAD) and comfort noise generator (CNG) algorithm in Annex B of G.729 is recommended for digital simultaneous voice and data applications; they can be used in conjunction with G.729 or G.729 Annex A. A G.729 or G.729 Annex A frame contains 10 octets, while the G.729 Annex B comfort noise frame occupies 2 octets.

The Aastra unit supports G.729A and G.729AB for encoding and G.729, G.729A and G.729AB for decoding.

Table 192: G.729 Features

Feature	Description
Packetization time	Range of 20 ms to 80 ms with increments of 10 ms. See "G.729 Codec Parameters" on page 242 for more details. For reception, the range is extended from 10 ms to 100 ms with increments of 10 ms only if the stream is not encrypted (SRTP).
Voice Activity Detection (VAD)	Supports the annex B, which is the built-in support of VAD in G.729. See "G.729 Codec Parameters" on page 242 for more details.
Payload type	18
Available for voice	Yes
Available for fax	No
Available for modem	No

Clear Mode

Standards Supported	• RFC 4040: RTP Payload Format for a 64 kbit/s Transparent Call

The Clear Mode codec is similar to the G.711 codec but without any modification of the 64 kbit/s payload (no encoding or decoding). The Clear Mode codec thus does not have echo cancellation and a fix jitter buffer. Clear Mode is a method to carry 64 kbit/s channel data transparently in RTP packets. This codec always uses the RTP transport.

Table 193: Clear Mode Features

Feature	Description
Packetization time	Range of 10 ms to 30 ms with increments of 10 ms. See "Clear Mode Codec Parameters" on page 243 for more details. For the reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).
Voice Activity Detection (VAD)	N/A
Comfort noise	N/A
Payload type	Configurable as per "Clear Mode Codec Parameters" on page 243.
Available for voice	Yes
Available for fax	Yes
Available for modem	Yes

Clear Channel

Standards Supported	• RFC 4040: RTP Payload Format for a 64 kbit/s Transparent Call

The Clear Channel codec is similar to the G.711 codec but without any modification of the 64 kbit/s payload (no encoding or decoding). The Clear Channel codec thus does not have echo cancellation and a fix jitter buffer. Clear Channel is a method to carry 64 kbit/s channel data transparently in RTP packets. The Clear Channel codec follows the specification of RFC 4040 and uses the "X-CLEAR-CHANNEL" mime type instead of the "CLEARMODE" mime type.

This codec always uses the RTP transport.

Table 194: Clear Channel Features

Feature	Description
Packetization time	Range of 10 ms to 30 ms with increments of 10 ms. See "Clear Channel Codec Parameters" on page 245 for more details. For the reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).
Voice Activity Detection (VAD)	N/A
Comfort noise	N/A
Payload type	Configurable as per "Clear Channel Codec Parameters" on page 245.
Available for voice	Yes
Available for fax	Yes
Available for modem	Yes

X-CCD Clear Channel

Standards Supported	• RFC 4040: RTP Payload Format for a 64 kbit/s Transparent Call

The Clear Channel codec is similar to the G.711 codec but without any modification of the 64 kbit/s payload (no encoding or decoding). The X-CCD Clear Channel codec thus does not have echo cancellation and a fix jitter buffer. The X-CCD Clear Channel is a method to carry 64 kbit/s channel data transparently in RTP packets. The Clear Channel codec follows the specification of RFC 4040 and uses the “X-CCD” mime type instead of the “CLEARMODE” mime type.

This codec always uses the RTP transport.

Table 195: X-CCD Clear Channel Features

Feature	Description
Packetization time	Range of 10 ms to 100 ms with increments of 1 ms. See “X-CCD Clear Channel Codec Parameters” on page 246 for more details.
Voice Activity Detection (VAD)	N/A
Comfort noise	N/A
Payload type	Configurable as per “X-CCD Clear Channel Codec Parameters” on page 246.
Available for voice	Yes
Available for fax	Yes
Available for modem	Yes

T.38

Standards Supported	• ITU-T Recommendation T.38 version 0

T.38 fax relay is a real-time fax transmission; that is, two fax machines communicating with each other as if there were a direct phone line between the two. T.38 is called a fax relay, which means that instead of sending inband fax signals, which implies a loss of signal quality, it sends those fax signals out-of-band in a T.38 payload, so that the remote end can reproduce the signal locally.

Table 196: T.38 Features

Feature	Description
Packetization time	N/A
Voice Activity Detection (VAD)	N/A
Payload type	N/A
Available for voice	No
Available for fax	Yes
Available for modem	No

T.38 is an unsecure protocol, thus will not be used along with secure RTP (SRTP), unless the *Allow Unsecure T.38 with Secure RTP* parameter has been set to **Enable**. See “Chapter 32 - Security” on page 377 for more details.

Codec Parameters

The *Codec* section allows you to enable or disable the codecs of the Aastra unit, as well as access the codec-specific parameters.

Standards Supported	• draft-choudhuri-sip-info-digit-00 • ITU-T Recommendation Q.24: Multifrequency push-button signal reception • RFC 2833: RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals • RFC 1890: RTP Profile for Audio and Video Conferences with Minimal Control

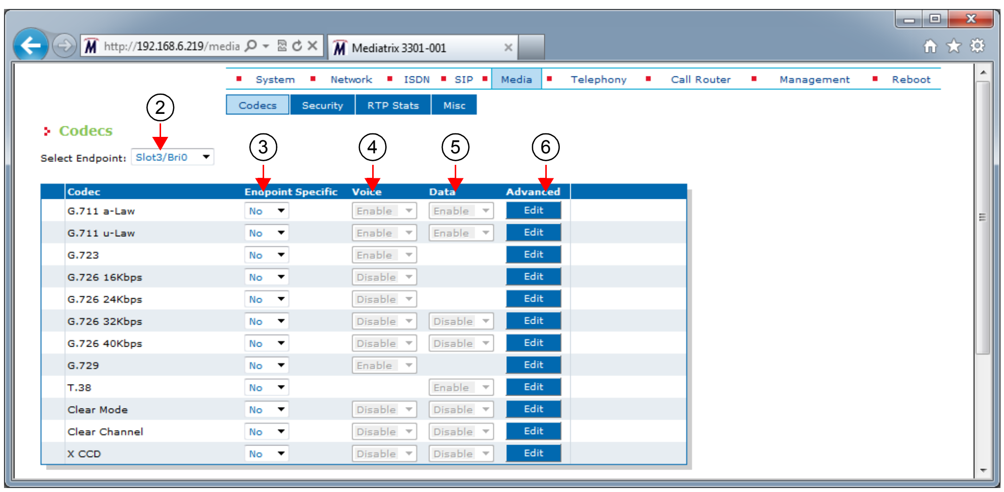
You can use two types of configuration:

- Default configurations that apply to all the endpoints of the Aastra unit.
- Specific configurations that override the default configurations. You can define specific configurations for each endpoint in your Aastra unit.

To enable or disable the codecs:

1. In the web interface, click the *Telephony* link, then the *CODECS* sub-link.

Figure 106: Telephony – Codecs Web Page



2. Select to which endpoint (interface) you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

   You have the choice between *Default* and the interfaces of your Aastra unit. The number of interfaces available vary depending on the Aastra unit model you have.

   You can also perform this operation in the codec-specific pages.

3. Select whether or not you want to override one or more of the available default codecs parameters in the *Endpoint Specific* column of the corresponding codec(s).

   This column is available only in the specific endpoints configuration.

   You can also perform this operation in the codec-specific pages.

4. Enable one or more codecs for voice transmission by selecting **Enable** in the *Voice* column of the corresponding codec(s).

   This indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

You can also perform this operation in the codec-specific pages.

5. Enable one or more codecs for data transmission by selecting **Enable** in the *Data* column of the corresponding codec(s).

This indicates if the codec can be selected for data transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

You can also perform this operation in the codec-specific pages.

6. Click the Edit button to access the corresponding codec-specific parameters.

These parameters are described in the following sections.

7. Click *Submit* if you do not need to set other parameters.

Generic Voice Activity Detection (VAD)

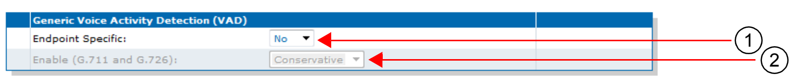
VAD defines how the Aastra unit sends information pertaining to silence. This allows the unit to detect when the user talks, thus avoiding to send silent RTP packets. This saves on network resources. However, VAD may affect packets that are not really silent (for instance, cut sounds that are too low). VAD can thus slightly affect the voice quality.

▶ **To set the generic Voice Activity Detection (VAD)**

1. In the *Generic Voice Activity Detection (VAD)* section, select whether or not you want to override the VAD parameters set in the *Default* configuration in the *Endpoint Specific* drop-down menu.

This menu is available only in the specific endpoints configuration.

Figure 107: Generic Voice Activity Detection (VAD) Section



2. Enable the G.711 and G.726 Voice Activity Detection (VAD) by selecting the proper setting in the *Enable (G711 and G726)* drop-down menu.

Table 197: G.711/G.726 VAD Settings

Setting	Description
Disable	VAD is not used.
Transparent	VAD is enabled. It has low sensitivity to silence periods.
Conservative	VAD is enabled. It has normal sensitivity to silence periods.

The difference between transparent and conservative is how “aggressive” the algorithm considers something as an inactive voice and how “fast” it stops the voice stream. A setting of conservative is a little bit more aggressive to react to silence compared to a setting of transparent.

3. Click *Submit* if you do not need to set other parameters.

G.711 Codec Parameters

The following are the G.711 codec parameters you can set. There are two sections for G.711:

- G.711 a-law
- G.711 u-law

These sections use the same parameters, so only one of them is described below.

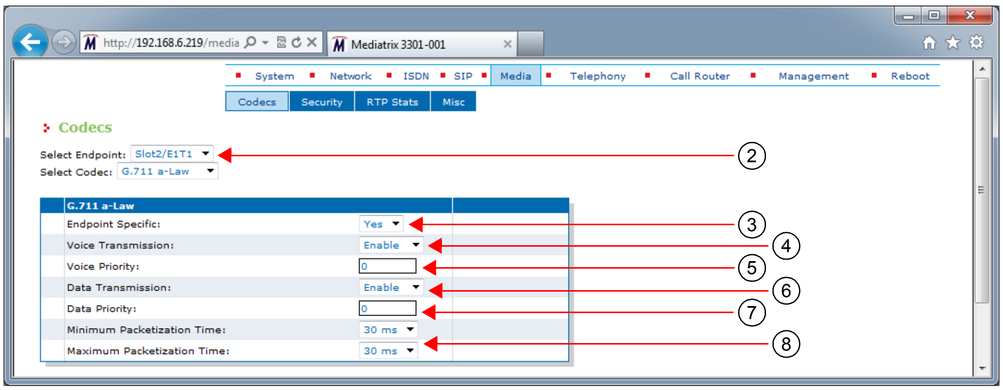
▶ To set the G.711 codec parameters:

1. In the *CODEC* section of the *CODECS* page, click the Edit button at the right of the corresponding G.711 codec to access the codec-specific parameters.

2. Select to which endpoint (interface) you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

You have the choice between *Default* and the interfaces of your Aastra unit. The number of interfaces available vary depending on the Aastra unit model you have.

Figure 108: G.711 a-law Section



3. Select whether or not you want to override the G.711 parameters set in the *Default* configuration in the *Use Endpoint Specific* drop-down menu.

This menu is available only in the specific endpoints configuration.

You can also perform this operation in the main *CODEC* section.

4. Enable the G.711 codec for voice transmission by selecting **Enable** in the *Voice Transmission* drop-down menu.

This indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

You can also perform this operation in the main *CODEC* section.

5. Set the default priority for voice in the *Voice Priority* field.

This sets the priority between different codecs. Codecs with a higher priority are used first, a priority of 0 being the lowest priority. For instance, a codec with priority 3 is used before a codec with priority 2. The maximum priority is 10.

The Aastra unit uses an internal order for codecs with the same priority.

Note: The codec used is also related to the SIP negotiation. The priority order affects the SIP negotiation, which decides on the codec to use.

6. Enable the G.711 codec for data transmission by selecting **Enable** in the *Data Transmission* drop-down menu.

This indicates if the codec can be selected for data transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

You can also perform this operation in the main *CODEC* section.

7. Set the default priority for data in the *Data Priority* field.

This sets the priority between different codecs. Codecs with a higher priority are used first, a priority of 0 being the lowest priority. For instance, a codec with priority 3 is used before a codec with priority 2. The maximum priority is 10.

The Aastra unit uses an internal order for codecs with the same priority.

8. Select the minimum and maximum packetization time values for the codec in the *Minimum Packetization Time* and *Maximum Packetization Time* drop-down menus.

The packetization time (also called packetization period or ptime) is the duration, in ms, of the voice packet. The range is from 10 ms to 30 ms with increments of 10 ms.

For the reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

9. Click *Submit* if you do not need to set other parameters.

You can also access the specific parameters of another codec by selecting the codec in the *Select CODEC* drop-down menu at the top of the page.

G.723 Codec Parameters

The following are the G.723 codec parameters you can set.

Note that the G.723 codec is not available on the Asatra TA7102i Series models.

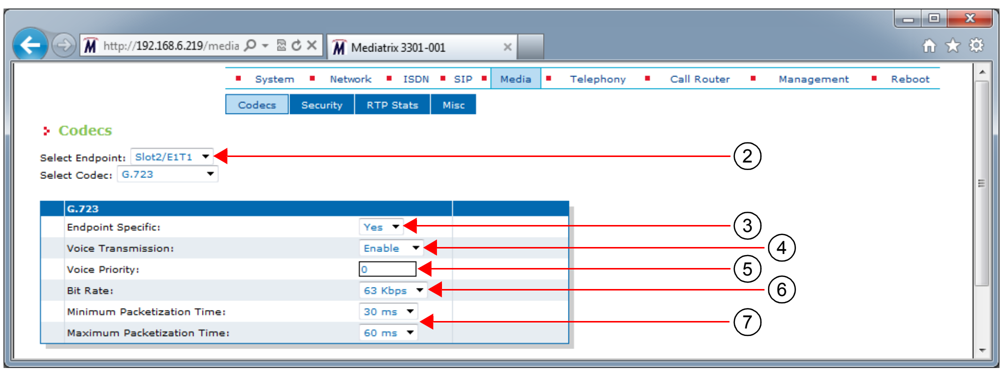
▶ **To set the G.723 codec parameters:**

1. In the *CODEC* section of the *CODECS* page, click the Edit button at the right of the G.723 codec to access the codec-specific parameters.

2. Select to which endpoint (interface) you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

You have the choice between *Default* and the interfaces of your Aastra unit. The number of interfaces available vary depending on the Aastra unit model you have.

Figure 109: G.723 Section



3. Select whether or not you want to override the G.723 parameters set in the *Default* configuration in the *Use Endpoint Specific* drop-down menu.

This menu is available only in the specific endpoints configuration.

You can also perform this operation in the main *CODEC* section.

4. Enable the G.723 codec for voice transmission by selecting **Enable** in the *Voice Transmission* drop-down menu.

This indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

You can also perform this operation in the main *CODEC* section.

5. Set the default priority for voice in the *Voice Priority* field.

This sets the priority between different codecs. Codecs with a higher priority are used first, a priority of 0 being the lowest priority. For instance, a codec with priority 3 is used before a codec with priority 2. The maximum priority is 10.

The Aastra unit uses an internal order for codecs with the same priority.

> **Note:** The codec used is also related to the SIP negotiation. The priority order affects the SIP negotiation, which decides on the codec to use.

6. Select the G.723 bit rate in the *Bit Rate* drop-down menu.

   You have the following choices:
   - 53 Kbs
   - 63 Kbs

7. Select the minimum and maximum packetization time values for the codec in the *Minimum Packetization Time* and *Maximum Packetization Time* drop-down menus.

   The packetization time (also called packetization period or ptime) is the duration, in ms, of the voice packet. The range is from 30 ms to 60 ms with increments of 30 ms.

   For the reception, the range is extended from 30 ms to 120 ms with increments of 30 ms only if the kstream is not encrypted (SRTP).

8. Click *Submit* if you do not need to set other parameters.

   You can also access the specific parameters of another codec by selecting the codec in the *Select CODEC* drop-down menu at the top of the page.

G.726 Codecs Parameters

The following are the G.726 codecs parameters you can set. There are four sections for G.726:

- G.726 16 Kbps
- G.726 24 Kbps
- G.726 32 Kbps
- G.726 40 Kbps

These sections offer almost the same parameters, except that you cannot use the G.726 16 Kbps and G.726 24 Kbps codecs for fax transmission.

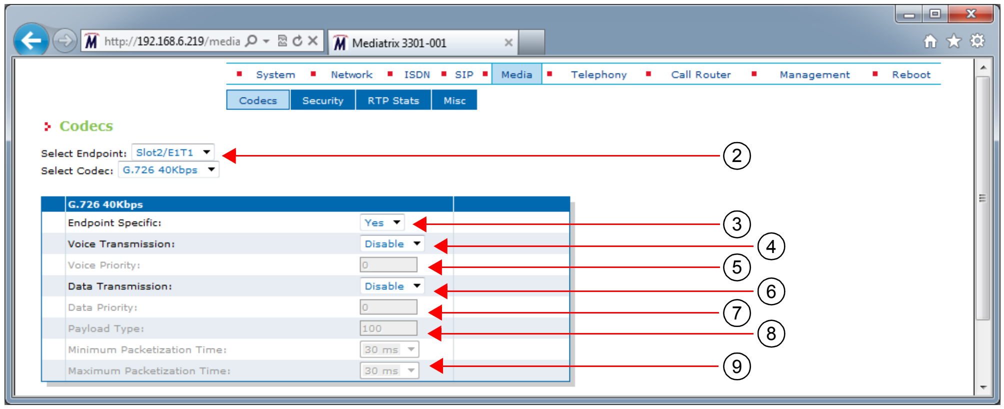
To set the G.726 codecs parameters:

1. In the *CODEC* section of the *CODECS* page, click the Edit button at the right of the corresponding G.726 codec to access the codec-specific parameters.

2. Select to which endpoint (interface) you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

   You have the choice between *Default* and the interfaces of your Aastra unit. The number of interfaces available vary depending on the Aastra unit model you have.

Figure 110: G.726 Section



3. Select whether or not you want to override the G.726 parameters set in the *Default* configuration in the *Use Endpoint Specific* drop-down menu.

This menu is available only in the specific endpoints configuration.

You can also perform this operation in the main *CODEC* section.

4. Enable the corresponding G.726 codec for voice transmission by selecting **Enable** in the *Voice Transmission* drop-down menu.

This indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

You can also perform this operation in the main *CODEC* section.

5. Set the default priority for voice in the *Voice Priority* field.

This sets the priority between different codecs. Codecs with a higher priority are used first, a priority of 0 being the lowest priority. For instance, a codec with priority 3 is used before a codec with priority 2. The maximum priority is 10.

The Aastra unit uses an internal order for codecs with the same priority.

Note: The codec used is also related to the SIP negotiation. The priority order affects the SIP negotiation, which decides on the codec to use.

6. Enable the codec for data transmission by selecting **Enable** in the *Data Transmission* drop-down menu.

This indicates if the codec can be selected for data transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

This menu is not available for the G.726 16 Kbps and G.726 24 Kbps codecs.

You can also perform this operation in the main *CODEC* section.

7. Set the default priority for data in the *Data Priority* field.

This sets the priority between different codecs. Codecs with a higher priority are used first, a priority of 0 being the lowest priority. For instance, a codec with priority 3 is used before a codec with priority 2. The maximum priority is 10.

The Aastra unit uses an internal order for codecs with the same priority.

This field is not available for the G.726 16 Kbps and G.726 24 Kbps codecs.

8. Set the G.726 actual RTP dynamic payload type used in an initial offer in the *Payload Type* field.

The payload types available are as per RFC 3551. The values range from 96 to 127. The default values are as follows:

Table 198: G.726 Default Payload Type

Codec	Default Value
G.726 (16 kbps)	97
G.726 (24 kbps)	98
G.726 (32 kbps)	99
G.726 (40 kbps)	100

9. Select the minimum and maximum packetization time values for the G.726 codec in the *Minimum Packetization Time* and *Maximum Packetization Time* drop-down menus.

The packetization time (also called packetization period or ptime) is the duration, in ms, of the voice packet. The range is from 10 ms to 30 ms with increments of 10 ms.

For the reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

10. Click *Submit* if you do not need to set other parameters.

You can also access the specific parameters of another codec by selecting the codec in the *Select CODEC* drop-down menu at the top of the page.

G.729 Codec Parameters

The following are the G.729 codec parameters you can set.

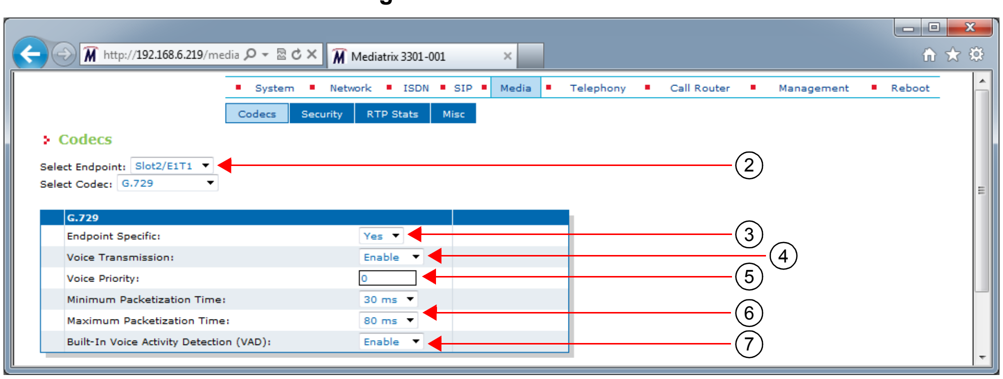
▶ **To set the G.729 codec parameters:**

1. In the *CODEC* section of the *CODECS* page, click the Edit button at the right of the G.729 codec to access the codec-specific parameters.

2. Select to which endpoint (interface) you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

You have the choice between *Default* and the interfaces of your Aastra unit. The number of interfaces available vary depending on the Aastra unit model you have.

Figure 111: G.729 Section



3. In the *G.729* section, select whether or not you want to override the G.729 parameters set in the *Default* configuration in the *Use Endpoint Specific* drop-down menu.

This menu is available only in the specific endpoints configuration.

You can also perform this operation in the main *CODEC* section.

4. Enable the G.729 codec for voice transmission by selecting **Enable** in the *Voice Transmission* drop-down menu.

This indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

You can also perform this operation in the main *CODEC* section.

5. Set the default priority for voice in the *Voice Priority* field.

This sets the priority between different codecs. Codecs with a higher priority are used first, a priority of 0 being the lowest priority. For instance, a codec with priority 3 is used before a codec with priority 2. The maximum priority is 10.

The Aastra unit uses an internal order for codecs with the same priority.

> **Note:** The codec used is also related to the SIP negotiation. The priority order affects the SIP negotiation, which decides on the codec to use.

6. Select the minimum and maximum packetization time values for the codec in the *Minimum Packetization Time* and *Maximum Packetization Time* drop-down menus.

The packetization time (also called packetization period or ptime) is the duration, in ms, of the voice packet. The range is from 20 ms to 80 ms with increments of 10 ms.

For reception, the range is extended from 10 ms to 100 ms with increments of 10 ms only if the stream is not encrypted (SRTP).

7. Select the G.729 Voice Activity Detection (VAD) in the *Built-in Voice Activity Detection (VAD)* drop-down menu.

Table 199: G.729 VAD

Parameter	Description
Disable	G.729 uses annex A only.
Enable	G.729 annex A is used with annex B. Speech frames are only sent during talkspurts (periods of audio activity). During silence periods, no speech frames are sent, but Comfort Noise (CN) packets containing information about background noise may be sent in accordance with annex B of G.729.

VAD defines how the Aastra unit sends information pertaining to silence. This allows the unit to detect when the user talks, thus avoiding to send silent RTP packets. This saves on network resources. However, VAD may affect packets that are not really silent (for instance, cut sounds that are too low). VAD can thus slightly affect the voice quality.

G.729 has a built-in VAD in its Annex B version. It is recommended for digital simultaneous voice and data applications and can be used in conjunction with G.729 or G.729 Annex A. A G.729 or G.729 Annex A frame contains 10 octets, while the G.729 Annex B frame occupies 2 octets. The CN packets are sent in accordance with annex B of G.729.

8. Click *Submit* if you do not need to set other parameters.

You can also access the specific parameters of another codec by selecting the codec in the *Select CODEC* drop-down menu at the top of the page.

Clear Mode Codec Parameters

The following are the Clear Mode codec parameters you can set.

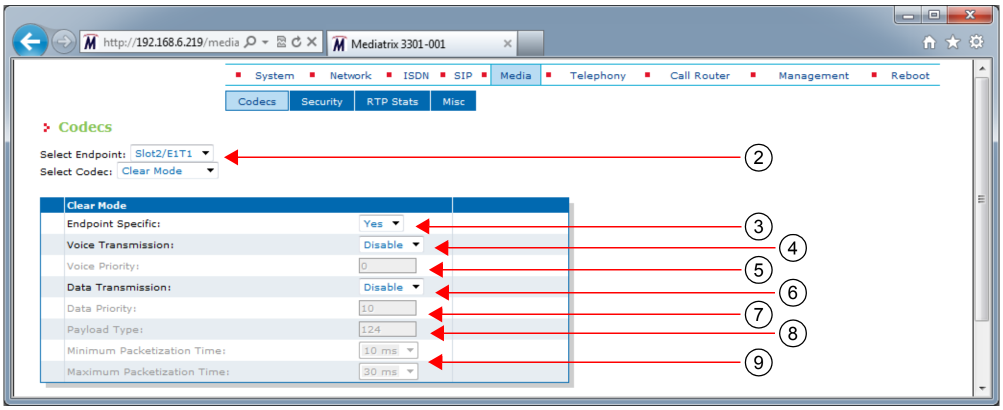
▶ To set the Clear Mode codec parameters:

1. In the *CODEC* section of the *CODECS* page, click the Edit button at the right of the Clear Mode codec to access the codec-specific parameters.

2. Select to which endpoint (interface) you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

   You have the choice between *Default* and the interfaces of your Aastra unit. The number of interfaces available vary depending on the Aastra unit model you have.

Figure 112: Clear Mode Section



3. Select whether or not you want to override the Clear Mode parameters set in the *Default* configuration in the *Use Endpoint Specific* drop-down menu.

   This menu is available only in the specific endpoints configuration.

   You can also perform this operation in the main *CODEC* section.

4. Enable the Clear Mode codec for voice transmission by selecting **Enable** in the *Voice Transmission* drop-down menu.

   This indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

   You can also perform this operation in the main *CODEC* section.

5. Set the default priority for voice in the *Voice Priority* field.

   This sets the priority between different codecs. Codecs with a higher priority are used first, a priority of 0 being the lowest priority. For instance, a codec with priority 3 is used before a codec with priority 2. The maximum priority is 10.

   The Aastra unit uses an internal order for codecs with the same priority.

> **Note:** The codec used is also related to the SIP negotiation. The priority order affects the SIP negotiation, which decides on the codec to use.

6. Enable the Clear Mode codec for data transmission by selecting **Enable** in the *Data Transmission* drop-down menu.

   This indicates if the codec can be selected for data transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

   You can also perform this operation in the main *CODEC* section.

7. Set the default priority for data in the *Data Priority* field.

   This sets the priority between different codecs. Codecs with a higher priority are used first, a priority of 0 being the lowest priority. For instance, a codec with priority 3 is used before a codec with priority 2. The maximum priority is 10.

   The Aastra unit uses an internal order for codecs with the same priority.

8. Set the Clear Mode RTP dynamic payload type used in an initial offer in the *Payload Type* field.

The payload types available are as per RFC 3551. The values range from 96 to 127. The default value is 125.

9. Select the minimum and maximum packetization time values for the codec in the *Minimum Packetization Time* and *Maximum Packetization Time* drop-down menus.

The packetization time (also called packetization period or ptime) is the duration, in ms, of the voice packet. The range is from 10 ms to 30 ms with increments of 10 ms.

For the reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

10. Click *Submit* if you do not need to set other parameters.

You can also access the specific parameters of another codec by selecting the codec in the *Select CODEC* drop-down menu at the top of the page.

Clear Channel Codec Parameters

The following are the Clear Channel codec parameters you can set.

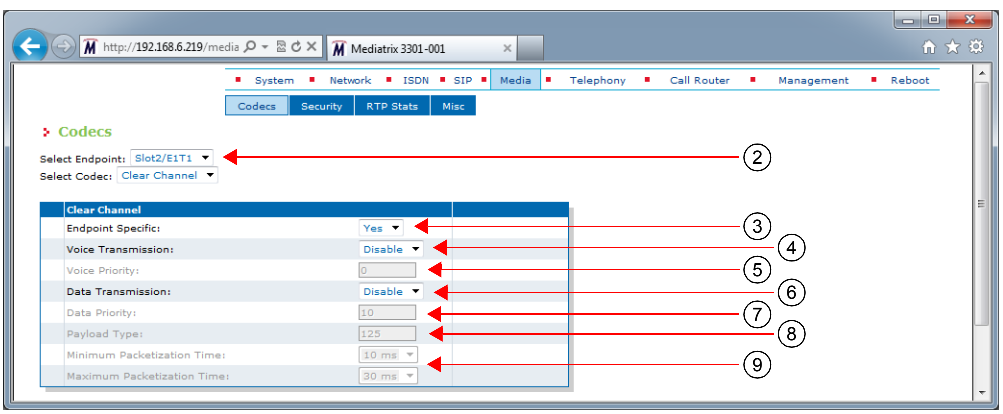
▶ **To set the Clear Channel codec parameters:**

1. In the *CODEC* section of the *CODECS* page, click the Edit button at the right of the Clear Channel codec to access the codec-specific parameters.

2. Select to which endpoint (interface) you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

You have the choice between *Default* and the interfaces of your Aastra unit. The number of interfaces available vary depending on the Aastra unit model you have.

Figure 113: Clear Channel Section



3. Select whether or not you want to override the Clear Channel parameters set in the *Default* configuration in the *Use Endpoint Specific* drop-down menu.

This menu is available only in the specific endpoints configuration.

You can also perform this operation in the main *CODEC* section.

4. Enable the Clear Channel codec for voice transmission by selecting **Enable** in the *Voice Transmission* drop-down menu.

This indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

You can also perform this operation in the main *CODEC* section.

5. Set the default priority for voice in the *Voice Priority* field.

This sets the priority between different codecs. Codecs with a higher priority are used first, a priority of 0 being the lowest priority. For instance, a codec with priority 3 is used before a codec with priority 2. The maximum priority is 10.

The Aastra unit uses an internal order for codecs with the same priority.

> **Note:** The codec used is also related to the SIP negotiation. The priority order affects the SIP negotiation, which decides on the codec to use.

6. Enable the Clear Channel codec for data transmission by selecting **Enable** in the *Data Transmission* drop-down menu.

   This indicates if the codec can be selected for data transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

   You can also perform this operation in the main *CODEC* section.

7. Set the default priority for data in the *Data Priority* field.

   This sets the priority between different codecs. Codecs with a higher priority are used first, a priority of 0 being the lowest priority. For instance, a codec with priority 3 is used before a codec with priority 2. The maximum priority is 10.

   The Aastra unit uses an internal order for codecs with the same priority.

8. Set the Clear Channel RTP dynamic payload type used in an initial offer in the *Payload Type* field.

   The payload types available are as per RFC 3551. The values range from 96 to 127. The default value is 125.

9. Select the minimum and maximum packetization time values for the codec in the *Minimum Packetization Time* and *Maximum Packetization Time* drop-down menus.

   The packetization time (also called packetization period or ptime) is the duration, in ms, of the voice packet. The range is from 10 ms to 30 ms with increments of 10 ms.

   For the reception, the range is extended from 10 ms to 100 ms with increments of 1 ms only if the stream is not encrypted (SRTP).

10. Click *Submit* if you do not need to set other parameters.

    You can also access the specific parameters of another codec by selecting the codec in the *Select CODEC* drop-down menu at the top of the page.

X-CCD Clear Channel Codec Parameters

The following are the X-CCD Clear Channel codec parameters you can set.

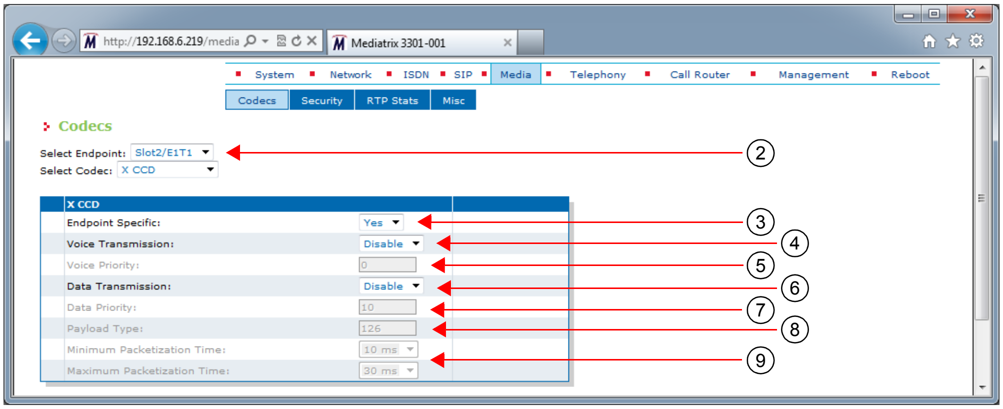
▶ **To set the Clear Channel codec parameters:**

1. In the *CODEC* section of the *CODECS* page, click the Edit button at the right of the X CCD codec to access the codec-specific parameters.

2. Select to which endpoint (interface) you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

   You have the choice between *Default* and the interfaces of your Aastra unit. The number of interfaces available vary depending on the Aastra unit model you have.

Figure 114: X CCD Section



3. Select whether or not you want to override the X CCD parameters set in the *Default* configuration in the *Endpoint Specific* drop-down menu.

This menu is available only in the specific endpoints configuration.

You can also perform this operation in the main *CODEC* section.

4. Enable the X CCD codec for voice transmission by selecting **Enable** in the *Voice Transmission* drop-down menu.

This indicates if the codec can be selected for voice transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

You can also perform this operation in the main *CODEC* section.

5. Set the default priority for voice in the *Voice Priority* field.

This sets the priority between different codecs. Codecs with a higher priority are used first, a priority of 0 being the lowest priority. For instance, a codec with priority 3 is used before a codec with priority 2. The maximum priority is 10.

The Aastra unit uses an internal order for codecs with the same priority.

> **Note:** The codec used is also related to the SIP negotiation. The priority order affects the SIP negotiation, which decides on the codec to use.

6. Enable the X CCD codec for data transmission by selecting **Enable** in the *Data Transmission* drop-down menu.

This indicates if the codec can be selected for data transmission. If enabled, this codec is listed as supported for this specific endpoint. Otherwise, it is ignored.

You can also perform this operation in the main *CODEC* section.

7. Set the default priority for data in the *Data Priority* field.

This sets the priority between different codecs. Codecs with a higher priority are used first, a priority of 0 being the lowest priority. For instance, a codec with priority 3 is used before a codec with priority 2. The maximum priority is 10.

The Aastra unit uses an internal order for codecs with the same priority.

> **Note:** The codec used is also related to the SIP negotiation. The priority order affects the SIP negotiation, which decides on the codec to use.

8. Set the X CCD RTP dynamic payload type used in an initial offer in the *Payload Type* field.

The payload types available are as per RFC 3551. The values range from 96 to 127. The default value is 125.

9. Select the minimum and maximum packetization time values for the codec in the *Minimum Packetization Time* and *Maximum Packetization Time* drop-down menus.

The packetization time (also called packetization period or ptime) is the duration, in ms, of the voice packet. The range is from 10 ms to 30 ms with increments of 10 ms.

10. Click *Submit* if you do not need to set other parameters.

You can also access the specific parameters of another codec by selecting the codec in the *Select CODEC* drop-down menu at the top of the page.

Fax Parameters

The Aastra unit handles G3 fax transmissions at speeds up to 14.4 kbps. Automatic fax mode detection is standard on all endpoints. Real-Time Fax Over UDP with the T.38 protocol stack is also available.

A fax call works much like a regular voice call, with the following differences:

1. The fax codec may be re-negotiated by using a re-INVITE.

2. The goal of the re-INVITE is to allow both user agents to agree on a fax codec, which is either:

a. Clear channel (G.711 or G.726) without Echo Cancellation nor Silence Suppression (automatically disabled).

b. T.38.

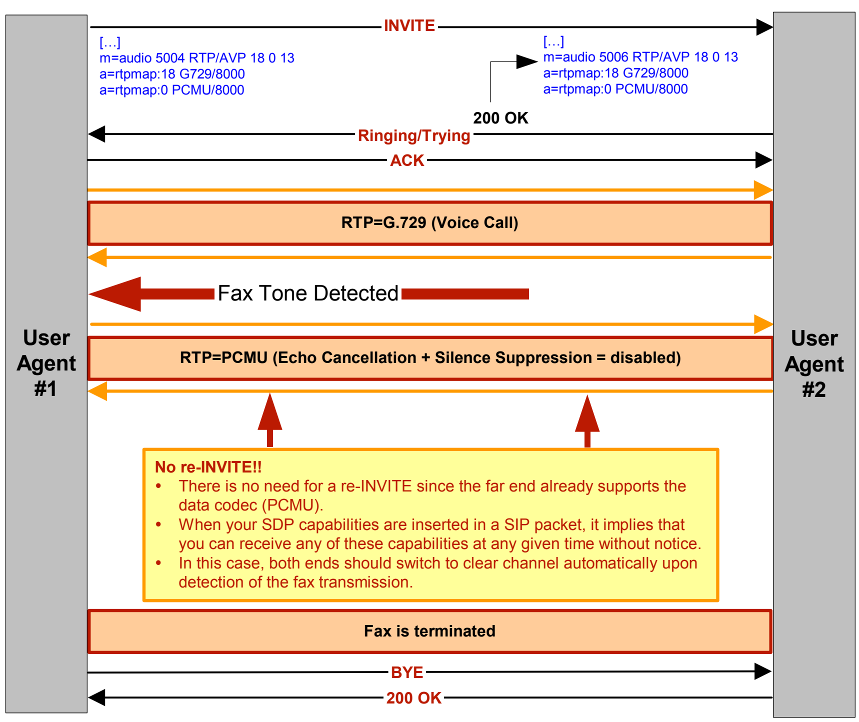
3. Upon fax termination, if the call is not BYE, the previous voice codec is recovered with another re-INVITE.

All endpoints of the Aastra unit can simultaneously use the same codec (for instance, T.38), or a mix of any of the supported codecs. Set and enable these codecs for **each** endpoint.

Clear Channel Fax

The Aastra unit can send faxes in clear channel. The following is a clear channel fax call flow:

Figure 115: Clear Channel Fax Call Flow



DSP Limitation

The Aastra unit currently suffers from a limitation of its DSP. Because of this limitation, the voice does not switch back to the original negotiated codec after a clear channel fax is performed.

The Aastra unit cannot detect the end of a clear channel fax, which means that the unit cannot switch back to the original negotiated codec if this codec was not a clear channel codec, e.g., a session established in G.729.

When the unit detects a fax, it automatically switches to a negotiated clear channel codec such as PCMU (if there is no T.38 or if T.38 negotiation failed). Once the fax is terminated, the Aastra unit is not notified by the DSP. The unit thus stays in the clear channel codec and does not switch back to G.729.

T.38 Fax

The Aastra unit can send faxes in T.38 mode over UDP. T.38 is used for fax if both units are T.38 capable; otherwise, transmission in clear channel over G.711 as defined is used (if *G.711 μ-law* and/or *G.711 A-law* are enabled). If no clear channel codecs are enabled and the other endpoint is not T.38 capable, the fax transmission fails.

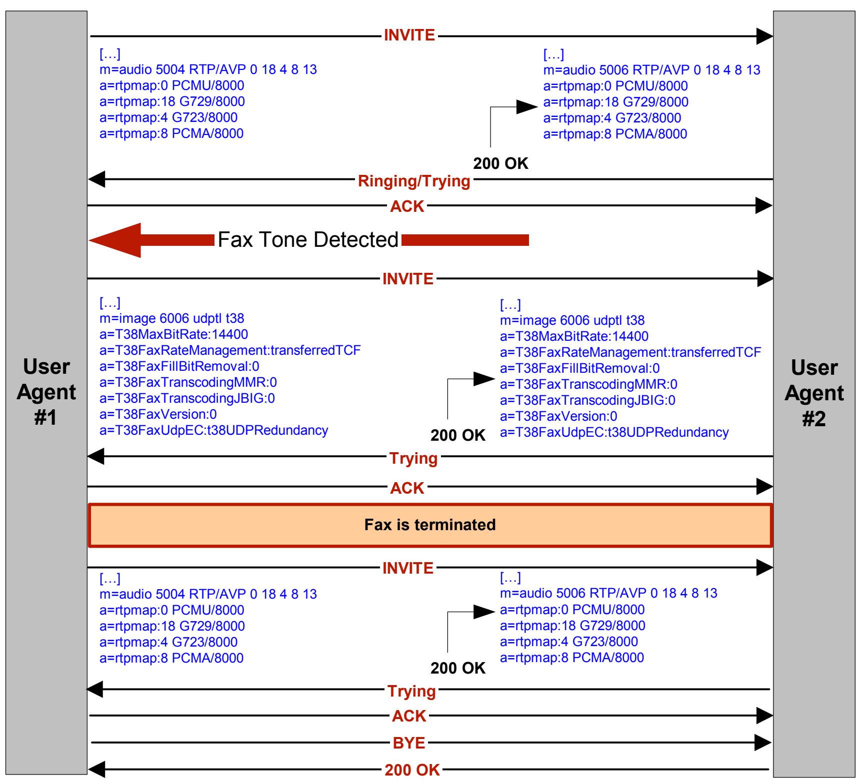
Caution: The Aastra unit opens the T.38 channel only after receiving the “200 OK” message from the peer. This means that the Aastra unit cannot receive T.38 packets before receiving the “200 OK”. Based on RFC 3264, the T.38 channel should be opened as soon as the unit sends the “INVITE” message.

The quality of T.38 fax transmissions depends upon the system configuration, type of call control system used, type of Aastra units deployed, as well as the model of fax machines used. Should some of these conditions be unsatisfactory, performance of T.38 fax transmissions may vary and be reduced below expectations.

Note: Aastra recommends not to use a fax that does not send a CNG tone. If you use such a fax to send a fax communication to the public network, this might result in a communication failure.

The following is a T.38 fax call flow:

Figure 116: T.38 Fax Call Flow



T.38 Parameters Configuration

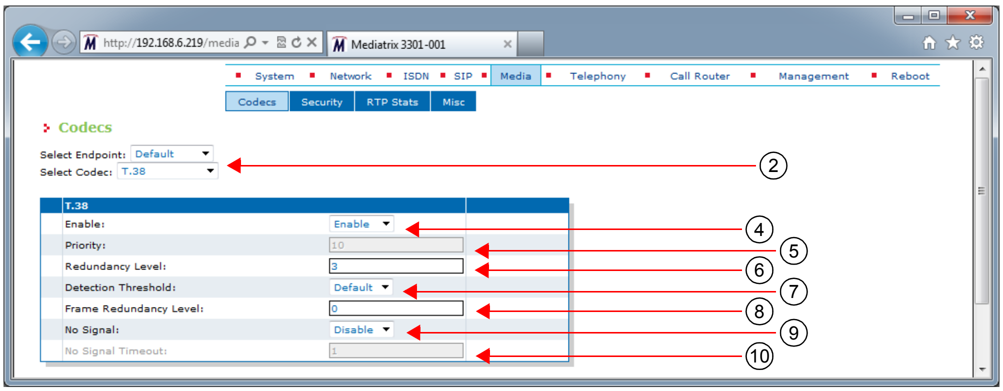
The following are the T.38 codec parameters you can set.

▶ **To set the T.38 codec parameters:**

1. In the *CODEC* section of the *CODECS* page, click the Edit button at the right of the corresponding G.726 codec to access the codec-specific parameters.
2. Select to which endpoint (interface) you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

   You have the choice between *Default* and the interfaces of your Aastra unit. The number of interfaces available vary depending on the Aastra unit model you have.

Figure 117: T.38 Section



3. In the *T.38* section, select whether or not you want to override the T.38 parameters set in the *Default* configuration in the *Use Endpoint Specific* drop-down menu.

   This menu is available only in the specific endpoints configuration.

   You can also perform this operation in the main *CODEC* section.
4. Enable the T.38 codec by selecting **Enable** in the *Enable* drop-down menu.

   You can also perform this operation in the main *CODEC* section.
5. Set the default priority for fax in the *Priority* field.

   This sets the priority between different codecs. Codecs with a higher priority are used first, a priority of 0 being the lowest priority. For instance, a codec with priority 3 is used before a codec with priority 2. The maximum priority is 10.

   The Aastra unit uses an internal order for codecs with the same priority.

Note: Currently, the only T.38 priority accepted is **10**. Priority between 1 and 9 is refused.

6. Set the number of redundancy packets sent with the current packet in the *Redundancy Level* field.

   This is the standard redundancy offered by T.38. Available values range from 1 to 5. Please see step ***7*** for additional reliability options for T.38.
7. Set the T.38 input signal detection threshold in the *Detection Threshold* drop-down menu.

   Lowering the threshold allows detecting lower amplitude fax signals. The following values are available:

   - Default: (-26 dB)
   - Low: (-31 dB)
   - Lowest: (-43 dB)

8. For additional reliability, define the number of times T.38 packets are retransmitted in the *Frame Redundancy Level* field.

   This field is available only in the default endpoint configuration.

   This only applies to the T.38 packets where the PrimaryUDPTL contains the following T.38 data type:

   - HDLC_SIG_END,
   - HDLC_FCS_OK_SIG_END,
   - HDLC_FCS_BAD_SIG_END and
   - T4_NON_ECM_SIG_END

9. Define whether or not the Aastra unit sends no-signal packets during a T.38 fax transmission in the *No Signal* drop-down menu.

   This menu is available only in the default endpoint configuration.

   When enabled, the unit ensures that, during a T.38 fax transmission, data is sent out at least every time the *No Signal Timeout* delay expires. The Aastra unit sends no-signal packets if no meaningful data have been sent for a user-specified period of time.

10. Set the period, in seconds, at which no-signal packets are sent during a T.38 transmission in the *No Signal Timeout* field.

    This field is available only in the default endpoint configuration.

    No-signal packets are sent out if there are no valid data to send.

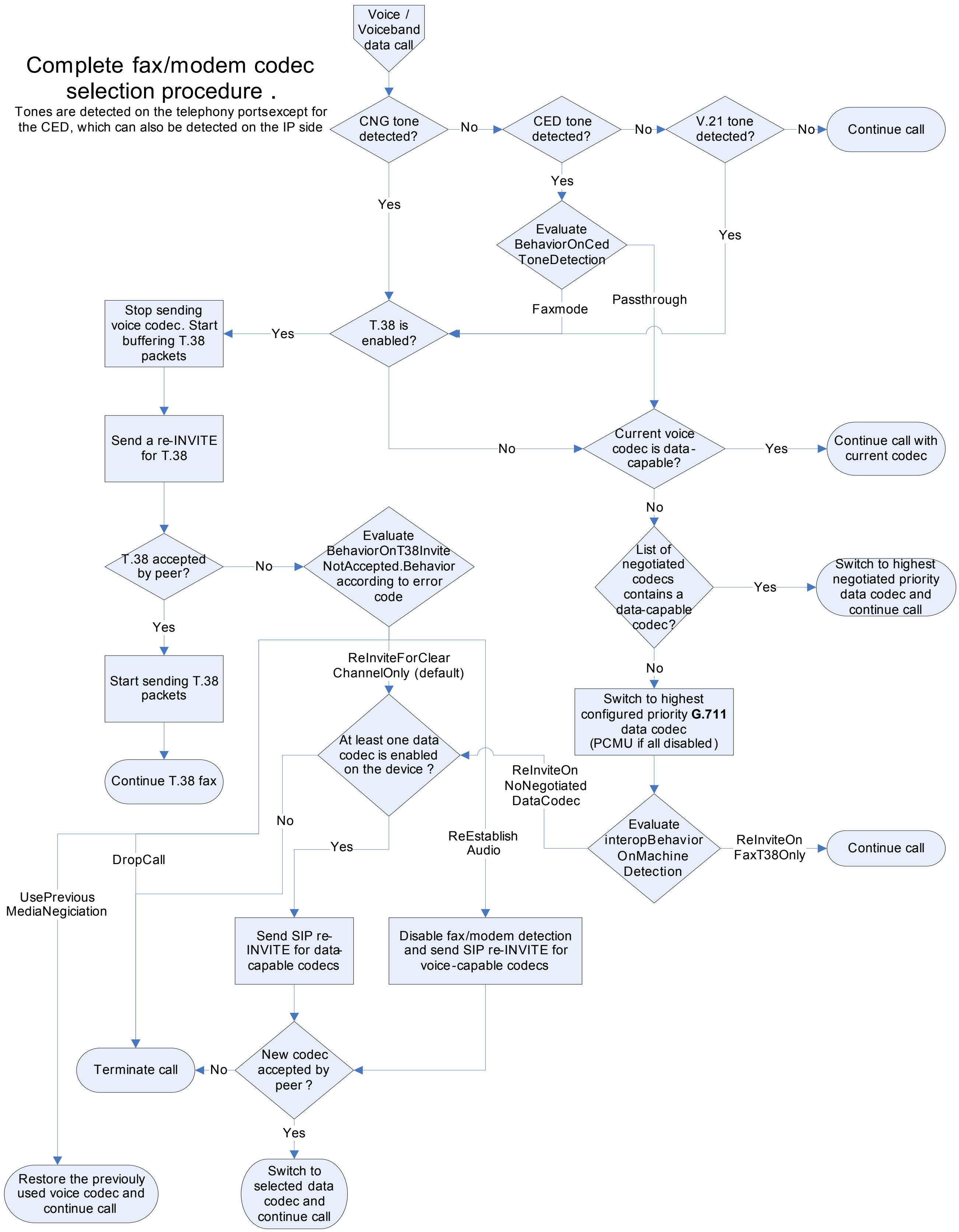
11. Click *Submit* if you do not need to set other parameters.

    You can also access the specific parameters of another codec by selecting the codec in the *Select CODEC* drop-down menu at the top of the page.

Data Codec Selection Procedure

The Aastra unit follows a procedure when selecting data codec. This procedure is the default behaviour of the Aastra unit. Some interop variables may modify this procedure. Tones are detected on the analog ports only.

Figure 118: Data Codec Selection Procedure



CHAPTER

29

Security

This chapter describes how to properly configure the security parameters of the Aastra unit.

Standards Supported	• RFC 3711: The Secure Real-time Transport Protocol (SRTP) (Supports only the AES-CM encryption) • RFC 3830: MIKEY: Multimedia Internet KEYing (Compliant for method Pre-Shared Key only) • RFC 4567: Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP) • RFC 4568: SDES: Security Descriptions for Media Streams

Introduction

You can define security features on the Aastra unit. This section applies to media security parameters. Applying security on the Aastra unit involves several steps:

- Properly set the time on the Aastra unit by configuring a valid SNTP server (“SNTP Configuration” on page 93) and time zone (“Time Configuration” on page 94).
- Transfer a valid CA certificate into the Aastra unit (“Chapter 46 - Certificates Management” on page 557).
- Use secure signalling by enabling the TLS transport protocol (“Chapter 28 - SIP Transport Parameters” on page 305).

Caution: If you enable Secure RTP (SRTP) on at least one line, it is acceptable to have the secure SIP transport (TLS) disabled for testing purposes. However, you must never use this configuration in a production environment, since an attacker could easily break it. Enabling TLS for SIP Transport is strongly recommended and is usually mandatory for security interoperability with third-party equipments.

Caution: When using a codec other than G.711, enabling Secure RTP (SRTP) has an impact on the Aastra unit’s overall performance as SRTP requires CPU power. The more lines use SRTP, the more overall performance is affected. See also “DSP Limitation” on page 429 for more details on resources limitations with SRTP and conferences.

- Use secure media by:
  - Defining the SRTP/ SRTCP base port (“Base Ports Configuration” on page 397).
  - Setting the RTP secure mode to “Secure” or “Secure with fallback” (this section).

Security Parameters

The *Security* section allows you to secure the RTP stream (media) of the Aastra unit.

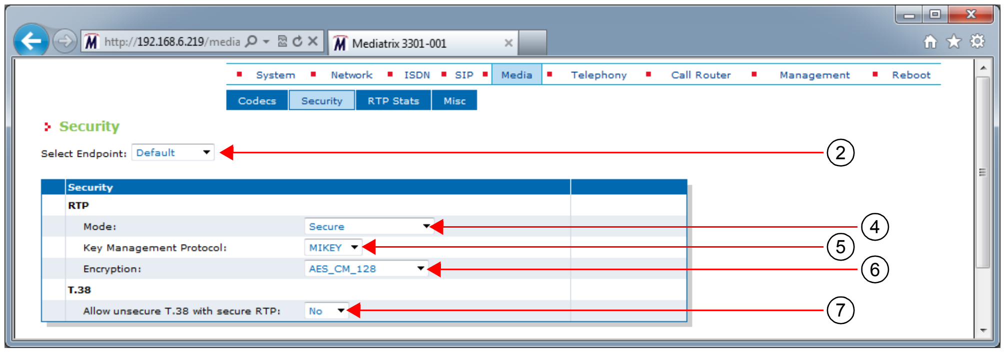
Since the SRTP encryption and authentication needs more processing, the number of calls that the Aastra unit can handle simultaneously may be reduced, depending of the codecs enabled. You could set the Aastra unit not to impact the number of simultaneous calls by enabling only G.711 codecs and disabling every other voice or data codec, even T.38.

The Aastra unit supports the MIKEY protocol using pre-shared keys (MIKEY-PS) or the SDES protocol for negotiating SRTP keys.

▶ **To set the RTP stream security parameters:**

1. In the web interface, click the *Media* link, then the *Security* sub-link.

Figure 119: Media – Security Web Page



2. Select to which endpoint (interface) you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

You have the choice between *Default* and the interfaces of your Aastra unit. The number of interfaces available vary depending on the Aastra unit model you have.

3. Select whether or not you want to override one or more of the available default security parameters in the *Endpoint Specific* drop-down menu.

This menu is available only in the specific endpoints configuration.

4. In the *Security* section of the *Security* page, select the RTP payload mode in the *Mode* drop-down menu.

The unit relies on these modes when negotiating an audio stream.

Table 200: Default RTP Mode

Mode	Description
Unsecure	The Aastra unit supports only unsecure RTP. It rejects secure RTP offers it receives.
Secure	The Aastra unit supports only secure RTP. It rejects unsecure RTP offers it receives.
Secure with fallback	The Aastra unit supports both secure and unsecure RTP. It prioritizes secure RTP but permits unsecure RTP fallback when the remote peer does not support security.

The TLS SIP transport must usually be enabled for secure audio negotiation via SDP (refer to the Caution box above). See “Chapter 28 - SIP Transport Parameters” on page 305 for more details.

The RTP mode is reflected in the SIP/SDP payload, with a RTP/AVP for unsecure RTP, and a RTP/SAVP for secure RTP.

The following basic rules apply when sending units capabilities via SDP:

- When the RTP mode is set to *Unsecure*, the Aastra unit offers/answers with only one active RTP/AVP audio stream. Any other audio stream present in the offer is disabled in the answer.
- When the RTP mode is set to *Secure*, the Aastra unit offers/answers with only one active RTP/SAVP audio stream. Any other audio stream present in the offer is disabled in the answer.

- When the RTP mode is set to *Secure with fallback*, the Aastra unit offers one RTP/AVP and one RTP/SAVP audio streams. The unit answers with only the most secure stream.
- If the remote unit answers to an offer with both RTP/AVP and RTP/SAVP streams enabled, a new offer is sent with only RTP/SAVP enabled.

5. Select the key management protocol for SRTP in the *Key Management* drop-down menu.

Table 201: Key Management Protocol

Protocol	Description
Mikey	Use MIKEY (Multimedia Internet KEYing).
Sdes	Use SDES (Security DEScriptions).

This parameter has no effect if the *Mode* parameter is set to **Unsecure**.

If the unit receives an offer with both MIKEY and SDES, only the configured key management protocol is kept.

6. Select the encryption type to be used with SRTP in the *Encryption* drop-down menu.

Table 202: Default RTP Mode

Encryption	Description
Null	No encryption. It is ignored for the **Sdes** Key Management as defined in Step 3. Use only for debug.
AesCm128	AES (Advanced Encryption Standard) Counter Mode 128 bits.

This parameter has no effect if the *Mode* parameter is set to **Unsecure**.

7. Select whether or not to enable T.38 even if the call has been established previously in SRTP in the *Allow Unsecure T.38 with Secure RTP* drop-down menu.

Table 203: Default RTP Mode

Mode	Description
Disable	T.38 is disabled for SRTP calls.
Enable	T.38 is enabled for SRTP calls. **Caution:** Enabling this parameter opens a security hole, because T.38 is an unsecure protocol.

This menu is available only in the default configuration.

Note that this parameter has no effect if the *Mode* parameter is set to **Unsecure**.

8. Click *Submit* if you do not need to set other parameters.

Enforcing Symmetric RTP

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

For each bi-directional RTP streams, you can define whether or not to enforce that incoming RTP packets are from the same source as the destination of outgoing RTP packets.

Enforcing symmetric RTP may prevent legitimate RTP streams coming from a media server from being processed, for example: Music and conferencing servers.

The following parameters are available:

Table 204: Enforce Symmetric RTP Parameters

Parameter	Description
disable	Accept packets from all sources. This is the default value.
enable	Silently discard incoming RTP packets with source address and port differing from the destination address and port of outgoing packets.

▶ **To enforce symmetric RTP:**

1. In the mipt*MIB*, set the `enforceSymmetricRtpEnable` variable with the proper behaviour.

   You can also use the following line in the CLI or a configuration script:

   `mipt.enforceSymmetricRtpEnable="Value"`

   where *Value* may be as follows:

Figure 120: Symmetric RTP Values

Value	Meaning
0	disable
1	enable

CHAPTER

30

RTP Statistics Configuration

The Aastra unit collects meaningful statistics that can be read via the web interface. This chapter describes how to read and configure the RTP statistics.

Note that the RTP statistics are also available via SNMP and CLI.

Statistics Displayed

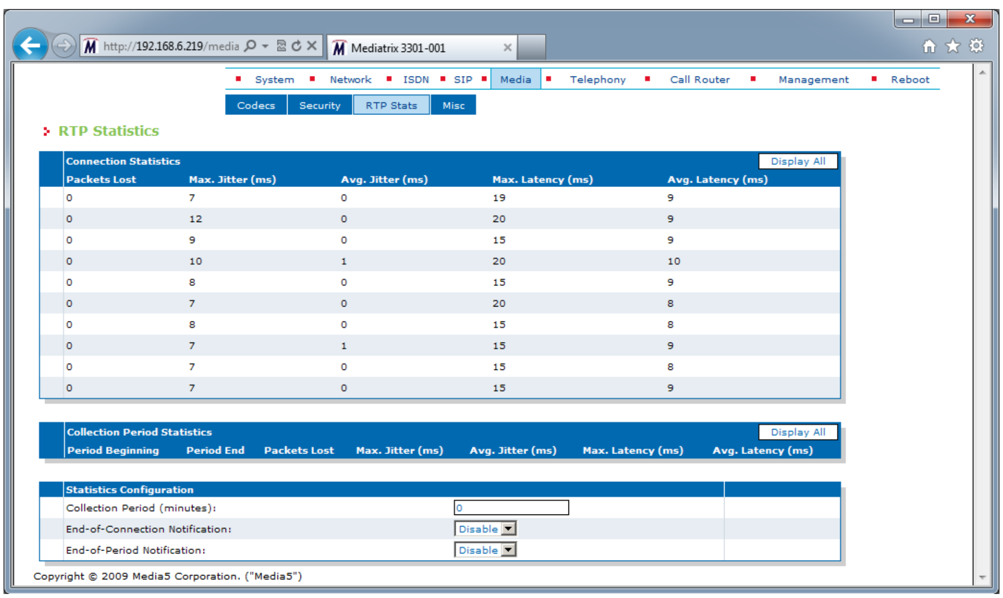
The Aastra unit collects two types of statistics:

- statistics for the last 10 connections
- statistics for the last 10 collection periods

The *Connection Statistics* section displays the statistics for the last 10 connections. You can use the *Display All* button to display more information or the *Display Overview* button to display less information.

The *Connection Period Statistics* section displays the statistics for the last 10 periods. The period duration is defined in the *Statistics Configuration* section. You can use the *Display All* button to display more information or the *Display Overview* button to display less information.

Figure 121: Telephony – RTP Stats Web Page



The following table describes the statistics available.

Table 205: Statistics Displayed

Statistic	Connection Statistics	Collection Period Statistics
Octets Tx	Number of octets transmitted during the connection.	Number of octets transmitted during the collection period. This value is obtained by cumulating the octets transmitted in all connections that were active during the collection period.

Table 205: Statistics Displayed (Continued)

Statistic	Connection Statistics	Collection Period Statistics
Octets Rx	Number of octets received during the connection.	Number of octets received during the collection period. This value is obtained by cumulating the octets received in all connections that were active during the collection period.
Packets Tx	Number of packets transmitted during the connection.	Number of packets transmitted during the collection period. This value is obtained by cumulating the packets transmitted in all connections that were active during the collection period.
Packets Rx	Number of packets received during the connection.	Number of packets received during the collection period. This value is obtained by cumulating the packets received in all connections that were active during the collection period.
Packets Lost	Number of packets lost during the connection. This value is obtained by substracting the expected number of packets based on the sequence number from the number of packets received.	Number of packets lost during the collection period. This value is obtained by cumulating the packets lost in all connections that were active during the collection period.
Min. Jitter	Minimum interarrival time, in ms, during the connection. All RTP packets belonging to the connection and received at the RTP level are considered in the calculation.	Minimum interarrival time, in ms, during the collection period. This value is the lowest interarrival jitter for all connections that were active during the collection period.
Max. Jitter	Maximum interarrival time, in ms, during the connection. All RTP packets belonging to the connection and received at the RTP level are considered in the calculation.	Maximum interarrival time, in ms, during the collection period. This value is the highest interarrival jitter for all connections that were active during the collection period.
Avg. Jitter	Average interarrival time, in ms, during the connection. All RTP packets belonging to the connection and received at the RTP level are considered in the calculation.	Average interarrival time, in ms, during the collection period. This value is the weighted average of the interarrival jitter for all connections that were active during the collection period. For each connection, the total jitter of packets received during the collection period and the total number of packets received during the collection period are used in the weighted average calculation.
Min. Latency	Minimum latency, in ms, during the connection. The latency value is computed as one half of the round-trip time, as measured through RTCP.	Minimum latency, in ms, during the collection period. This value is the lowest latency for all connections that were active during the collection period.
Max. Latency	Maximum latency, in ms, during the connection. The latency value is computed as one half of the round-trip time, as measured through RTCP.	Maximum latency, in ms, during the collection period. This value is the highest latency for all connections that were active during the collection period.

Table 205: Statistics Displayed (Continued)

Statistic	Connection Statistics	Collection Period Statistics
Avg. Latency	Average latency, in ms, during the connection. The latency value is computed as one half of the round-trip time, as measured through RTCP.	Average latency, in ms, during the collection period. This value is the weighted average of the latency for all connections that were active during the collection period. For each connection, the total latency of packets received during the collection period and the total number of packets received during the collection period are used in the weighted average calculation.

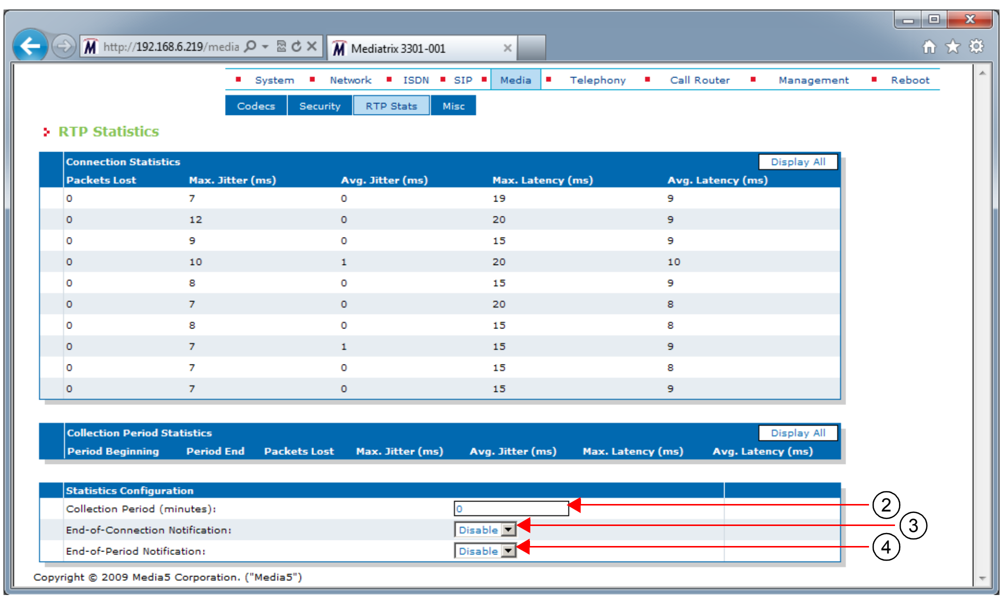
Statistics Configuration

You can define how to collect the statistics. The statistics are sent as syslog messages, so you must properly set the syslog information before setting the statistics. You must set the *Media IP Transport (MIPT)* service to the **Info** or **Debug** level. See "Syslog Daemon Configuration" on page 71 for more details on how to configure the Syslog.

▶ **To configure how to collect statistics:**

1. In the web interface, click the *Telephony* link, then the *RTP Stats* sub-link.

Figure 122: Telephony – RTP stats Web Page



2. Set the *Collection Period* field with the collection period duration in minutes.

   Putting a value of **0** disables the collection period statistics feature.

3. Set the *End-of-Connection Notification* drop-down menu with the proper behaviour.

Table 206: End-of-Connection Notification

Parameter	Description
Enable	Notifications are generated.
Disable	Notifications are not generated.

4. Set the *End-of-Period Notification* drop-down menu with the proper behaviour.

Table 207: End-of-Period Notification

Parameter	Description
Enable	Notifications are generated.
Disable	Notifications are not generated.

5. If you do not need to set other parameters, do one of the following:

- To save your settings, click *Submit*.
- To save your settings and reset the statistics of the current period., click *Submit & Reset Current Collection Period Statistics*.

  The previous periods are left unchanged.

Channel Statistics

This section describes how to access data available only in the MIB parameters of the Aastra unit. You can display these parameters as follows:

- by using a MIB browser
- by using the CLI

The channel statistics are cumulated RTP statistics for all calls using a specific channel of a telephony interface. Statistics are updated at the end of each call.

The statistics are associated to the channel in use at the end of the call. In some cases, such as in hold/resume scenarios, the channel assignment may change during a call. This can result in discrepancies between the RTP statistics and the actual usage of the telephony interface.

The following are the channel statistics the Aastra unit keeps.

Table 208: Channel Statistics

MIB Variable	Statistics Description
PacketsSent	Number of packets transmitted on the channel since service start. This value is obtained by cumulating the packets transmitted in all the connections that ended during the collection period.
PacketsReceived	Number of packets received on the channel since service start. This value is obtained by cumulating the packets received in all the connections that ended during the collection period.
BytesSent	Number of bytes transmitted on the channel since service start. This value is obtained by cumulating the bytes transmitted in all the connections that ended during the collection period.
BytesReceived	Number of bytes received on the channel since service start. This value is obtained by cumulating the bytes received in all the connections that ended during the collection period.
AverageReceiveInterarrivalJitter	Average interarrival time, in microseconds, for the channel since service start. This value is based on the average interarrival jitter of each call ended during the collection period. The value is weighted by the duration of the calls.

▶ To display channel statistics:

1. In the *miptMIB*, go to the *ChannelStatistics* table.

You can also use the following line in the CLI:

```
get mipt.channelStatistics
```

▶ To reset channel statistics values to zero:

1. In the *miptMIB*, set `ChannelStatistics.Reset` to *Reset* for the endpoint to reset.

You can also use the following line in the CLI:

```
set mipt.channelStatistics.Reset=Reset
```

2. In the *miptMIB*, set `ChannelStatistics[EpChannelId=channelStatisticsEpChannelId].Reset` to *Reset* to reset only one specific endpoint.

where:

- `channelStatisticsEpChannelId` is the string that identifies the combination of an endpoint and a channel. The endpoint name is the same as the `EpId` used to refer to endpoints in other tables. On endpoints with multiple channels, the channel number must be appended at the end of the endpoint name, separated with a dash.

You can also use the following line in the CLI:

```
set mipt.channelStatistics[EpChannelId=channelStatisticsEpChannelId].Reset=Reset
```

Examples:

`Slot3/E1T1-12` refers to endpoint Slot3/E1T1, channel 12.

`Phone-Fax1` refers to FXS endpoint Phone-Fax1 on a 4102s.

`Port06` refers to FXS endpoint Port06 on 4108/4116/4124.

No channel number is appended to FXS endpoint strings because FXS lines do not support multiple channels.

CHAPTER
31 Miscellaneous Media Parameters

This chapter describes how to configure parameters that apply to all codecs.

Standards Supported	• draft-choudhuri-sip-info-digit-00.txt

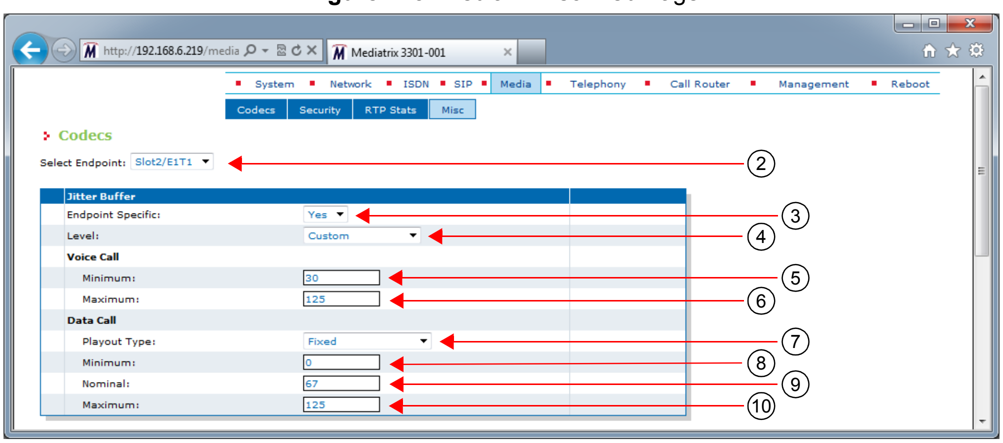
Jitter Buffer Configuration

The *Jitter Buffer* section allows you to configure parameters to reduce jitter buffer issues.

▶ **To set the jitter buffer parameters:**

1. In the web interface, click the *Media* link, then the *Misc* sub-link.

Figure 123: Media – Misc Web Page



2. Select to which endpoint (interface) you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

You have the choice between *Default* and the interfaces of your Aastra unit. The number of interfaces available vary depending on the Aastra unit model you have.

3. In the *Jitter Buffer* section, if you have selected a specific endpoint, select whether or not you want to override the jitter buffer parameters set in the *Default* configuration in the *Endpoint Specific* drop-down menu.

This menu is available only in the specific endpoints configuration.

4. Select the jitter buffer level in the *Level* drop-down menu.

Jitter is an abrupt and unwanted variation of one or more signal characteristics, such as the interval between successive pulses or the frequency or phase of successive cycles. An adaptive jitter buffer usually consists of an elastic buffer in which the signal is temporarily stored and then retransmitted at a rate based on the average rate of the incoming signal.

Table 209: Jitter Buffer Levels

Level	Description
Optimize Latency	The jitter buffer is set to the lowest effective value to minimize the latency. Voice cut can be heard if the network is not optimal. The predefined values are as follows: • Minimum value: 10 ms • Maximum value: 40 ms
Normal	The jitter buffer tries to find a good compromise between the latency and the voice quality. This setting is recommended in private networks. The predefined values are as follows: • Minimum value: 30 ms • Maximum value: 90 ms
Optimize Quality	The jitter buffer is set to a high value to minimize the voice cuts at the cost of high latency. This setting is recommended in public networks. The predefined values are as follows: • Minimum value: 50 ms • Maximum value: 125 ms
Fax / Modem	The jitter buffer is set to maximum. The Fax/Modem transmission is very sensitive to voice cuts but not to latency, so the fax has a better chance of success with a high buffer. The predefined values are as follows: • Minimum value: 70 ms • Maximum value: 135 ms
Custom	The jitter buffer uses the configuration of the *Minimum* and *Maximum* variables (Steps 4 and 5).

5. If you have selected the **Custom** level, define the target jitter buffer length in the *Minimum* field of the *Voice Call* part.

   The adaptive jitter buffer attempts to hold packets to the minimal holding time. This is the minimal delay the jitter buffer adds to the system. The minimal jitter buffer is in ms and must be equal to or smaller than the maximal jitter buffer.

   Values range from 0 ms to 135 ms. The default value is 30 ms. You can change values by increments of 1 ms, but Aastra recommends to use multiples of 5 ms. The minimal jitter buffer should be a multiple of ptime.

   It is best not to set the minimal jitter value below the default value. Setting a minimal jitter buffer below 5 ms could cause an error. Jitter buffer adaptation behaviour varies from one codec to another. See "About Changing Jitter Buffer Values" on page 265 for more details.

6. If you have selected the **Custom** level, define the maximum jitter buffer length in the *Maximum* field of the *Voice Call* part.

   This is the highest delay the jitter buffer is allowed to introduce. The jitter buffer length is in ms and must be equal to or greater than the minimum jitter buffer.

   Values range from 0 ms to 135 ms. The default value is 125 ms. You can change values by increments of 1 ms, but Aastra recommends to use multiples of 5 ms. The maximal jitter buffer should be a multiple of ptime.

   The maximum jitter buffer value should be equal to the minimum jitter buffer value + 4 times the ptime value. Let's say for instance that:

   - Minimum jitter buffer value is 30 ms

- Ptime value is 20 ms

  The maximum jitter buffer value should be: 30 + 4x20 = 110 ms

7. If you have selected the **Custom** level, define the voiceband data custom jitter buffer type in the *Playout Type* drop-down menu of the *Data Call* part.

This is the algorithm to use for managing the jitter buffer during a call. The *Nominal* field value serves as the delay at the beginning of the call and might be adapted afterwards based on the selected algorithm.

Table 210: Voiceband Data Custom Jitter Buffer Type

Level	Description
Adaptive Immediately	The nominal delay varies based on the estimated packet jitter. Playout adjustment is done immediately when the actual delay goes out of bounds of a small window around the moving nominal delay.
Adaptive Silence	The nominal delay varies based on the estimated packet jitter. Playout adjustment is done based on the actual delay going out of bounds of a small window around the moving nominal delay. The adjustment is deferred until silence is detected (either from playout buffer underflow or by analysis of packet content). Playout adjustment is also done when overflow or underflow events occur.
Fixed	The nominal delay is fixed to the value of the *Nominal* field value and does not change thereafter. Playout adjustment is done when overflow or underflow events occur.

8. If you have selected the **Custom** level, define the voiceband data jitter buffer minimal length (in milliseconds) in the Minimum field of the *Data Call* part.

The voiceband data jitter buffer minimal length is the delay the jitter buffer tries to maintain. The minimal jitter buffer MUST be equal to or smaller than the voiceband data maximal jitter buffer.

The minimal jitter buffer should be a multiple of ptime.

This value is not available when the *Playout Type* drop-down menu is set to **Fixed**.

9. If you have selected the **Custom** level, define the voiceband data custom jitter buffer nominal length in the *Nominal* field of the *Data Call* part.

The jitter buffer nominal length (in milliseconds) is the delay the jitter buffer uses when a call begins. The delay then varies depending on the type of jitter buffer.

In adaptive mode, the nominal jitter buffer should be equal to (voice band data minimal jitter buffer + voice band data maximal jitter buffer) / 2.

10. If you have selected the **Custom** level, define the default voiceband data custom jitter buffer maximal length in the *Maximum* field of the *Data Call* part.

The jitter buffer maximal length (in milliseconds) is the highest delay the jitter buffer is allowed to introduce. The maximal jitter buffer MUST be equal to or greater than the minimal jitter buffer.

The maximal jitter buffer should be a multiple of ptime.

The maximal jitter buffer should be equal to or greater than voiceband data minimal jitter buffer + (4 * ptime) in adaptive mode.

See "About Changing Jitter Buffer Values" on page 265 for more details.

11. Click *Submit* if you do not need to set other parameters.

About Changing Jitter Buffer Values

Aastra recommends to avoid changing the target and maximum jitter buffer values unless experiencing or strongly expecting one of the following symptoms:

- If the voice is scattered, try to increase the maximum jitter buffer value.
- If the delay in the voice path (end to end) is too long, you can lower the target jitter value, but

ONLY if the end-to-end delay measured matches the target jitter value.

For instance, if the target jitter value is 50 ms, the maximum jitter is 300 ms and the delay measured is 260 ms, it would serve nothing to reduce the target jitter. However, if the target jitter value is 100 ms and the measured delay is between 100 ms and 110 ms, then you can lower the target jitter from 100 ms to 30 ms.

Starting a Call in Voiceband Data Mode

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

You can define whether or not a call should be started in voiceband data mode.

The following values are available:

Table 211: Voiceband Data Mode Parameters

Parameter	Description
Disable	The call is started in voice mode. A fax/modem tone detection triggers a transition from voice to voiceband data according to the configuration in the Machine Detection Group (“Miscellaneous Media Parameters” on page 263).
Enable	The call is started in voiceband data mode.

▶ **To start a call in voiceband data mode:**

1. In the *telIfMIB*, set the voiceband data mode in the `InteropStartCallInVbdEnable` variable.

   You can also use the following line in the CLI or a configuration script:

   `telIf.InteropStartCallInVbdEnable="Value"`

   where *Value* may be as follows:

Table 212: Voiceband Data Mode Values

Value	Method
0	Disable
1	Enable

DTMF Transport Configuration

The DTMF Transport section allows you to set the DTMF transport parameters of the Aastra unit.

▶ **To set DTMF transport parameters:**

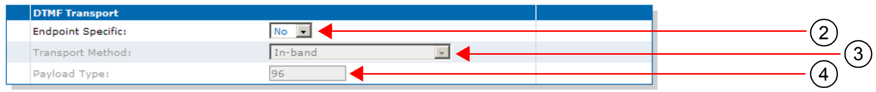
1. Select to which endpoint (interface) you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

   You have the choice between *Default* and the interfaces of your Aastra unit. The number of interfaces available vary depending on the Aastra unit model you have.

2. In the *DTMF Transport* section of the *Misc* page, select whether or not you want to override the DTMF transport parameters set in the *Default* configuration in the *Endpoint Specific* drop-down menu.

   This menu is available only in the specific endpoints configuration.

Figure 124: DTMF Transport Section



3. Select the DTMF transport type in the *Transport Method* drop-down menu.

The following choices are available:

Table 213: DTMF Transport Type Parameters

Transport Parameter	Description
In-band	The DTMFs are transmitted like the voice in the RTP stream.
Out-of-band using RTP	The DTMFs are transmitted as per RFC 2833. This parameter also works with SRTP.
Out-of-band using SIP	The DTMFs are transmitted as per *draft-choudhuri-sip-info-digit-00*.
Signaling protocol Dependant	The signalling protocol has the control to select the DTMF transport mode. The SDP body includes both RFC 2833 and *draft-choudhuri-sip-info-digit-00* in that order of preference.

4. If you have selected the **Out-of-band using SIP** transport method, select the method used to transport DTMFs out-of-band over the SIP protocol in the *SIP Transport Method* drop-down menu.

This menu is available only in the default endpoint configuration.

Table 214: DTMF Out-of-Band Transport Methods

Method	Description
draftChoudhuriSipInfoDigit00	Transmits DTMFs by using the method defined in *draft-choudhuri-sip-info-digit-00*. Only the unsolicited-digit part is supported.

DTMF out-of-band

Certain compression codecs such as G.723.1 and G.729 effectively distort voice because they lose information from the incoming voice stream during the compression and decompression phases. For normal speech this is insignificant and becomes unimportant. In the case of pure tones (such as DTMF) this distortion means the receiver may no longer recognize the tones. The solution is to send this information as a separate packet to the other endpoint, which then plays the DTMF sequence back by re-generating the true tones. Such a mechanism is known as out-of-band DTMF. The Aastra unit receives and sends out-of-band DTMFs as per ITU Q.24. DTMFs supported are 0-9, A-D, *, #.

Table 214: DTMF Out-of-Band Transport Methods (Continued)

Method	Description

Info DTMF Relay	Transmits DTMFs by using a custom method. This custom method requires no SDP negotiation and assumes that the other peer uses the same method.
	It uses a SIP INFO message with a content of type *application/ dtmf-relay*. The body of the message contains the DTMF transmitted and the duration of the DTMF:
	`Signal= 1`
	`Duration= 160`
	When transmitting, the duration is the one set in the `interopDtmfTransportDuration` variable (see "DTMF Transport over the SIP Protocol" on page 268).
	When receiving, the duration of the DTMF received is not used and the DTMF is played for 100 ms.
	DTMFs are transmitted one at a time.
	Available digits are "0123456789ABCD*#". The Aastra unit also supports the ",;p" characters when receiving DTMFs.

5. If you have selected the **Out-of-band using RTP** transport method, set the payload type in the *Payload Type* field.

   You can determine the actual RTP dynamic payload type used for the "telephone-event" in an initial offer. The payload types available are as per RFC 1890. Available values range from 96 to 127.

6. Click *Submit* if you do not need to set other parameters.

DTMF Transport over the SIP Protocol

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

You can set the DTMF duration sent in the INFO message when using the **Info DTMF Relay** method to transmit DTMFs (see "Miscellaneous Media Parameters" on page 263, Step 8 for more details).

To set the DTMF duration sent in the INFO message:

1. In the *sipEpMIB*, set the DTMF duration sent in the INFO message when using the **infoDtmfRelay** method to transmit DTMFs in the `interopDtmfTransportDuration` variable.

   You can also use the following line in the CLI or a configuration script:

   ```
   sipEp.interopDtmfTransportDuration="Value"
   ```

   This value is expressed in milliseconds (ms). The default value is **100** ms.

DTMF Detection

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

The default DTMF detection parameters of the Aastra unit may sometimes not be enough to properly detect the DTMFs. This section describes how to set additional DTMF detection parameters.

DTMF Frequencies

The DTMF keypad is laid out in a 4x4 matrix, with each row representing a low frequency, and each column representing a high frequency. For example, pressing a single key (such as '1') sends a sinusoidal tone of the two frequencies (697 Hz and 1209 Hz). When the unit is configured to send DTMFs out-of-band, its DSP detects these DTMFs, removes them from the RTP stream, and sends them out-of-band.

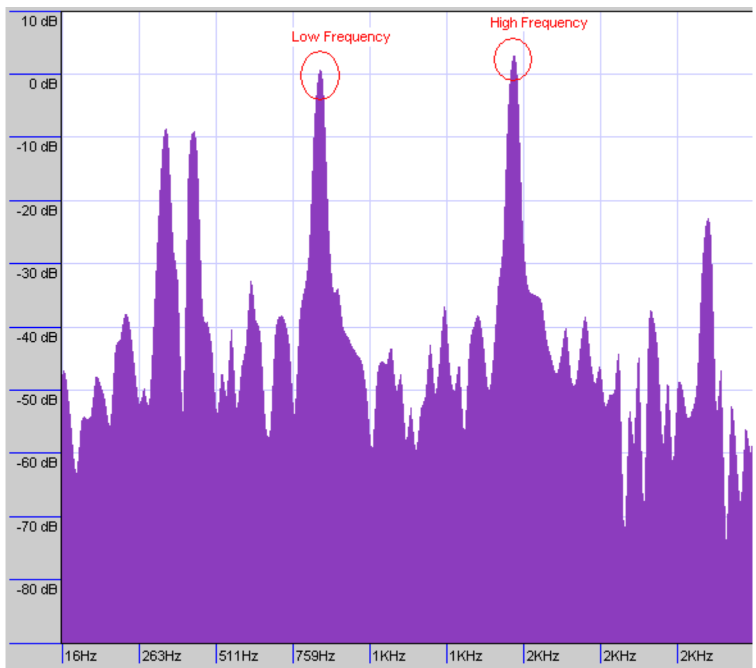
Table 215: DTMF Keypad Frequencies

Low/High (Hz)	1209	1336	1477	1633
697	1	2	3	A
770	4	5	6	B
852	7	8	9	C
941	*	0	#	D

DTMF Detection Configuration

Below is a frequency spectrum analysis of a DTMF (9) with the Frequency in Hertz on the x axis and the Power in dBm on the y axis. The low and high frequencies of the DTMF are in red and you can clearly see that they are the most powerful frequencies in the signal.

Figure 125: DTMF Detection Example



▶ **To configure the DTMF detection:**

1. In the *tellfMIB*, define how the Rise Time criteria should be configured for DTMF detection in the `interopDtmfDetectionRiseTimeCriteria` variable.

   You can also use the following line in the CLI or a configuration script:

   `sipEp.interopDtmfDetectionRiseTimeCriteria="Value"`

where *Value* may be as follows:

Table 216: DTMF Detection Values

Value	Method	
100	CheckSr	Enables the Step Rise criteria and disables the Confirm DTMF SNR criteria. The Step Rise criteria compares the current frame energy to the high frequency power of the previous frame. If the current frame energy is high enough, then it passes the test, further validating the DTMF. Disabling the Step Rise criteria may result in deteriorated talk-off performance, but increases the detection of malformed DTMF.
200	ConfirmSnr	Enable the Confirm DTMF SNR criteria and disable the Step Rise criteria. The Confirm DTMF SNR criteria is an additional Signal-to-noise ratio test performed before a confirmed DTMF report is sent to finally validate the DTMF.

2. Set the `interopDtmfDetectionPositiveTwist` variable.

   You can also use the following line in the CLI or a configuration script:

   `sipEp.interopDtmfDetectionPositiveTwist="Value"`

   When the high-group frequency of a DTMF is more powerful than the low-group frequency, the difference between the high-group frequency absolute power and the low-group frequency absolute power must be smaller than or equal to the value set in this variable. Otherwise, the DTMF is not detected.

   Raising this value increases the sensitivity of DTMF detection. Raising this value too high may also cause false detections of DTMFs.

Using the Payload Type Found in the Answer

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

The default behaviour when sending an initial offer that contains an RFC 2833 payload type is to keep using that payload type even if the response comes back with a different one. You can set the Aastra unit to rather use the payload type found in the answer.

This feature is effective only if the *Transport Method* drop-down menu is set to **Out-of-band using RTP** (see “Miscellaneous Media Parameters” on page 263 for more details).

The following parameters are available:

Table 217: Payload Type in Answer

Parameter	Description
disable	Keep using the initial payload type. This is the default value.
enable	Use the RFC 2833 payload type found in the received answer.

▶ **To use the payload type found in the answer:**

1. In the *sipEpMIB*, set the `interopUseDtmfPayloadTypeFoundInAnswer` variable with the proper behaviour.

   You can also use the following line in the CLI or a configuration script:

   `sipEp.interopUseDtmfPayloadTypeFoundInAnswer="Value"`

where *Value* may be as follows:

Figure 126: Payload Type Values

Value	Meaning
0	disable
1	enable

Quantity of initial packets sent to transmit a DTMF Out-of-Band using RTP

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

You can specify the quantity of packets sent at the beginning of an Out-of-Band DTMF using RTP. This variable also specifies the quantity of terminating packets that are sent at the end of the DTMF transmission.

Note that this variable has an effect only if the *Transport Method* drop-down menu is set to **Out-of-band using RTP** (see "Miscellaneous Media Parameters" on page 263 for more details).

▶ To set the initial quantity of RTP packets:

1. In the *miptMIB*, set the `InteropDtmfRtpInitialPacketQty` variable with the proper quantity.

   You can also use the following line in the CLI or a configuration script:

   `mipt.interopDtmfRtpInitialPacketQty="Value"`

   where *Value* may be between 1 and 3.

Machine Detection Configuration

The *Machine Detection* section allows you to set the tone detection parameters of the Aastra unit.

▶ To set Machine detection parameters:

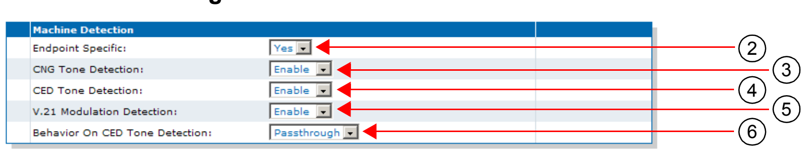
1. Select to which endpoint (interface) you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

   You have the choice between *Default* and the interfaces of your Aastra unit. The number of interfaces available vary depending on the Aastra unit model you have.

2. In the *Machine Detection* section of the *Misc* page, select whether or not you want to override the machine detection parameters set in the *Default* configuration in the *Endpoint Specific* drop-down menu.

   This menu is available only in the specific endpoints configuration.

Figure 127: Machine Detection Section



3. Select whether or not you want to enable fax calling tone (CNG tone) detection in the *CNG Tone Detection* drop-down menu.

Table 218: CNG Tone Detection Settings

Setting	Description
Enable	Upon recognition of the CNG tone, the unit switches the communication from voice mode to fax mode and the CNG is transferred by using the preferred fax codec. **Note:** This option allows for quicker fax detection, but it also increases the risk of false detection.
Disable	The CNG tone does not trigger a transition from voice to data and the CNG is transferred in the voice channel. **Note:** With this option, faxes are detected later, but the risk of false detection is reduced.

4. Select whether or not you want to enable CED tone detection in the *CED Tone Detection* drop-down menu.

Table 219: CNG CED Detection Settings

Setting	Description
Enable	Upon recognition of the CED tone, the unit behaves as defined in the *Behavior on CED Tone Detection* parameter Step 6).
Disable	The CED tone does not trigger a transition to fax or voiceband data mode. The CED is transferred in the voice channel.

5. Select whether or not you want to enable fax V.21 modulation detection in the *V.21 Modulation Detection* drop-down menu.

Table 220: V.21 Modulation Detection Settings

Setting	Description
Enable	Upon recognition of the V.21 modulation tone, the unit switches the communication from voice mode to fax mode and the signal is transferred by using the preferred fax codec.
Disable	The V.21 modulation does not trigger a transition from voice to data and the signal is transferred in the voice channel.

6. Define the behaviour of the unit upon detection of a CED tone in the *Behavior on CED Tone Detection* drop-down menu.

Table 221: CED Tone Detection Settings

Setting	Description
Passthrough	The CED tone triggers a transition from voice to voice band data and is transferred in the voice channel.. Use this setting when any kind of analog device (i.e.: telephone, fax or modem) can be connected to this port.
Fax Mode	Upon detection of a CED tone, the unit switches the communication from voice mode to fax mode and the CED is transferred by using the preferred fax codec. Only a fax can then be connected to this port.

Note: This parameter has no effect if the C*ED Tone Detection* parameter is set to **Disabled**.

7. Click *Submit* if you do not need to set other parameters.

Base Ports Configuration

The *Base Ports* section allows you to set the ports that the Aastra unit uses for different transports.

This section is available only in the default endpoint configuration.

▶ **To set base ports parameters:**

1. Select to which endpoint (interface) you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

   You have the choice between *Default* and the interfaces of your Aastra unit. The number of interfaces available vary depending on the Aastra unit model you have.

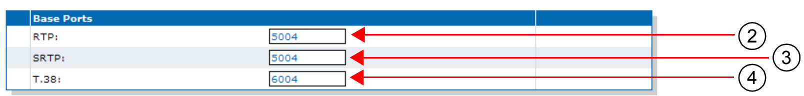
2. In the *Base Ports* section of the *Misc* page, set the UDP port number you want to use as RTP/RTCP base port in the *RTP* field.

   The RTP/RTCP ports are allocated starting from this base port.

   RTP ports number are even and RTCP ports number are odd.

   The default RTP/RTCP base port is **5004**. For instance, assuming that the base port is defined on 5004, if there is currently no ongoing call and there is an incoming or outgoing call, the unit uses the RTP/RTCP ports 5004 and 5005.

   Figure 128: Base Ports Section

3. Set the UDP port number you want to use as SRTP/SRTCP base port in the *SRTP* field.

   The SRTP/SRTCP ports are allocated starting from this base port.

   SRTP ports number are even and SRTCP ports number are odd.

   The default SRTP/SRTCP base port is **5004**. For instance, assuming that the base port is defined on 5004, if there is currently no ongoing call and there is an incoming or outgoing call, the unit uses the SRTP/SRTCP ports 5004 and 5005.

   Using the same base port for RTP/RTCP and SRTP/SRTCP does not conflict.

   Note that if the media transport is set to "Secure with fallback" ("Chapter 32 - Security" on page 377), both RTP and SRTP base ports are used at the same time when initiating an outgoing call. If there is currently no call and the default base ports are used, the RTP port is 5004 and the SRTP port is the next available port starting from the base port, which is 5006.

4. Set the port number you want to use as T.38 base port in the *T.38* field.

   The T.38 ports are allocated starting from this base port.

   The default T.38 base port is **6004**. For instance, assuming that the base port is defined on 6004 if there is currently no ongoing call and there is an incoming or outgoing call, the unit uses the T.38 port 6005.

   This menu is available only in the default endpoint configuration.

5. Click *Submit* if you do not need to set other parameters.

AastraSoftware Configuration Guide

Telephony Parameters

Page Left Intentionally Blank

CHAPTER
32

DTMF Maps Configuration

This chapter describes how to configure and use the DTMF maps of the Aastra unit.

Standards Supported	• RFC 2705: Media Gateway Control Protocol (MGCP) Version 1.0, section 3.4 (Formal syntax description of the protocol).

- DTMF maps syntax.
- General DTMF maps parameters.
- Allowed DTMF maps parameters.
- Refused DTMF maps parameters.

Introduction

A DTMF map (also called digit map or dial map) allows you to compare the number users just dialed to a string of arguments. If they match, users can make the call. If not, users cannot make the call and get an error signal. It is thus essential to define very precisely a DTMF map before actually implementing it, or your users may encounter calling problems.

Because the Aastra unit cannot predict how many digits it needs to accumulate before transmission, you could use the DTMF map, for instance, to determine exactly when there are enough digits entered from the user to place a call.

Syntax

The permitted DTMF map syntax is taken from the core MGCP specification, RFC 2705, section 3.4:

```
DigitMap = DigitString  / '(' DigitStringList ')'
DigitStringList = DigitString 0*( '|' DigitString )
DigitString = 1*(DigitStringElement)
DigitStringElement = DigitPosition ['.']
DigitPosition = DigitMapLetter / DigitMapRange
DigitMapLetter = DIGIT / '#' / '*' / 'A' / 'B' / 'C' / 'D' / 'T'
DigitMapRange =  'x' / '[' 1*DigitLetter ']'
DigitLetter ::= *((DIGIT '-' DIGIT ) / DigitMapLetter)
```

Where “x” means “any digit” and “.” means “any number of”.

For instance, using the telephone on your desk, you can dial the following numbers:

Table 222: Number Examples

Number	Description
0	Local operator
00	Long distance operator
xxxx	Local extension number
8xxxxxxx	Local number
#xxxxxxx	Shortcut to local number at other corporate sites
91xxxxxxxxxx	Long distance numbers

Table 222: Number Examples (Continued)

Number	Description
9011 + up to 15 digits	International number

The solution to this problem is to load the Aastra unit with a DTMF map that corresponds to the dial plan.

A Aastra unit that detects digits or timers applies the current dial string to the DTMF map, attempting a match to each regular expression in the DTMF map in lexical order.

- If the result is under-qualified (partially matches at least one entry in the DTMF map), waits for more digits.
- If the result matches, dials the number.
- If the result is over-qualified (i.e., no further digits could possibly produce a match), sends a fast busy signal.

Special Characters

DTMF maps use specific characters and digits in a particular syntax.

Table 223: DTMF Map Characters

Character	Use
Digits (0, 1, 2... 9)	Indicates specific digits in a telephone number expression.
T	The Timer indicates that if users have not dialed a digit for the time defined, it is likely that they have finished dialing and the SIP Server can make the call.
x	Matches any digit, excluding “#” and “*”.
|	Indicates a choice of matching expressions (OR).
.	Matches an arbitrary number of occurrences of the preceding digit, including 0.
[	Indicates the start of a range of characters.
]	Indicates the end of a range of characters.

How to Use a DTMF Map

Let’s say you are in an office and you want to call a co-worker’s 3-digits extension. You could build a DTMF map that says “after the user has entered 3 digits, make the call”. The DTMF map could look as follows:

```
xxx
```

You could refine this DTMF map by including a range of digits. For instance, you know that all extensions in your company either begin with 2, 3, or 4. The corresponding DTMF map could look as follows:

```
[2-4]xx
```

If the number you dial begins with anything other than 2, 3, or 4, the call is not placed and you get a busy signal.

Combining Several Expressions

You can combine two or more expressions in the same DTMF map by using the “|” operator, which is equal to OR.

Let’s say you want to specify a choice: the DTMF map is to check if the number is internal (extension), or external (a local call). Assuming that you must first dial “9” to make an external call, you could define a DTMF map as follows:

```
([2-4]xx|9[2-9]xxxxxx)
```

The DTMF map checks if:

- the number begins with 2, 3, or 4 **and**
- the number has 3 digits

If not, it checks if:

- the number begins with 9 **and**
- the second digit is any digit between 2 and 9 **and**
- the number has 7 digits

> **Note:** Enclose the DTMF map in parenthesis when using the “|” option.

Using the # and * Characters

It may sometimes be required that users dial the “#” or “*” to make calls. This can be easily incorporated in a DTMF map:

```
xxxxxxx#
xxxxxxx*
```

The “#” or “*” character could indicate users must dial the “#” or “*” character at the end of their number to indicate it is complete. You can specify to remove the “#” or “*” found at the end of a dialed number. See “General DTMF Maps Parameters” on page 282.

Using the Timer

The Timer indicates that if users have not dialed a digit for the time defined, it is likely that they have finished dialing and the Aastra unit can make the call. A DTMF map for this could be:

```
[2-9]xxxxxxT
```

> **Note:** When making the actual call and dialing the number, the Aastra unit automatically removes the “T” found at the end of a dialed number, if there is one (after a match). This character is for indication purposes only.

See “General DTMF Maps Parameters” on page 282 for more details.

Calls Outside the Country

If your users are making calls outside their country, it may sometimes be hard to determine exactly the number of digits they must enter. You could devise a DTMF map that takes this problem into account:

```
001x.T
```

In this example, the DTMF map looks for a number that begins with 001, and then any number of digits after that (x.).

Example

Table 222 on page 279 outlined various call types one could make. All these possibilities could be covered in one DTMF map:

```
(0T|00T|[1-7]xxx|8xxxxxxx|#xxxxxxx|91xxxxxxxxxx|9011x.T)
```

Validating a DTMF Map

The Aastra unit validates the DTMF map as you are entering it and it forbids any invalid value.

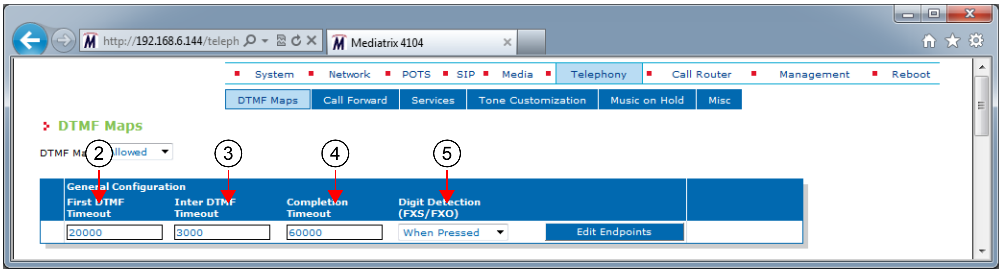
General DTMF Maps Parameters

The following are the general DTMF maps parameters you can set.

▶ **To set the general DTMF map parameters:**

1. In the web interface, click the *Telephony* link, then the *DTMF Maps* sub-link.

Figure 129: Telephony – DTMF Maps Web Page



2. In the *General Configuration* section, define the time, in milliseconds (ms), between the start of the dial tone and the receiver off-hook tone, if no DTMF is detected, in the *First DTMF Timeout* field.

Values range from 1000 ms to 180000 ms. The default value is **20000** ms.

If you want to set a different *First DTMF Timeout* value for one or more endpoints, click the **Edit Endpoints** button (see "Configuring Timeouts per Endpoint" on page 283 for more details).

3. Define the value, in milliseconds (ms), of the "T" digit in the *Inter Digit Timeout* field.

The "T" digit expresses a time lapse between the detection of two DTMFs. Values range from 500 ms to 10000 ms. The default value is **4000** ms.

If you want to set a different *Inter Digit Timeout* value for one or more endpoints, click the **Edit Endpoints** button (see "Configuring Timeouts per Endpoint" on page 283 for more details).

4. Define the total time, in milliseconds (ms), the user has to dial the DTMF sequence in the *Completion Timeout* field.

The timer starts when the dial tone is played. When the timer expires, the receiver off-hook tone is played. Values range from 1000 ms to 180000 ms. The default value is **60000** ms.

If you want to set a different *Completion Timeout* value for one or more endpoints, click the **Edit Endpoints** button (see "Configuring Timeouts per Endpoint" on page 283 for more details).

5. In the *DTMF Maps Digit Detection (FXO/FXS)* drop-down menu, define when a digit is processed through the DTMF maps.

This parameters is available only when the unit has FXS or FXO ports.

Table 224: DTMF Maps Digit Detection Parameters

Parameter	Description
When Pressed	Digits are processed as soon as they are pressed. This can lead to a digit leak in the RTP at the beginning of a call if the voice stream is established before the last digit is released.
When Released	Digits are processed only when released. This option increases the delay needed to match a dialed string to a DTMF map. There is also an impact on the *First DTMF Timeout*, *Inter Digit Timeout* and *Completion Timeout* parameters since the timers are stopped at the end of a digit instead of the beginning.

6. Click *Submit* if you do not need to set other parameters.

Configuring Timeouts per Endpoint

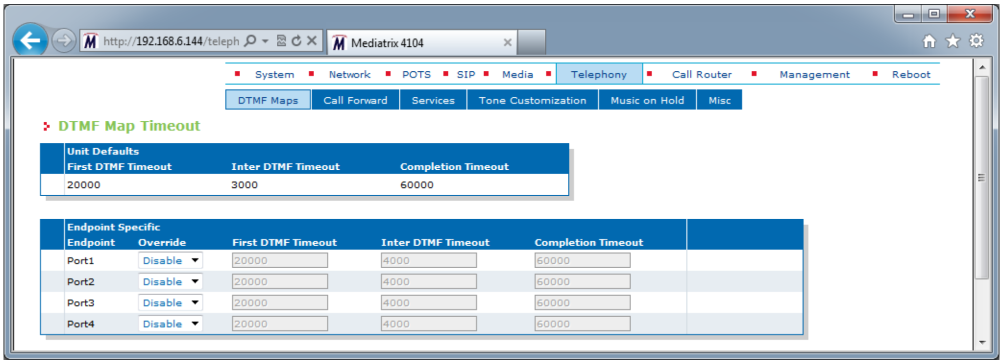
You can set a different timeout value for one or more endpoints.

▶ **To set a different value per endpoint:**

1. In the *General Configuration* section of the *DTMF Maps* page, click the **Edit Endpoints** button.

   The following window is displayed:

Figure 130: DTMF Map Timeout Section



2. Set the *Override* drop-down menu for the endpoint you want to set to **Enable**.
3. Change the value of one or more timeouts as required.
4. Repeat for each endpoint that you want to modify.
5. Click *Submit* when finished.

Allowed DTMF Maps

You can create/edit ten DTMF maps for the Aastra unit. DTMF map rules are checked sequentially. If a telephone number potentially matches two of the rules, the first rule encountered is applied.

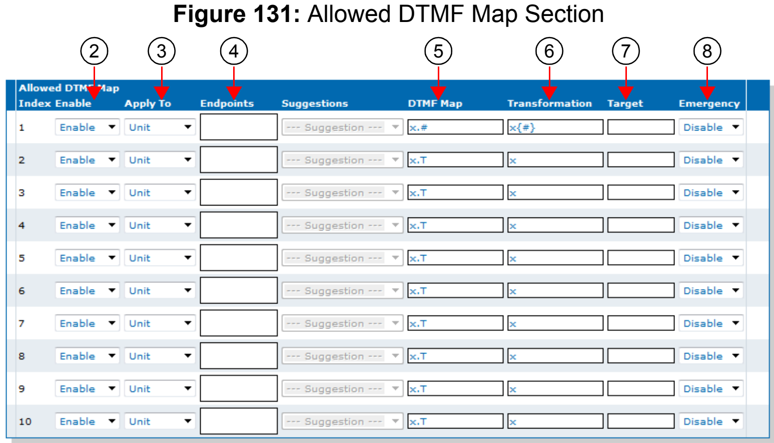
▶ **To set up DTMF maps:**

1. In the *DTMF Map* drop-down menu at the top of the window, select **Allowed**.

   The *Allowed DTMF Map* section displays.

2. In the *Allowed DTMF Map* section – *Enable* column, enable one or more DTMF maps by selecting the corresponding **Enable** choice.

Figure 131: Allowed DTMF Map Section



3. Select the entity to which apply the allowed DTMF map in the *Apply to* column.

Table 225: DTMF Map Entity

Parameter	Description
Unit	The DTMF map entry applies to the unit.
Endpoint	The DTMF map applies to a specific endpoint. The endpoint is specified in the *Endpoint* column of the same row.

4. Enter a string that identifies an endpoint in other tables in the *Endpoint* column.

This field is available only if you have selected the **Endpoint** entity in the previous step for the specific row.

You can specify more than one endpoint. In that case, the endpoints are separated with a comma (,). You can use the *Suggestions* column's drop-down menu to select between suggested values, if any.

5. Define the DTMF map string that is considered valid when dialed in the *DTMF Map* column.

The string must use the syntax described in "DTMF Maps Configuration" on page 279. A DTMF map string may have a maximum of 64 characters.

6. Enter the DTMF transformation to apply to the signalled DTMFs before using it as call destination in the *Transformation* column.

The following are the rules you must follow; "x" represents the signalled number.

- Add before "x" the DTMF to prefix or/and after "x" the suffix to add. Characters "0123456789*# ABCD" are allowed.
- Use a sequence of DTMFs between "{}" to remove a prefix/suffix from the dialed number if present. Use before "x" to remove a prefix and after "x" to remove a suffix. Characters "0123456789*#ABCD" are allowed.
- Use a number between "()" to remove a number of DTMFs. Use before "x" to remove DTMFs at the beginning of the number and after "x" to remove DTMFs at the end. Characters "0123456789" are allowed.

The transformations are applied in order from left to right.

The following table gives an example with "18195551111#" as signalled number.

Table 226: DTMF Map Transformation Examples

Action	Transformation	Result
Add the prefix "0" to the dialed number	0x	018195551111#
Remove the suffix "#" from the dialed number	x{#}	18195551111
Remove the first four DTMFs from the dialed number	(4)x	5551111#
Remove the international code and termination and replace the area code by another one	(1){819}514x{#}	5145551111
Replace the signalled DTMFs by "3332222"	3332222	3332222

7. Define the target to use when the DTMF map matches in the *Target* column.

This allows associating a target (FQDN) with a DTMF map. This defines a destination address to use when the DTMF map matches. This address is used as destination for the INVITEs in place of the "home domain proxy". This is useful for such features as the speed dial and emergency call.

The default target is used when the value is empty.

The dialed DTMFs are not used if the target contains a user name.

8. Enable/Disable the emergency process of the call in the *Emergency* column.

- Disable: The call is processed normally.
- Enable: The call is processed as emergency.

The Emergency Call service (also called urgent gateway) allows a “911”-style service. It allows a user to dial a special DTMF map resulting in a message being sent to a specified urgent gateway, bypassing any other intermediaries.

If enabled, whenever the user dials the specified DTMF map, a message is sent to the target address.

9. Click *Submit* if you do not need to set other parameters.

Refused DTMF Maps

A refused DTMF map forbids to call specific numbers; for instance, you want to accept all 1-8xx numbers except 1-801. You can create/edit ten refused DTMF maps for the Aastra unit.

A refused DTMF map applies before an allowed DTMF map.

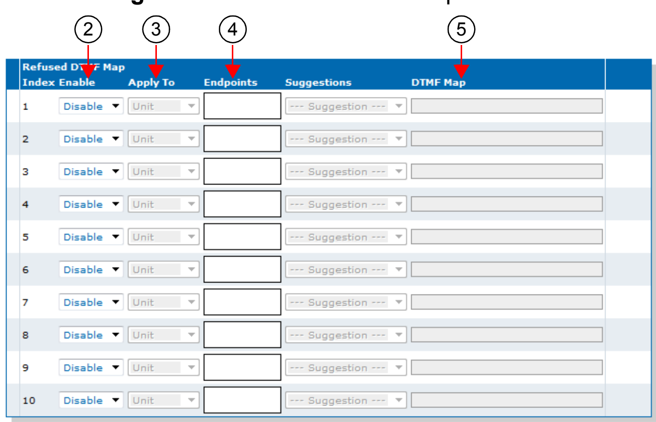
▶ **To set up refused DTMF maps:**

1. In the *DTMF Map* drop-down menu at the top of the window, select **Refused**.

The *Refused DTMF Map* section displays.

2. In the *Refused DTMF Map* section – *Enable* column, enable one or more DTMF maps by selecting the corresponding **Enable** choice.

Figure 132: Refused DTMF Map Section



3. Select the entity to which apply the refused DTMF map in the *Apply to* column.

Table 227: DTMF Map Entity

Parameter	Description
Unit	The DTMF map entry applies to the unit.
Endpoint	The DTMF map applies to a specific endpoint. The endpoint is specified in the *Endpoint* column of the same row.

4. Enter a string that identifies an endpoint in other tables in the *Endpoint* column.

This field is available only if you have selected the **Endpoint** entity in the previous step for the specific row.

You can specify more than one endpoint. In that case, the endpoints are separated with a comma (,). You can use the *Suggestions* column's drop-down menu to select between suggested values, if any.

5. Define the DTMF map string that is considered valid when dialed in the *DTMF Map* column.

The string must use the syntax described in "DTMF Maps Configuration" on page 279. A DTMF map string may have a maximum of 64 characters.

6. Click *Submit* if you do not need to set other parameters.

CHAPTER 33 Call Forward Configuration

This chapter describes how to set three types of Call Forward:

- On Busy
- On No Answer
- Unconditional

You can use two types of configuration:

- Default configurations that apply to all the endpoints of the Aastra unit.
- Specific configurations that override the default configurations. You can define specific configurations for each endpoint in your Aastra unit.

> **Note:** This web page is available only on the following models: TA7102i

Call Forward On Busy

You can automatically forward the incoming calls of your users to a pre-determined target if they are already on the line. The user does not have any feedback that a call was forwarded.

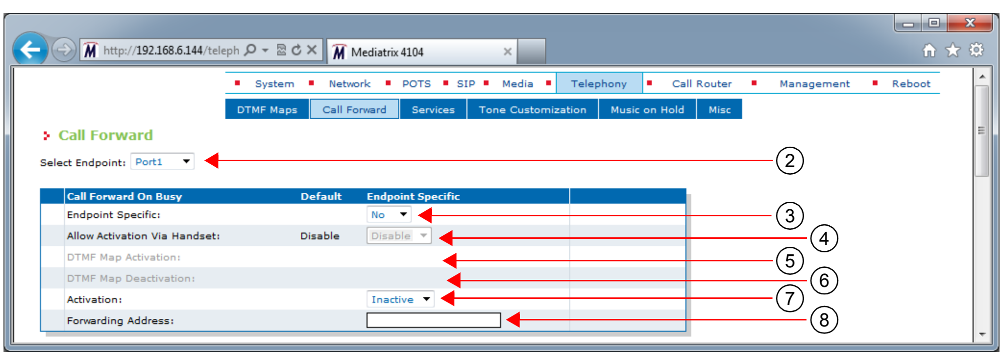
You can enable the Call Forward On Busy feature in two ways:

- By allowing the user to configure the call forward activation and its destination via the handset (Steps 4-6).
- By manually enabling the service (Steps 7-8).

▶ To set the Call Forward On Busy feature:

1. In the web interface, click the *Telephony* link, then the *Call Forward* sub-link.

Figure 133: Telephony – Call Forward Web Page



2. Select to which endpoint you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

   You have the choice between *Default* and all FXS endpoints your Aastra unit has.

3. In the *Call Forward On Busy* section, define whether or not you want to override the Call Forward On Busy parameters set in the *Default* configuration in the *Endpoint Specific* drop-down menu.

   This menu is available only in the specific endpoints configuration.

4. Enable the Call forward configuration via handset service by setting the *Allow Activation via Handset* drop-down menu to **Enable**.

You also need to configure the activation and deactivation DTMF maps (steps 5 and 6).

If you select **Disable**, this does not disable the call forward, but prevents the user from activating or deactivating the call forward service. The user will not be able to use the digits used to activate and deactivate the call forward service.

5. Define the digits that users must dial to start the service in the *DTMF Map Activation* field.

This field is available only in the *Default* configuration.

For instance, you could decide to put "*72" as the sequence to activate the service. This sequence must be unique and follow the syntax for DTMF maps (see "Chapter 35 - DTMF Maps Configuration" on page 401). Dialing this DTMF map does not have any effect unless the service's status is "enabled".

The activating sequence is set for all the endpoints of the Aastra unit. You cannot have a different sequence for each endpoint.

6. Define the digits that users must dial to stop the service in the *DTMF Map Deactivation* field.

This field is available only in the *Default* configuration.

For instance, you could decide to put "*73" as the sequence to deactivate the service. This sequence must be unique and follow the syntax for DTMF maps (see "Chapter 35 - DTMF Maps Configuration" on page 401). Dialing this DTMF map does not have any effect unless the service's status is "enabled".

The deactivating sequence is set for all the endpoints of the Aastra unit. You cannot have a different sequence for each endpoint.

7. Set the call forward service in the *Activation* field to **Inactive** or **Active**.

Table 228: Activation State

State	Description
Inactive	The call forward service is not available on the telephone connected to the specific endpoint. A call to this endpoint is not forwarded if the endpoint is busy.
Active	The call forward service is available on the telephone connected to the specific endpoint. A call to the endpoint is forwarded to the specified destination if the endpoint is busy. You must define the call forward destination in the *Forwarding Address* field (Step 8). The call forward service behaves as if it is inactive if the Forwarding Address is empty.

To let the user activate or deactivate this service with his or her handset, see steps 4, 5, and 6. In that case, the field is automatically updated to reflect the activation status.

8. Define the address to which forward incoming calls in the *Forwarding Address* field.

Accepted formats are:

- telephone numbers (5551111)
- SIP URLs such as "scheme:user@host". For instance, "sip:user@foo.com".

This string is used literally, so cosmetic symbols (such as the dash in "555-xxxx") should not be present.

9. Click *Submit* if you do not need to set other parameters.

Configuring Call Forward on Busy via Handset

The following is the procedure to use this service on the user's telephone.

▶ **To forward calls:**

1. Take the receiver off-hook.

2. Wait for the dial tone.

3. Dial the sequence implemented to activate the call forward on busy service.

This sequence could be something like *72.

4. Wait for the stutter dial tone (three “beeps”) followed by the dial tone.

5. Dial the number to which you want to forward your calls. Dial any access code if required.

6. Wait for three “beeps” followed by a silent pause.

The call forward is established.

7. Hang up your telephone.

▶ **To cancel the call forward:**

1. Take the receiver off-hook.

2. Wait for the dial tone.

3. Dial the sequence implemented to deactivate the call forward on busy service.

This sequence could be something like *73.

4. Wait for the transfer tone (three “beeps”) followed by the dial tone.

The call forward is cancelled.

5. Hang up your telephone.

Call Forward On No Answer

You can forward the incoming calls of your users to a pre-determined target if they do not answer their telephone before a specific amount of time. The user does not have any feedback that a call was forwarded.

You can enable the Call Forward On Busy feature in two ways:

- By allowing the user to configure the call forward activation and its destination via the handset (Steps 3-5).
- By manually enabling the service (Steps 6-8).

▶ **To set the Call Forward On No Answer feature:**

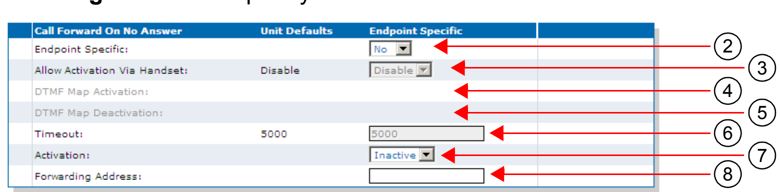
1. Select to which endpoint you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

You have the choice between *Default* and all FXS endpoints your Aastra unit has.

2. In the *Call Forward On No Answer* section, define whether or not you want to override the Call Forward On No Answer parameters set in the *Default* configuration in the *Endpoint Specific* drop-down menu.

This menu is available only in the specific endpoints configuration.

Figure 134: Telephony – Call Forward on No Answer section



3. Enable the Call forward configuration via handset service by setting the *Allow Activation via Handset* drop-down menu to **Enable**.

   You also need to configure the activation and deactivation DTMF maps (steps 4 and 5).

   If you select **Disable**, this does not disable the call forward, but prevents the user from activating or deactivating the call forward service. The user will not be able to use the digits used to activate and deactivate the call forward service.

4. Define the digits that users must dial to start the service in the *DTMF Map Activation* field.

   This field is available only in the *Default* configuration.

   For instance, you could decide to put “*74” as the sequence to activate the service. This sequence must be unique and follow the syntax for DTMF maps (see “Chapter 35 - DTMF Maps Configuration” on page 401). Dialing this DTMF map does not have any effect unless the service’s status is “enabled”.

   The activating sequence is set for all the endpoints of the Aastra unit. You cannot have a different sequence for each endpoint.

5. Define the digits that users must dial to stop the service in the *DTMF Map Deactivation* field.

   This field is available only in the *Default* configuration.

   For instance, you could decide to put “*75” as the sequence to deactivate the service. This sequence must be unique and follow the syntax for DTMF maps (see “Chapter 35 - DTMF Maps Configuration” on page 401). Dialing this DTMF map does not have any effect unless the service’s status is “enabled”.

   The deactivating sequence is set for all the endpoints of the Aastra unit. You cannot have a different sequence for each endpoint.

6. Define the time, in milliseconds, the telephone keeps ringing before the call forwarding activates in the *Timeout* field.

7. Set the status of the service in the *Activation* field to **Inactive** or **Active**.

Table 229: Activation State

State	Description
Inactive	The call forward service is not available on the telephone connected to the specific endpoint. A call to this endpoint is not forwarded if the endpoint is busy.
Active	The call forward service is available on the telephone connected to the specific endpoint. A call to the endpoint is forwarded to the specified destination if the endpoint is busy. You must define the call forward destination in the *Forwarding Address* field (Step 8). The call forward service behaves as if it is inactive if the Forwarding Address is empty.

   To let the user activate or deactivate this service with his or her handset, see steps 3, 4, and 5. In that case, the field is automatically updated to reflect the activation status.

8. Define the address to which forward incoming calls in the *Forwarding Address* field.

   Accepted formats are:

   - telephone numbers (5551111)
   - SIP URLs such as ”scheme:user@host”. For instance, “sip:user@foo.com”.

   This string is used literally, so cosmetic symbols (such as the dash in “555-xxxx”) should not be present.

9. Click *Submit* if you do not need to set other parameters.

Configuring Call Forward on Answer via Handset

The following is the procedure to use this service on the user’s telephone.

▶ **To forward calls:**

1. Take the receiver off-hook.
2. Wait for the dial tone.
3. Dial the sequence implemented to activate the call forward on no answer service.

   This sequence could be something like *74.
4. Wait for the transfer tone (three “beeps”) followed by the dial tone.
5. Dial the number to which you want to forward your calls. Dial any access code if required.
6. Wait for three “beeps” followed by a silent pause.

   The call forward is established.
7. Hang up your telephone.

▶ **To cancel the call forward:**

1. Take the receiver off-hook.
2. Wait for the dial tone.
3. Dial the sequence implemented to deactivate the call forward on no answer service.

   This sequence could be something like *75.
4. Wait for the stutter dial tone (three “beeps”) followed by the dial tone.

   The call forward is cancelled.
5. Hang up your telephone.

Call Forward Unconditional

The Call Forward Unconditional feature allows users to forward all of their calls to another extension or line.

You can enable the Call Forward On Busy feature in two ways:

- By allowing the user to configure the call forward activation and its destination via the handset (Steps 3-5).
- By manually enabling the service (Steps 6-7).

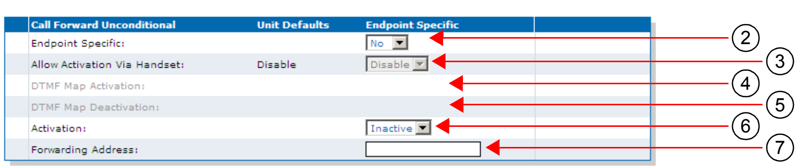
▶ **To set the Call Forward Unconditional feature:**

1. Select to which endpoint you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

   You have the choice between *Default* and all FXS endpoints your Aastra unit has.
2. In the *Unconditional* section, define if you want to override the Call Forward Unconditional parameters set in the *Default* configuration in the *Endpoint Specific* drop-down menu.

   This menu is available only in the specific endpoints configuration.

Figure 135: Telephony – Call Forward Unconditional Section



3. Enable the Call forward configuration via handset service by setting the *Allow Activation via Handset* drop-down menu to **Enable**.

You also need to configure the activation and deactivation DTMF maps (steps 4 and 5).

If you select **Disable**, this does not disable the call forward, but prevents the user from activating or deactivating the call forward service. The user will not be able to use the digits used to activate and deactivate the call forward service.

4. Define the digits that users must dial to start the service in the *DTMF Map Activation* field.

This field is available only in the *Default* configuration.

For instance, you could decide to put "*76" as the sequence to activate the service. This sequence must be unique and follow the syntax for DTMF maps (see "Chapter 35 - DTMF Maps Configuration" on page 401). Dialing this DTMF map does not have any effect unless the service's status is "enabled".

The activating sequence is set for all the endpoints of the Aastra unit. You cannot have a different sequence for each endpoint.

5. Define the digits that users must dial to stop the service in the *DTMF Map Deactivation* field.

This field is available only in the *Default* configuration.

For instance, you could decide to put "*77" as the sequence to deactivate the service. This sequence must be unique and follow the syntax for DTMF maps (see "Chapter 35 - DTMF Maps Configuration" on page 401). Dialing this DTMF map does not have any effect unless the service's status is "enabled".

The deactivating sequence is set for all the endpoints of the Aastra unit. You cannot have a different sequence for each endpoint.

6. Set the status of the service in the *Activation* field to **Inactive** or **Active**.

Table 230: Activation State

State	Description
Inactive	The call forward service is not available on the telephone connected to the specific endpoint. A call to this endpoint is not forwarded if the endpoint is busy.
Active	The call forward service is available on the telephone connected to the specific endpoint. A call to the endpoint is forwarded to the specified destination if the endpoint is busy. You must define the call forward destination in the *Forwarding Address* field (Step 7). The call forward service behaves as if it is inactive if the Forwarding Address is empty.

To let the user activate or deactivate this service with his or her handset, see steps 3, 4, and 5. In that case, the field is automatically updated to reflect the activation status.

7. Define the address to which forward incoming calls in the *Forwarding Address* field.

Accepted formats are:

- telephone numbers (5551111)
- SIP URLs such as "scheme:user@host". For instance, "sip:user@foo.com".

This string is used literally, so cosmetic symbols (such as the dash in "555-xxxx") should not be present.

8. Click *Submit* if you do not need to set other parameters.

Configuring Call Forward on Unconditional via Handset

When forwarding calls outside the system, a brief ring is heard on the telephone to remind the user that the call forward service is active. The user can still make calls from the telephone.

▶ **To forward calls:**

1. Take the receiver off-hook.

2. Wait for the dial tone.

3. Dial the sequence implemented to activate the call forward unconditional service.

   This sequence could be something like *76.
4. Wait for the stutter dial tone (three “beeps”) followed by the dial tone.
5. Dial the number to which you want to forward your calls. Dial any access code if required.
6. Wait for three “beeps” followed by a silent pause.

   The call forward is established.
7. Hang up your telephone.

▶ **To check if the call forward has been properly established:**

1. Take the receiver off-hook.
2. Wait for the dial tone.
3. Dial your extension or telephone number.

   The call is forwarded to the desired telephone number.
4. Hang up your telephone.

▶ **To cancel the call forward:**

1. Take the receiver off-hook.
2. Wait for the dial tone.
3. Dial the sequence implemented to deactivate the call forward – unconditional service.

   This sequence could be something like *77.
4. Wait for the stutter dial tone (three “beeps”) followed by the dial tone.

   The call forward is cancelled.
5. Hang up your telephone.

CHAPTER

34

Telephony Services Configuration

This chapter describes how to set the following subscriber services:

- Hook Flash Processing
- Automatic call
- Call completion
- Delayed Hotline
- Call Transfer
- Call Waiting
- Conference
- Direct IP address call
- Hold
- Second call
- Message Waiting Indicator

Some of the subscriber services are not supported on all Aastra unit models, so your specific model may not have all subscriber services listed in this chapter.

You can use two types of configuration:

- Default configurations that apply to all the endpoints of the Aastra unit.
- Specific configurations that override the default configurations. You can define specific configurations for each endpoint in your Aastra unit.

General Configuration

Standards Supported	• RFC 2976: The SIP INFO Method

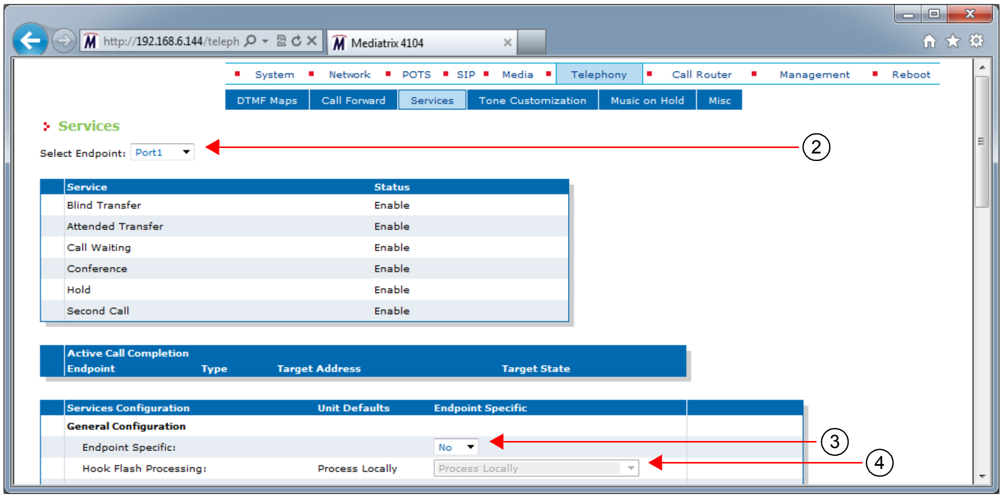
The *General Configuration* sub-section of the *Services Configuration* section allows you to define the Hook Flash Processing feature.

Note: Performing a flash hook and pressing the flash button means the same thing. However, not all telephone models have a flash button.

▶ To set general services parameters:

1. In the web interface, click the *Telephony* link, then the *Services* sub-link.

Figure 136: Telephony – Services Web Page



2. Select to which endpoint you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

You have the choice between *Default* and the interfaces of your Aastra unit. The number of interfaces available vary depending on the Aastra unit model you have.

3. In the *General Configuration* sub-section, define whether or not you want to override the general services parameters set in the *Default* configuration in the *Endpoint Specific* drop-down menu.

This menu is available only in the specific endpoints configuration.

4. Select how to process hook-flash detection in the *Hook Flash Processing* drop-down menu.

Hook flash processing allows hook flash signals to be transported over the IP network allowing to use advanced telephony services. Users normally press the “flash” button of the telephone during a call in progress to put this call on hold, transfer it, or even initiate a conference call.

You can define whether these subscriber services are handled by the unit or delegated to a remote party. If services are to be handled by a remote party, a SIP INFO message is sent to transmit the user's intention.

Note: The hook-flash processing attribute is not negotiated in SDP.

Table 231: Hook Flash Settings

Setting	Definition
Process Locally	The hook-flash is processed locally. The actual behaviour of the “flash” button depends on which endpoint services are enabled for this endpoint.
Transmit Using Signaling Protocol	The hook-flash is processed by a remote party. The hook-flash event is carried by a signaling protocol message. The actual behaviour of the “flash” button depends on the remote party. The hook-flash event is relayed as a SIP INFO message as described in RFC 2976.

5. Click *Submit* if you do not need to set other parameters.

Automatic Call

The automatic call feature allows you to define a telephone number that is automatically dialed when taking the handset off hook.

When this service is enabled, the second line service is disabled but the call waiting feature is still functional. The user can still accept incoming calls.

▶ **To set the automatic call feature:**

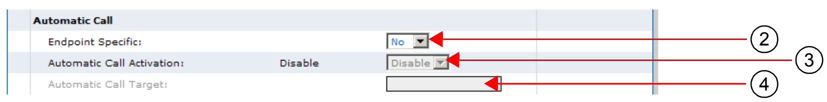
1. Select to which endpoint you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

You have the choice between *Default* and the interfaces of your Aastra unit. The number of interfaces available vary depending on the Aastra unit model you have.

2. In the *Automatic Call* sub-section, define whether or not you want to override the automatic call parameters set in the *Default* configuration in the *Endpoint Specific* drop-down menu.

This menu is available only in the specific endpoints configuration.

Figure 137: Telephony – Automatic Call Section



3. Enable the service by setting the *Automatic Call Activation* drop-down menu to **Enable**.

4. Define the string to dial when the handset is taken off hook in the *Automatic Call Target* field.

Accepted formats are:

- telephone numbers (5551111)
- SIP URLs such as ”scheme:user@host”. For instance, “sip:user@foo.com”.

This string is used literally, so cosmetic symbols (such as the dash in “555-xxxx”) should not be present.

5. Click *Submit* if you do not need to set other parameters.

Call Completion

Standards Supported	• RFC 4235: An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)[a] • draft draft-poetzl-bliss-call-completion-00[b]

a. Implemented in client mode only and used for the call completion.

b. Implement the solution 1 in 5.1.

The call completion service allows you to configure the Completion of Calls on No Reply (CCNR) and Completion of Calls to Busy Subscriber (CCBS) features.

CCBS allows a caller to establish a call with a “busy” callee as soon as this callee is available to take the call. It is implemented by monitoring the activity of a UA and look for the busy-to-idle state transition pattern.

CCNR allows a caller to establish a call with an “idle” callee right after this callee uses his phone. It is implemented by monitoring the activity of a UA and look for the idle-busy-idle state transition pattern.

The information about the call completion is not kept after a restart of the *EpServ* service. This includes the call completion activation in the *Pots* service and the call completion monitoring in the *SipEp* service.

▶ **To set the call completion feature:**

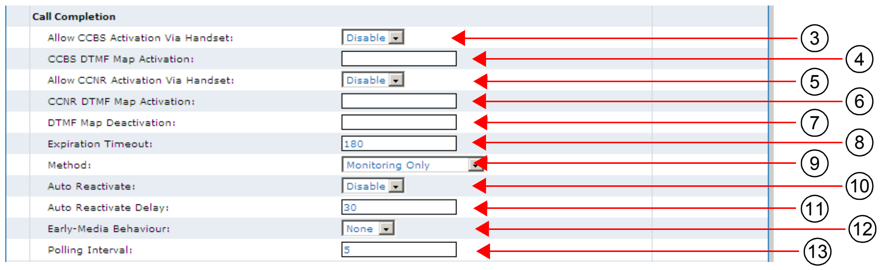
1. Select to which endpoint you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

You have the choice between *Default* and the interfaces of your Aastra unit. The number of interfaces available vary depending on the Aastra unit model you have.

2. In the *Call Completion* sub-section*,* define whether or not you want to override the call completion parameters set in the *Default* configuration in the *Endpoint Specific* drop-down menu.

   This menu is available only in the specific endpoints configuration.

Figure 138: Telephony – Call Completion Section



3. Enable or disable the (CCBS) service by selecting the proper value in the *Allow CCBS Activation Via Handset* drop-down menu.

   You also need to configure the activation and deactivation DTMF maps (steps 4 and 7).

4. If the CCBS service is enabled, define the digits that users must dial to start the service in the *CCBS DTMF Map Activation* field.

   This field is available only in the *Default* configuration.

   You can use the same code in the *CCNR DTMF Map Activation* field.

   For instance, you could decide to put "*92" as the sequence to activate the service. This sequence must be unique and follow the syntax for DTMF maps (see "Chapter 35 - DTMF Maps Configuration" on page 401). Dialing this DTMF map does not have any effect unless the service's status is "enabled".

   The activating sequence is set for all the endpoints of the Aastra unit. You cannot have a different sequence for each endpoint.

5. Enable or disable the (CCNR) service by selecting the proper value in the *Allow CCNR Activation Via Handset* drop-down menu.

   You also need to configure the activation and deactivation DTMF maps (steps 6 and 7).

6. If the CCNR service is enabled, define the digits that users must dial to start the service in the *CCNR DTMF Map Activation* field.

   This field is available only in the *Default* configuration.

   You can use the same code in the *CCBS DTMF Map Activation* field.

   For instance, you could decide to put "*93" as the sequence to activate the service. This sequence must be unique and follow the syntax for DTMF maps (see "Chapter 35 - DTMF Maps Configuration" on page 401). Dialing this DTMF map does not have any effect unless the service's status is "enabled".

   The activating sequence is set for all the endpoints of the Aastra unit. You cannot have a different sequence for each endpoint.

7. Define the digits that users must dial to stop the CCBS and CCNR services in the *DTMF Map Deactivation* field.

   This field is available only in the *Default* configuration.

   For instance, you could decide to put "*94" as the sequence to deactivate the services. This sequence must be unique and follow the syntax for DTMF maps (see "Chapter 35 - DTMF Maps Configuration" on page 401). Dialing this DTMF map does not have any effect unless the service's status is "enabled".

   The deactivating sequence is set for all the endpoints of the Aastra unit. You cannot have a different sequence for each endpoint.

8. Define the delay, in minutes, after the call completion activation to automatically deactivate the call completion if the call is not completed in the *Expiration Timeout* field.

This field is available only in the *Default* configuration.

9. Select the call completion method to detect that the call completion destination is ready to complete the call in the *Method* drop-down menu.

Table 232: Call Completion Method Parameters

Method	Desciption
Monitoring Only	The call completion only uses the monitoring method to detect that the destination is ready to complete the call.
Monitoring And Polling	The call completion only uses the monitoring method to detect that the destination is ready to complete the call. The polling mechanism is used if the call completion destination cannot be monitored.

This field is available only in the *Default* configuration.

The monitoring method consists of using the protocol signalling to detect the destination state without using the call. When the destination is ready to complete the call, the local user is notified that the call is ready to be completed and the call to the destination is initiated when the user is ready to initiate the call.

The polling method consists of using periodic calls to the call completion destination until the destination responds with a ringing or connect. Upon receiving these responses, the local user is notified that the call is ready to be completed.

The polling mechanism can only be used for call completion to busy subscriber (CCBS).

The retransmission of the polling mechanism is configurable with DefaultCallCompletionPollingInterval.

10. Enable or disable the call completion auto reactivation in the *Auto Reactivate* drop-down menu.

This field is available only in the *Default* configuration.

When enabled, the call completion busy subscriber is automatically activated if the call initiated by a call completion busy subscriber or call completion no response fails because of a busy destination.

11. Define the minimal delay to wait, in seconds, before executing a call completion after its activation in the *Auto Reactivate Delay* field.

This field is available only in the *Default* configuration.

This delay only applies to call completion activated via the call completion auto reactivation feature (See Step 9).

Aastra recommends to set a delay when the method to monitor the target state is based on the target calls instead of its ability to answer a call.

If the timeout is set to 0 and the target is off hook, the FXS endpoint always rings to notify that the call completion is ready to be completed. However the call is always busy and thus reactivated without the possibility for the user to cancel the call completion. The call completion will continue until the ringing or call completion timeout or if the target became ready to receive call.

12. Define how the call completion service needs to interpret the reception of a progress message with early media in the *Early Media Behaviour* drop-down menu.

Table 233: Call Completion Early Media Behaviour Parameters

Parameter	Description
None	The progress message with early media is not considered as a busy or a ringing response.
CCBS	The progress message with early media is interpreted as a busy response and the CCBS can be activated on the call.
CCNR	The progress message with early media is interpreted as a ringing response and the CCNR can be activated on the call.

This field is available only in the *Default* configuration.

13. Define the delay, in seconds, between the calls to the call completion target used for the polling mechanism in the *Polling Interval* field.

    This field is available only in the *Default* configuration.

    This parameter is used only if the *Default Call Completion Method* drop-down menu is set to **Monitoring And Polling**.

14. Click *Submit* if you do not need to set other parameters.

Special SIP Configuration

If you are using an Asterisk® IP PBX, it returns the error code 503 instead of 486 for a busy destination when the call limit is reached. The following error mapping can be required:

1. Go to the page *SIP* > *Misc*.
2. Insert a new mapping (with the plus button) in the *SIP To Cause Error Mapping* section.
3. Set the SIP code to 503 “Service Unavailable” and the cause to 17 “User busy”.
4. Click *Submit*.

Using the Call Completion Services

The following are the various procedures to use these services on the user’s telephone.

▶ **To start the CCBS (procedure 1)**

The call has reached a busy destination and the busy tone is played.

1. Dial the sequence implemented to enable the CCBS.

   This sequence could be something like *92.

   The confirmation tone is played.

2. Hang up the telephone.

   Alternatively, you can use procedure 2.

▶ **To start the CCBS (procedure 2)**

The call has reached a busy destination and the busy tone is played.

1. Hang up the telephone.
2. Take the receiver off-hook.

   The dial tone is played

3. Dial the sequence implemented to enable the CCBS.

   This sequence could be something like *92.

   The confirmation tone is played.

4. Hang up the telephone.

   Alternatively, you can use procedure 1.

▶ **To start the CCNR**

The call has reached a destination but the call is still not yet established. A ring back or welcome message is generally played at this moment.

1. Hang up the telephone.
2. Take the receiver off-hook.

   The dial tone is played

3. Dial the sequence implemented to enable the CCNR.

This sequence could be something like *93.
The confirmation tone is played.

4. Hang up the telephone.

▶ **To stop the CCBS or CCNR**

1. Take the receiver off-hook.
The dial tone is played

2. Dial the sequence implemented to disable the CCBS and CCNR.

This sequence could be something like *93.
The confirmation tone is played.

3. Hang up the telephone.

▶ **When the call completion target is ready to receive a call:**

1. The telephone rings with the distinctive ringing “Bellcore-dr2” (0.8 On – 0.4 Off, 0.8 On – 4.0 Off).

2. Hang up the telephone.

The call is initiated to the call completion destination.

Call Transfer

The Call Transfer service offers two ways to transfer calls:

- Blind Transfer
- Attended Transfer

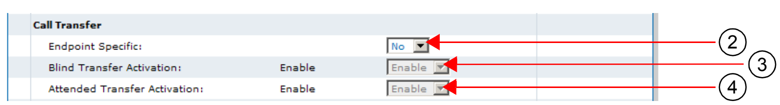
▶ **To enable the Call Transfer services:**

1. Select to which endpoint you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.
You have the choice between *Default* and all FXS endpoints your Aastra unit has.

2. In the *Call Transfer* sub-section, define whether or not you want to override the call transfer parameters set in the *Default* configuration in the *Endpoint Specific* drop-down menu.

This menu is available only in the specific endpoints configuration.

Figure 139: Telephony – Call Transfer Web Page



3. Enable the Blind Transfer service by setting the *Blind Transfer Activation* drop-down menu to **Enable**.

The blind call transfer service is sometimes called Transfer without Consultation or Unattended Transfer. It allows a user to transfer a call on hold to a still ringing (unanswered) call. The individual at the other extension or telephone number does not need to answer to complete the transfer.

The call hold and second call services must be enabled for this service to work. See “Call Hold” on page 311 and “Second Call” on page 311.

4. Enable the Attended Transfer service by setting the *Attended Transfer Activation* drop-down menu to **Enable**.

The attended call transfer service is sometimes called Transfer with Consultation. It allows a user to transfer a call on hold to an active call. The individual at the other extension or telephone number must answer to complete the transfer.

The call hold and second call services must be enabled for this service to work. See “Call Hold” on page 311 and “Second Call” on page 311.

5. Click *Submit* if you do not need to set other parameters.

Using Blind Call Transfer

The following is the procedure to use this service on the user’s telephone.

To configure the SIP Blind Transfer Method, see “SIP Blind Transfer Method” on page 345.

► **To transfer a current call blind:**

1. Perform a Flash-Hook by pressing the “Flash” button on your analog telephone.

   This puts the call on hold.

2. Wait for the transfer tone (three “beeps”).
3. Dial the number to which you want to transfer the call.
4. Wait for the ringback tone, then hang up your telephone.

   The call is transferred.

   Once the transfer is executed, the remaining calls (call on hold and ringing call with third party) are then connected together. The call on hold is automatically unheld and hears the ringback tone provided by the third party's ringing.

   You can also wait for the third party to answer if you want. In this case, the call transfer becomes attended.

   If you want to get back to the first call (the call on hold), you must perform a Flash-Hook.

   You are back with the first call and the third party is released.

Using Attended Call Transfer

The following is the procedure to use this service on the user’s telephone.

► **To transfer a current call attended:**

1. Perform a Flash-Hook by pressing the “Flash” button on your analog telephone.

   This puts the call on hold.

2. Wait for the transfer tone (three “beeps”).
3. Dial the number to which you want to transfer the call.

   The third party answers.

4. Hang up your telephone.

   The call is transferred.

5. If you want to get back to the first call (the call on hold), you must perform a Flash-Hook before the target answers.

   You are back with the first call and the third party is released.

> **Note:** If the number to which you want to transfer the call is busy or does not answer, perform a Flash-Hook. The busy tone or ring tone is cancelled and you are back with the first call.

Call Waiting

The call waiting tone indicates to an already active call that a new call is waiting on the second line.

Your users can activate/deactivate the call waiting tone for their current call. This is especially useful when transmitting faxes. The user that is about to send a fax can thus deactivate the call waiting tone to ensure that the fax transmission will not be disrupted by an unwanted second call. When the fax transmission is completed and the line is on-hook, the call waiting tone is automatically reactivated.

▶ To set the Call Waiting services:

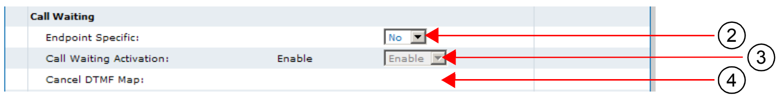
1. Select to which endpoint you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

You have the choice between *Default* and all FXS endpoints your Aastra unit has.

2. In the *Call Waiting* sub-section, define whether or not you want to override the call waiting parameters set in the *Default* configuration in the *Endpoint Specific* drop-down menu.

This menu is available only in the specific endpoints configuration.

Figure 140: Call Waiting Section



3. Enable the service by setting the *Call Waiting Activation* drop-down menu to **Enable**.

This permanently activates the call waiting tone. When receiving new calls during an already active call, a special tone is heard to indicate that a call is waiting on the second line. The user can then answer that call by using the “flash” button. The user can switch between the two active calls by using the “flash” button.

The call hold service must be enabled for this service to work. See “Call Hold” on page 311.

If the user is exclusively using faxes, select **Disable** to permanently disable the call waiting tone.

4. Define the digits that users must dial to disable the Call Waiting tone in the *Cancel DTMF Map* field.

This field is available only in the *Default* configuration.

This allows a user who has call waiting enabled to disable that service on the next call only. If, for any reason, the user wishes to undo the cancel, unhook and re-hook the telephone to reset the service.

For instance, you could decide to put “*76” as the sequence to disable the call waiting tone. This sequence must be unique and follow the syntax for DTMF maps (see “Chapter 35 - DTMF Maps Configuration” on page 401). Dialing this DTMF map does not have any effect unless the service’s status is “enabled”.

The deactivating sequence is set for all the endpoints of the Aastra unit. You cannot have a different sequence for each endpoint.

5. Click *Submit* if you do not need to set other parameters.

Using Call Waiting

The call waiting feature alerts the user if he or she is already on the telephone and a second call happens. A “beep” (the call waiting tone) is heard and repeated every ten seconds to indicate there is a second incoming call.

▶ To put the current call on hold:

1. Perform a Flash-Hook by pressing the “Flash” button on your analog telephone.

This puts the call on hold and the second line is automatically connected to your line.

2. Answer the call on the second line.

▶ To switch from one line to the other:

1. Perform a Flash-Hook each time you want to switch between lines.

▶ To terminate the first call before answering the second call:

1. Hang up the telephone.

2. Wait for the telephone to ring.

3. Answer the telephone.

The second call is on the line.

Removing the Call Waiting Tone

You can temporarily deactivate the call waiting tone indicating a call is waiting. This is especially useful when transmitting faxes. If you are about to send a fax, you can thus deactivate the call waiting tone to ensure that the fax transmission is not disrupted by an unwanted second call. When the fax transmission is completed and the line is on-hook, the call waiting tone is automatically reactivated.

► **To deactivate the call waiting tone:**

1. Take the receiver off-hook.
2. Wait for the dial tone.
3. Dial the sequence implemented to deactivate the call waiting tone.

   This sequence could be something like *76.
4. Wait for the transfer tone (three “beeps”) followed by the dial tone.

   The call waiting tone is disabled.

IMS-3GPP Communication Waiting

Upon receipt of a SIP INVITE with multipart/mixed content where a valid IMS communication waiting indicator is correctly specified such as in this example:

```
INVITE sip:...
[...]
Content-Type: multipart/mixed;boundary=boundary1
[...]

--boundary1
Content-Type: application/vnd.3gpp.cw+xml
Content-Disposition: render;handling=optional

<?xml version="1.0"?>
<ims-cw xmlns="urn:3gpp:ns:cw:1.0">
<communication-waiting-indication/>
</ims-cw>

--boundary1
Content-Type: application/sdp

[...]

--boundary1--
```

The 180 Ringing response to this may contain a special header :

```
Alert-Info: <urn:alert:service:call-waiting>
```

that is appended if all of the following are true :

1. The INVITE contained the <communication-waiting-indication/> 3GPP option.
2. The destination endpoint supports call waiting.
3. The call waiting feature is enabled for this endpoint.
4. The endpoint is currently in an active state (not ringing, not on hold, not on hook).

   There are no variables to control this behaviour, it is always activated.

   This header could be used by the server to notify the 2^{nd} caller that the destination is currently busy in a call but was notified of this new incoming call.

Conference

Note: It is recommended to use the conferencing functionality provided in the MX-ONE.

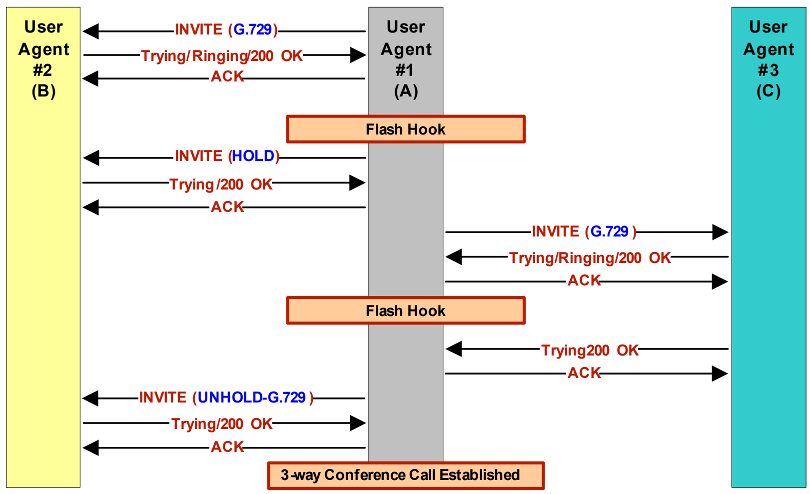
The Conference Call service allows a user to link two or more calls together to form a single conversation, called a conference.

- Only 3-way conferences are currently supported.
- A participant of the conference can put the conference on hold and attempt other calls. This participant may then rejoin the conference at a later time by unholding it. The participant who initiated the conference cannot put it on hold.

You must enable the call hold, second call and attended call transfer services for this service to work. See "Call Hold" on page 311, "Second Call" on page 311, and "The Call Transfer service offers two ways to transfer calls:" on page 301.

The following is a conference call flow example:

Figure 141: Conference Call Flow



DSP Limitation

The Aastra Ta7102i model suffer from a limitation of their DSPs. When using a codec other than G.711, enabling Secure RTP (SRTP) and/or using conferences has an impact on the Aastra unit's overall performance as SRTP and conferences require CPU power. That is the reason why there is a limitation on the lines that can be used simultaneously, depending on the codecs enabled and SRTP. This could mean that a user picking up a telephone on these models may not have a dial tone due to lack of resources in order to not affect the quality of ongoing calls. See "Security" on page 201 for more details on SRTP limitations.

The DSPs offer channels as resources to the Aastra unit. The Aastra unit is limited to two conferences per DSP.

Please note that:

- One FXS line requires one channel.
- Each conference requires one additional channel
- The TA7102i has one DSP
-

A total of eight channels per DSP are available when using unsecure communication, to be used between the FXS lines and up to two conferences.

A total of six channels per DSP are available when using SRTP, to be used between the FXS lines and up to two conferences.

Enabling the Conference Call Feature

You must enable this service before your users can use it.

▶ **To enable the Conference service:**

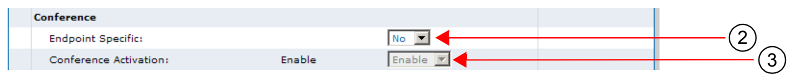
1. Select to which endpoint you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

   You have the choice between *Default* and all FXS endpoints your Aastra unit has.

2. In the *Conference* sub-section, define whether or not you want to override the conference parameters set in the *Default* configuration in the *Endpoint Specific* drop-down menu.

   This menu is available only in the specific endpoints configuration.

Figure 142: Conference Section



3. Enable the service by setting the *Conference Activation* drop-down menu to **Enable**.

4. Click *Submit* if you do not need to set other parameters.

Using an External Server for the Conference

Standards Supported	• RFC 4579: Session Initiation Protocol (SIP) - Call Control - Conferencing for User Agents[a]

a. Partially compliant. Only call flows of sections 5.4 and 5.6 are supported. RFC 4575 is not supported.

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

The Aastra unit can use an external server to mix the media of the conference. This conference type requires the configuration of an external server. Using this type of conference does not affect the number of simultaneous calls supported. You can use this feature only if the Conference service is enabled (see "Enabling the Conference Call Feature" on page 305 for more details).

You can use two types of configuration:

- Default configurations that apply to all the endpoints of the Aastra unit.
- Specific configurations that override the default configurations.

  You can define specific configurations for each endpoint in your Aastra unit. For instance, you could enable a codec for all the endpoints of the Aastra unit and use the specific configuration parameters to disable this same codec on one specific endpoint.

Using one or more specific parameter usually requires that you enable an override variable and set the specific configuration you want to apply.

▶ **To use a server-based conference:**

1. In the *EpServMIB*, specify how to manage the conference by setting the `defaultConferenceType` variable to the proper value.

   You can also use the following line in the CLI or a configuration script:

   This configuration only applies to a conference initiated by one of the unit's endpoint.

   ```
   EpServ.defaultConferenceType="Value"
   ```

where *Value* may be one of the following:

Table 234: Conference Type Parameters

Value	Parameter	Description
100	Local	The media of the conference is locally mixed by the unit. This conference type does not require any special support of the call peer or server. Using this type of conference can reduce the number of simultaneous calls supported.
200	ConferenceServer	The unit uses an external server to mix the media of the conference. This conference type requires the configuration of an external server (See Step 3). Using this type of conference does not affect the number of simultaneous calls supported.

In Local mode, the number of participants is limited to the unit's model capacity. In ConferenceServer mode, the number of participants is limited by the server's capacity.

2. If you want to set a different conference type for one or more endpoints, set the following variables:
   - `epSpecificConferenceEnableConfig` variable for the specific endpoint you want to configure to **enable**.
   - `epSpecificConferenceType` variable for the specific endpoint you want to configure to the proper value.

   You can also use the following lines in the CLI or a configuration script:

   ```
   EpServ.epSpecificConference.EnableConfig[Id="Specific_Endpoint"]="1"
   EpServ.epSpecificConference.Type[Id="Specific_Endpoint"]="Type"
   ```

   where:
   - *Specific_Endpoint* is the number of the endpoint you want to configure.
   - *Value* is the type as defined in Step 1.
3. If you have set the Conference type to **ConferenceServer**, in the *SipEpMIB*, set the `defaultConferenceType` variable with the URI used in the request-URI of the INVITE sent to the conference server as defined in RFC 4579.

   You can also use the following line in the CLI or a configuration script:

   ```
   SipEp.DefaultStaticConferenceServerUri="URI"
   ```
4. If you want to set a different URI for one or more endpoints, set the following variables:
   - `GwSpecificConferenceEnableConfig` variable for the specific endpoint you want to configure to **enable**.
   - `GwSpecificConference`ServerUri variable for the specific endpoint you want to configure to the proper value.

   You can also use the following lines in the CLI or a configuration script:

   ```
   EpServ.GwSpecificConference.EnableConfig[Id="Specific_Endpoint"]="1"
   EpServ.GwSpecificConference.ServerUri[Id="Specific_Endpoint"]="URIValue"
   ```

   where:
   - *Specific_Endpoint* is the number of the endpoint you want to configure.
   - *URIValue* is the URI you want to use.

Managing a Conference Call

If you are on the telephone with one person and want to conference with a third one, you can do so. In the following examples, let’s assume that:

- “A” is the conference initiator.

- "B" is the person called on the first line.
- "C" is the person called on the second line.
- "D" is a fourth person that "A" wants to add to the conference in **conferenceServer** conference type.
- "E" is a fifth person that "C" wants to add to the conference in **conferenceServer** conference type.

To initiate a three-way conference ("A" and "B" already connected):

1. "A" performs a Flash-Hook.

   This puts "B" on hold and the second line is automatically connected. "A" hears a dial tone.
2. "A" dials "C's" number.

   "A" and "C" are now connected.
3. "A" performs another Flash-Hook.

   The call on hold ("B") is reactivated. "A" is now conferencing with "B" and "C".

"B" (or "C") hangs up during the conference:

1. "B" (or "C") hangs up during the conference.

   The conference is terminated, but the call between "A" and "C" (or "B") is not affected and they are still connected.

"A" (conference initiator) hangs up during the conference:

1. "A" hangs up.

   The conference is terminated, both call "C" and "B" are also terminated.

"A" wants to add a fourth member to the conference:

This is available only in the **conferenceServer** conference type.

1. "A" performs a Flash-Hook.

   "A" hears a dial tone. The second line is automatically connected. "B" and "C" are still in conference.
2. "A" dials "D's" number.

   "A" and "D" are now connected.
3. "A" performs another Flash-Hook.

   "A" is now conferencing with "B", "C", and "D".

"C" wants to add a fifth member to the conference:

This is available only in the **conferenceServer** conference type.

1. "C" performs a Flash-Hook.

   "C" hears a dial tone. The second line is automatically connected. "A ", "B " and "D " are still in conference.
2. "C" dials "E's" number.

   "C" and "E" are now connected.
3. "C" performs another Flash-Hook.

   "E" is now conferencing with "A ", "B", "C", and "D".

Delayed Hot Line

The delayed hot line feature (also called warm line) is used to make an automatic call to a specified address on the two following conditions:

- When the user picks up the phone but does not dial any digit. The configured destination is automatically called upon picking up the phone and after waiting for the configurable number of seconds without dialling.

- When the user starts dialing but does not complete a valid number before the timeout set in the *Delayed Hotline Condition* drop-down menu expires.

The condition on which the delayed hotline is activated is configurable. This feature thus places an automatic call whenever the *Delayed Hotline Condition* timeout expires. It could be used as an alternative to the emergency number (for instance, the 911 number in North America).

▶ To configure the basic delayed hot line feature:

1. Select to which endpoint you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

You have the choice between *Default* and all FXS endpoints your Aastra unit has.

2. In the *Delayed Hotline* sub-section, define whether or not you want to override the delayed hotline parameters set in the *Default* configuration in the *Endpoint Specific* drop-down menu.

This menu is available only in the specific endpoints configuration.

Figure 143: Delayed Hotline Section

3. Enable the service by setting the *Delayed Hotline Activation* drop-down menu to **Enable**.

When the feature is disabled, a user picking up the phone but not pressing any telephone keys hears the Receiver Off-Hook tone after the amount of time specified in the *digitMapTimeoutFirstDigit* variable.

4. Click *Submit* if you do not need to set other parameters.

▶ To configure the delayed hotline activation condition:

1. In the *Delayed Hotline* sub-section, select the condition(s) that activate the delayed hotline in the *Delayed Hotline Condition* drop-down menu.

Figure 144: Delayed Hotline Section

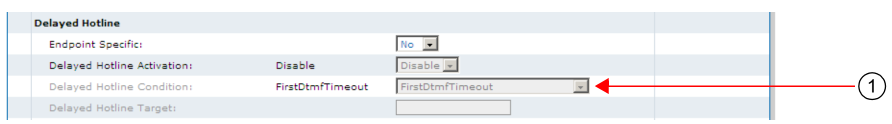


Table 235: Delayed Hotline Conditions

Parameter	Description
FirstDtmfTimeout	The delayed hotline is activated when the timeout configured in the *First DTMF Timeout* field of the *Telephony > DTMF Maps* page elapses ("General DTMF Maps Parameters" on page 404).
InterDtmfOrCompletionTimeout	The delayed hotline is activated when the timeout configured in the *Completion Timeout* field of the *Telephony > DTMF Maps* page elapses or when the DTMFs collection fails because the *Inter DTMF Timeout* parameter elapses ("General DTMF Maps Parameters" on page 404).

Table 235: Delayed Hotline Conditions (Continued)

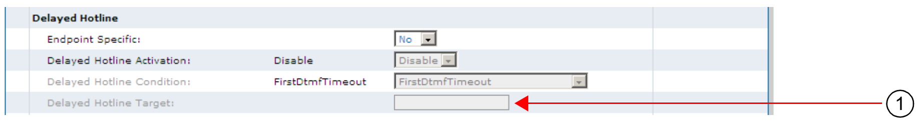
Parameter	Description
AnyTimeout	The delayed hotline is activated when the timeout configured in the *Completion Timeout* field of the *Telephony > DTMF Maps* page elapses and when the DTMFs collection fails because the *Inter DTMF Timeout* parameter elapses (“General DTMF Maps Parameters” on page 404).

2. Click *Submit* if you do not need to set other parameters.

▶ **To configure the delayed hotline target:**

1. In the *Delayed Hotline* sub-section, set the destination (address or telephone number) that is automatically called in the *Delayed Hotline* field.

Figure 145: Delayed Hotline Section



Accepted formats are:

- telephone numbers (5551111)
- SIP URLs such as ”scheme:user@host”. For instance, “sip:user@foo.com”.

This string is used literally, so cosmetic symbols (such as the dash in “555-xxxx”) should not be present.

2. Click *Submit* if you do not need to set other parameters.

Direct IP Address Call

The IP address call service allows a user to dial an IP address without the help of a SIP server. Using this method bypasses any server configuration of your unit.

The user can dial an IP address and enter an optional telephone number. Note that the optional telephone number is matched by using the same digit maps as a normal call.

The IP address call method can be used when a SCN user wants to reach a LAN endpoint.

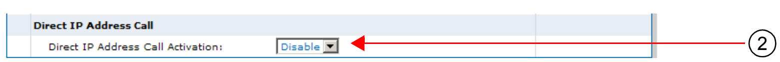
▶ **To set the direct IP call feature:**

1. Select to which endpoint you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

This menu is available only in the default endpoints configuration.

2. Enable the service by setting the *Direct IP Address Call* drop-down menu to **Enable**.

Figure 146: Telephony – Direct IP Address Call Section



Dialing an IP Address

▶ **To make an IP address call:**

1. Dial “**” (IP address prefix).

2. Dial the numerical digits of the IP address and use the “*” for the “.” of the IP address.

3. Dial “*” to terminate the IP address if you do not need to specify a phone number.

For instance, let's say you want to reach a one-line access device or another LAN endpoint such as an IP Phone with the IP address 192.168.0.23. You must then dial the following digits:

`**192*168*0*23*`

4. If you need to specify the phone number of a specific line, dial "#" to terminate the IP address.
5. Dial the telephone number of the specific line you want to reach.

For example, let's say you want to reach the telephone connected to Line 2 of the Aastra unit with the IP address 192.168.0.23. The phone number assigned to Line 2 of this Aastra unit is 1234. You must then dial the following digits:

`**192*168*0*23#1234`

In this case, the Aastra unit sends an INVITE *1234@192.168.0.23*.

Call Hold

The Call Hold service allows the user to temporarily put an existing call on hold, usually by using the "flash" button of the telephone. The user can resume the call in the same way.

You must enable this service for the following services to work properly:

- Call Waiting
- Second Call
- Blind Transfer
- Attended Transfer
- Conference

To enable the Call Hold service:

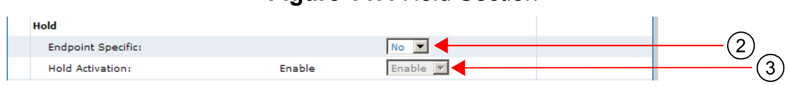
1. Select to which endpoint you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

   You have the choice between *Default* and all FXS endpoints your Aastra unit has.

2. In the *Hold* sub-section, define whether or not you want to override the call hold parameters set in the *Default* configuration in the *Endpoint Specific* drop-down menu.

   This menu is available only in the specific endpoints configuration.

Figure 147: Hold Section



3. Enable the service by setting the *Hold Activation* drop-down menu to **Enable**.
4. Click *Submit* if you do not need to set other parameters.

Using Call Hold

The following is the procedure to use this service on the user's telephone.

To put the current call on hold:

1. Perform a Flash-Hook by pressing the "Flash" button on your analog telephone.

   This puts the call on hold. You can resume the call in the same way.

Second Call

The Second Call service allows a user with an active call to put the call on hold, and then initiate a new call on a second line. This service is most useful with the transfer and conference services.

The call hold service must be enabled for this service to work. See "Call Hold" on page 311.

You must enable this service for the following services to work properly:

- Blind Transfer

- Attended Transfer
- Conference

To enable the Second Call service:

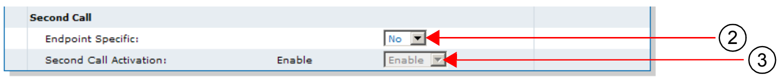
1. Select to which endpoint you want to apply the changes in the *Select Endpoint* drop-down menu at the top of the window.

   You have the choice between *Default* and all FXS endpoints your Aastra unit has.

2. In the *Second Call* sub-section, define whether or not you want to override the second call parameters set in the *Default* configuration in the *Endpoint Specific* drop-down menu.

   This menu is available only in the specific endpoints configuration.

Figure 148: Second Call Section



3. Enable the service by setting the *Second Call Activation* drop-down menu to **Enable**.
4. Click *Submit* if you do not need to set other parameters.

Using Second Call

The following is the procedure to use this service on the user’s telephone.

To use the second call service:

1. Perform a Flash-Hook by pressing the “Flash” button on your analog telephone.

   This puts the call on hold and the second line is automatically connected to your line.

2. Initiate the second call.

Message Waiting Indicator

Standards Supported	• RFC 3265: Session Initiation Protocol (SIP)-Specific Event Notification[a] • RFC 3842: The Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)[b]

a. Supports receiving blind NOTIFY without subscribing. Sending blind NOTIFY is not supported.

b. Supports receiving blind NOTIFY without subscribing. Sending blind NOTIFY is not supported.

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

The Message Waiting Indicator (MWI) service alerts the user when new messages have been recorded on a voice mailbox. It is enabled by default.

After the message is recorded, the server sends a message (SIP NOTIFY request) to the Aastra unit listing how many new and old messages are available. The Aastra unit alerts the user of the new message in two different ways:

- The telephone’s LED blinks (if present). A FSK signal is sent on the FXS line.
- A message waiting stutter dial tone replaces the normal dial tone when the user picks up the

FXS line.

> **Note:** The message waiting state does not affect the Second Call feature. When in an active call, performing a flash-hook to get access to the second line plays the usual dial tone.

The Aastra unit supports to receive SIP MWI notifications via SIP NOTIFY requests as defined in RFC 3842 but with the following limitations/diversions:

- In addition to the SIP event string "message-summary" (RFC 3842), the string "simple-message-summary" is accepted. The significations of those strings are identical.
- In addition to the SIP content type string "simple-message-summary" (RFC 3842), the string "message-summary" is accepted. The significations of those strings are identical.
- Support of message-summary is not advertised in the SIP REGISTER.

Note that received SIP NOTIFY with an event different than "message-summary" or "simple-message-summary" is not interpreted as a valid MWI notification.

You can use two types of configuration:

- Default configurations that apply to all the endpoints of the Aastra unit.
- Specific configurations that override the default configurations.

  You can define specific configurations for each endpoint in your Aastra unit. For instance, you could enable a codec for all the endpoints of the Aastra unit and use the specific configuration parameters to disable this same codec on one specific endpoint.

Using one or more specific parameter usually requires that you enable an override variable and set the specific configuration you want to apply.

To disable the Message Waiting Indicator service:

1. In the *potsMIB*, set the `fxsDefaultMessageWaitingIndicatorActivation` variable to the proper value.

   You can also use the following line in the CLI or a configuration script:

   ```
   pots.fxsDefaultMessageWaitingIndicatorActivation="100"
   ```

   If you want to reactivate the feature, use the following:

   ```
   pots.fxsDefaultMessageWaitingIndicatoreActivation="Value"
   ```

   where *Value* may be one of the following:

Table 236: Message Waiting Indicator Parameters

Value	Parameter	Description
100	Disabled	The user is not alerted of messages awaiting attention.
200	Tone	When messages are awaiting attention, the user is alerted by a message waiting tone when picking up the handset.
300	Visual	When messages are awaiting attention, the user is alerted by a Visual Message Waiting Indicator such as a blinking LED on the phone.
400	ToneAndVisual	When messages are awaiting attention, the user is alerted by a Visual Message Waiting Indicator such as a blinking LED on the phone, and a message waiting tone when picking up the handset.

2. If you want to set a different activation for one or more endpoints, set the following variables:

   - `fxsSpecificMessageWaitingIndicatorEnableConfig` variable for the specific endpoint you want to configure to **enable**.
   - `fxsSpecificMessageWaitingIndicatorActivation` variable for the specific endpoint you want to configure to the proper value.

   You can also use the following lines in the CLI or a configuration script:

   ```
   pots.fxsSpecificMessageWaitingIndicator.EnableConfig[Id="Specific_Endpoint"]="1"
   ```

```
pots.fxsSpecificMessageWaitingIndicator.Activation[Id="Specific_Endpoint"]="Valu
e"
```

where:

- *Specific_Endpoint* is the number of the endpoint you want to configure.
- *Value* is the activation as defined in Step 1.

Visual Message Waiting Indicator Type

You can configure how the Visual Message Waiting Indicator is sent on FXS lines.

▶ **To configure the visual message waiting indicator type:**

1. In the *potsMIB*, set the `fxsDefaultVisualMessageWaitingIndicatorType` variable to the proper value.

You can also use the following line in the CLI or a configuration script:

```
pots.fxsDefaultVisualMessageWaitingIndicatorType="Value"
```

where *Value* may be one of the following:

Table 237: Visual Message Waiting Indicator Type Parameters

Value	Parameter	Description
100	Fsk	A FSK signal is sent to activate the VMWI on the phone.
200	FskAndVoltage	Both FSK signal and high voltage signal are used to activate the VMWI on the phone. **Note:** This parameter applies only to the following models: TA7102i

Emergency Call Override

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

You can override the set of services that are activated during an emergency call.

▶ **To set the emergency call override:**

1. In the *epServMIB*, set the *defaultEmergencyCallOverride* variable to the proper value.

You can also use the following line in the CLI or a configuration script:

```
epServ.defaultEmergencyCallOverride="Value"
```

where *Value* may be one of the following:

Table 238: Emergency Call Override Parameters

Value	Parameter	Description
100	NoOverride	The set of services for emergency calls remains the same as configured.
200	NoServices	Ignores any service requiring a flash-hook. Call waiting and all other related services are deactivated.

Call Statistics

This section describes how to access data available only in the MIB parameters of the Aastra unit. You can display these parameters as follows:

- by using a MIB browser
- by using the CLI

The following are the call statistics the Aastra unit keeps. Statistics are updated at the end of each call.

Table 239: Call Statistics

MIB Variable	Statistics Description
IncomingCallsReceived	Number of incoming IP calls received on the endpoint since service start.
IncomingCallsAnswered	Number of incoming IP calls answered on the endpoint since service start.
IncomingCallsConnected	Number of incoming IP calls that successfully completed call setup signaling on the endpoint since service start.
IncomingCallsFailed	Number of incoming IP calls that failed to complete call setup signaling on the endpoint since service start.
OutgoingCallsAttempted	Number of outgoing IP calls attempted for the endpoint since service start.
OutgoingCallsAnswered	Number of outgoing IP calls answered by the called party for the endpoint since service start.
OutgoingCallsConnected	Number of outgoing IP calls that successfully completed call setup signaling for the endpoint since service start.
OutgoingCallsFailed	Number of outgoing IP calls that failed to complete call setup signaling for the endpoint since service start.
CallsDropped	Number of IP calls, on the endpoint since service start, that were successfully connected (incoming or outgoing), but dropped unexpectedly while in progress without explicit user termination.
TotalCallTime	Cumulative duration of all IP calls on the endpoint since service start, in seconds.

To display call statistics:

1. In the *epServMIB*, go to the *CallStatistics* table.

   You can also use the following line in the CLI:

   `get epServ.callStatistics`

To reset call statistics values to zero:

1. In the *epServMIB*, set `callStatistics.Reset` to *Reset* for the endpoint to reset.

   You can also use the following line in the CLI:

   `set epServ.callStatistics.Reset=Reset`

2. In the *epServMIB*, set `callStatistics[EplId=callStatisticsEpId].Reset` to *Reset* to reset only one specific endpoint.

   where:

   - `callStatisticsEpId` is the string that identifies the combination of an endpoint and a channel. The endpoint name is the same as the `EpId` used to refer to endpoints in other tables. On endpoints with multiple channels, the channel number must be appended at the end of the endpoint name, separated with a dash.

You can also use the following line in the CLI:

```
set epServ.callStatistics[EplId=callStatisticsEpId].Reset=Reset
```

Examples:

`Slot3/E1T1-12` refers to endpoint Slot3/E1T1, channel 12.

`Phone-Fax1` refers to FXS endpoint Phone-Fax1 on a 4102s.

`Port06` refers to FXS endpoint Port06 on 4108/4116/4124.

No channel number is appended to FXS endpoint strings because FXS lines do not support multiple channels.

Default Outbound Priority Call Routing

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

You can define how to route priority calls including emergency calls.

To set the default outbound priority call routing:

1. In the *sipEpMIB*, set the *defaultOutboundPriorityCallRouting* variable to the proper value.

   You can also use the following line in the CLI or a configuration script:

   ```
   sipEp.defaultOutboundPriorityCallRouting="Value"
   ```

   where *Value* may be one of the following:

Table 240: Default Outbound Priority Call Routing Parameters

Value	Parameter	Description
100	Normal	Sends the call using normal SIP call routing to the outbound proxy (if defined) and to the target host (usually the SIP server).
200	SkipOutbound Proxy	Sends the call directly to the configured server skipping the outbound proxy.

C H A P T E R

35

Tone Customization Parameters Configuration

This chapter describes how to override the pattern for a specific tone defined for the selected country (see “Appendix A - Country-Specific Parameters” on page 603 for more details). It covers the following topics:

- Current Tone Definition
- Tone Override

Current Tone Definition

The *Tone Customization* page allows you to both see the current definition and override the pattern of the following tones:

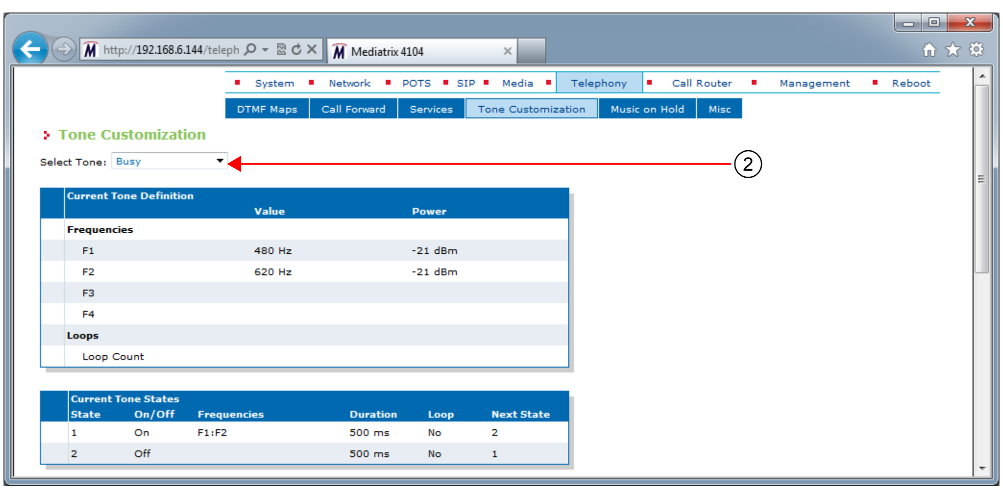
- Busy
- Call Waiting
- Confirmation
- Congestion
- Dial
- Hold
- Intercept
- Message Waiting
- Preemption
- Reorder
- Ringback
- Receiver Off Hook (ROH)
- Special Information Tone (SIT)
- Stutter

This includes the number of frequencies used, the tone value in Hertz (Hz), its power in dBm, as well as the states configured.

To see the current definition of a tone:

1. In the web interface, click the *Telephony* link, then the *Tone Customization* sub-link.

Figure 149: Telephony – Tone Customization Web Page



2. Select the proper tone to see in the *Select Tone* drop-down menu at the top of the window.

The *Current Tone Definition* and *Current Tone States* sections describe the current definition of the selected tone.

Tone Override

You can override the pattern for a specific tone. This is done in two sections:

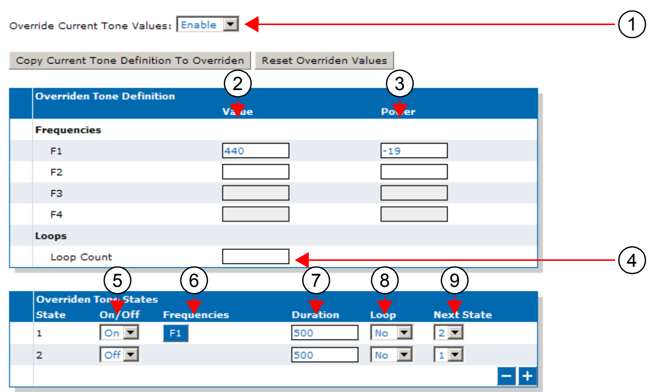
Table 241: Tone Override Sections

State	Description
Overridden Tone Definition	Allows you to define up to four frequencies (F1 to F4). You must enter at least one frequency.
Overridden Tone States	Description of the tone state. You can define up to eight states. You must enter at least one state.

▶ **To override the pattern of a tone:**

1. Select which tone you want to override in the *Override Current Tone Values* drop-down menu.

Figure 150: Tone Override Sections



- You can use the current values of the selected tone as a starting point for your customization by clicking the *Copy Current Tone Definition to Overridden* button.
- You can clear all override fields by clicking the *Reset Overridden Values* button.

2. In the *Overridden Tone Definition* section, define the value of the proper Frequency used in the corresponding *Value* field.

The value is in Hz. The range is from 10 Hz to 4000 Hz.

> **Note:** You can use only two frequencies for the Call Waiting tone.

3. Define the power level of the proper Frequency in dBm in the corresponding *Power* field.

The range is from -99 dBm to 3 dBm.

4. If applicable, enter a value for the loop counter in the *Loop Count* field.

The range is from 2 to 128. This value will be used in Step 8.

> **Note:** You can use only one loop count for the Call Waiting tone.

5. In the *Overridden Tone States* section, set the corresponding *On/Off* drop-down menu with the proper value for each state.

- **On** means the corresponding state plays a tone.
- **Off** means the corresponding state does not play a tone.
- **CID** means the moment where the Caller-ID will be sent to the analog port. This options is available only for the Call Waiting tone.

You may also want to perform the following operations:

- To add a state, click the  button at the bottom of the *Overridden Tone States* section.
- To remove a state, click the  button at the bottom of the *Overridden Tone States* section. This removes the last state in the list.

6. For the On states, select the frequency to play in the corresponding *Frequencies* column.

The frequencies defined in the *Overridden Tone Definition* section are listed as clickable buttons. You can use from one to four frequencies. A blue button indicates that the frequency is selected.

7. Set the corresponding *Duration* field with the number of times, in ms, to perform the action of the state.

The range is from 10 ms to 56000 ms. The tone stays indefinitely in the state (continuous) if no time is specified.

8. In the corresponding *Loop* drop-down menu, select whether or not to stop looping between states after a number of loops defined in Step 4.

When the number of loops is reached, the next state is s(n+1) for the state s(n) instead of the state defined in the *Next State* drop-down menu.

9. In the corresponding *Next State* drop-down menu, select the next tone state to use when the time has elapsed.

This value is not available if the *Duration* field is empty.

10. Click *Submit* if you do not need to set other parameters.

CHAPTER

36

Music on Hold Parameters Configuration

This chapter describes how to configure the Music on Hold (MoH) parameters.

- MP3 file download server setup.
- Music on Hold configuration.

Standards Supported	• RFC 1350: The TFTP Protocol (Revision 2) (client-side only) • RFC 2616: Hypertext Transfer Protocol - HTTP/1.1 (client-side only)

MP3 File Download Server

To download a MP3 file, you may need to setup the following applications on your computer:

- TFTP server with proper root path
- HTTP server with proper root path

Configuring the TFTP Server

When you perform a MP3 file download by using the TFTP (Trivial File Transfer Protocol) protocol, you must install a TFTP server running on the PC designated as the TFTP server host. It is assumed that you know how to set the TFTP root path. If not, refer to your TFTP server's documentation.

Configuring the HTTP Server

When you to perform a MP3 file download by using the HTTP protocol, you must install a HTTP server running on the PC designated as the server host. It is assumed that you know how to set the root path. If not, refer to your HTTP server's documentation.

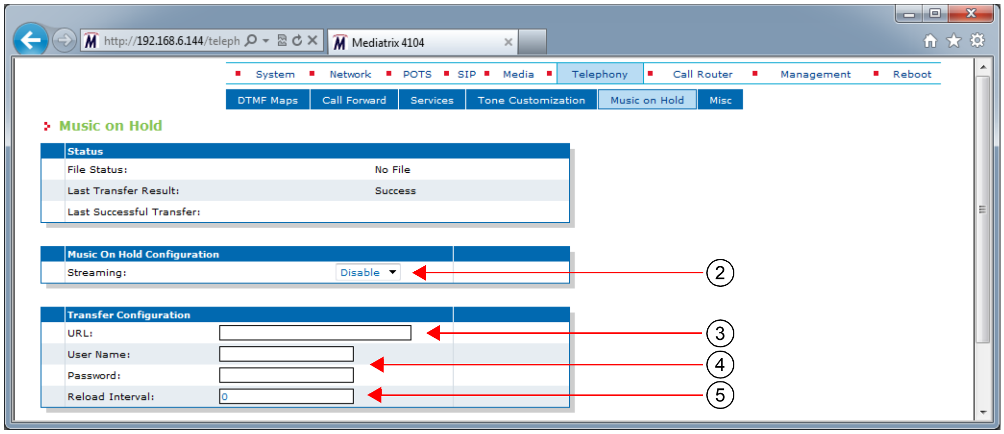
Music on Hold Configuration

The *Music on Hold* sub-page of the *Telephony* page allows you to configure the music (in the form of an MP3 file) that plays when a local user has been put on hold. Note that transfers exceeding 5 minutes are cancelled.

▶ To set the Music on Hold parameters:

1. In the web interface, click the *Telephony* link, then the *Music on Hold* sub-link.

Figure 151: Telephony – Music on Hold Web Page



2. In the *Music On Hold Configuration* section, indicate whether or not the unit should play music when being put on hold in the *Streaming* drop-down menu.

When enabled, music is played toward the telephony side when being put on hold from the network side.

3. In the *Transfer Configuration* section, enter the URL to the MP3 file to use in the *URL* field.

This file is loaded when the Aastra unit starts and reloaded every time the *Reload Interval* value elapses (see Step 5). It must be smaller than 1024 Kilobytes unless otherwise specified in a customer profile.

The MP3 file downloaded must be encoded with a sampling rate of 8000 Hz (only available through MPEG version 2.5) and in mono channel mode. All other types of file will be rejected. The decoding output will be in mono channel mode, with a sample rate of 8000 Hz and with 8 bits per sample.

You can use the following supported protocols to transfer the file:

- HTTP: HyperText Transfer Protocol.
- TFTP: Trivial File Transfer Protocol.

URLs using any other transfer protocol are invalid.

Note: The HTTP protocol does not support spaces between characters in the URL.

Examples of valid URLS:

- http://www.myserver.com/myfile.mp3
- tftp://myserver.com:69/myfolder/myfile.mp3

When the port is not included in the URL, the default port for the chosen protocol is used.

HTTP supports basic or digest authentication mode as described in RFC 2617.

If you have selected HTTP, please note that your server may activate some caching mechanism for the MP3 download. This mechanism caches the initial MP3 download for later processing, thus preventing changes of the original MP3.

4. If your server requires authentication when downloading the MP3, set the following:

- The user name in the *User Name* field.
- The password in the *Password* field.

Caution: The *User Name* and *Password* fields are not accessible if you have the User or Observer access right. See "Users" on page 591 for more details.

5. Set the time, in hours, between attempts to load the MP3 file in the *Reload Interval* field.

   If you enter the value **0**, this means that the unit loads the file only once at unit startup. Any other value between 1 and 6000 is the number of hours between automatic reloads of the file. When a manual file download is triggered, the counter is not reset so the next reload will happen at the same time.

6. If you do not need to set other parameters, do one of the following:

   - To save your settings without transferring the MP3 file, click *Submit*.
   - To save your settings and transfer the MP3 file now, click *Submit & Transfer Now*.
   - To save your settings and stop a file transfer in progress, click *Submit & Cancel Transfer*.

C H A P T E R

37

Country Parameters Configuration

This chapter describes how to configure the country information:

- Select a specific country.
- Additional country settings.
- Call Detail Record

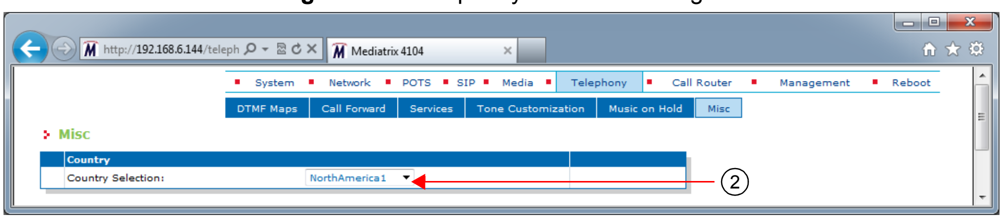
Country Configuration

The *Misc* sub-page of the *Telephony* page allows you to configure the country in which the unit is located.

To set the miscellaneous parameters:

1. In the web interface, click the *Telephony* link, then the *Misc* sub-link.

Figure 152: Telephony – Misc Web Page



2. In the *Country* section, select the country in which the Aastra unit is located in the *Country Selection* drop-down menu.

   It is very important to set the country in which the unit is used because a number of parameter values are set according to this choice, such as tones, rings, impedances, and line attenuations. See "Appendix A - Country-Specific Parameters" on page 603 for more information on these country-specific settings.

3. Click *Submit* if you do not need to set other parameters.

Additional Country Settings

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

Default vs. Specific Configurations

You can use two types of configuration:

- Default configurations that apply to all the endpoints of the Aastra unit.
- Specific configurations that override the default configurations.

  You can define specific configurations for each endpoint in your Aastra unit. For instance, you could enable a codec for all the endpoints of the Aastra unit and use the specific configuration parameters to disable this same codec on one specific endpoint.

Using one or more specific parameter usually requires that you enable an override variable and set the specific configuration you want to apply.

Input/Output User Gain

The user gain allows you to modify the input and output sound level of the Aastra unit.

> **Caution:** Use these settings with great care. Aastra recommends not to modify the user gain variables unless absolutely necessary because default calibrations may no longer be valid.
>
> Modifying user gains may cause problems with DTMF detection and voice quality – using a high user gain may cause sound saturation (the sound is distorted). Furthermore, some fax or modem tones may no longer be recognized. The user gains directly affect the fax communication quality and may even prevent a fax to be sent.

You can compensate with the user gain if there is no available configuration for the country in which the Aastra unit is located. Because the user gain is in dB, you can easily adjust the loss plan, e.g., if you need an additional 1 dB for analog to digital, put 1 for user gain output.

You can use two types of configuration as described in "Default vs. Specific Configurations" on page 326.

▶ To set user gain variables:

1. In the *telIfMIB*, locate the *countryCustomizationUserGainGroup* folder.
2. Define the default user output gain offset in dB (from analog to digital) in the `defaultCountryCustomizationUserGainOutputOffset` variable.

   You can also use the following line in the CLI or a configuration script:

   ```
   telIf.defaultCountryCustomizationUserGainOutputOffset="Value"
   ```

   Values range from -12 dB to +12 dB. However, going above +6 dB may introduce clipping/distortion depending on the country selected.
3. If you want to set a different output gain offset for one or more interfaces, set the following variables:
   - `specificCountryCustomizationUserGainEnableConfig` variable for the specific interface you want to configure to **enable**.
   - `specificCountryCustomizationUserGainOutputOffset` variable for the specific line you want to configure.

   You can also use the following lines in the CLI or a configuration script:

   ```
   telIf.specificCountryCustomizationUserGain.EnableConfig[InterfaceId="Interface"]
   ="1"
   telIf.specificCountryCustomizationUserGain.OutputOffset[InterfaceId="Interface"]
   ```

`="Value"`

where:

- *Interface* is the name of the interface you want to configure (for instance, Slot2/Pri1).
- *Value* is the output gain offset.

4. Define the default user input gain offset in dB (from digital to analog) in the `defaultCountryCustomizationUserGainInputOffset` variable.

You can also use the following line in the CLI or a configuration script:

```
telIf.defaultCountryCustomizationUserGainInputOffset="Value"
```

Values range from -12 dB to +12 dB. However, going above +6 dB may introduce clipping/distortion depending on the country selected.

5. If you want to set a different input gain offset for one or more interfaces, set the following variables:

- `specificCountryCustomizationUserGainEnableConfig` variable for the specific interface you want to configure to **enable**.
- `specificCountryCustomizationUserGainInputOffset` variable for the specific line you want to configure.

You can also use the following lines in the CLI or a configuration script:

```
telIf.specificCountryCustomizationUserGain.EnableConfig[InterfaceId="Interface"]
="1"
telIf.specificCountryCustomizationUserGain.InputOffset[InterfaceId="Interface"]=
"Value"
```

where:

- *Interface* is the name of the interface you want to configure (for instance, Slot2/Pri1).
- *Value* is the input gain offset.

6. Restart the *TelIf* service by accessing the *scmMIB* and setting the `serviceCommandsRestart` variable for the *TelIf* service to **restart**.

You can also use the following line in the CLI or a configuration script:

```
scm.serviceCommands.Restart[Name=TelIf]="10"
```

Dialing Settings

Dialing settings allow you to configure how the Aastra unit dials numbers.

When selecting a country (see “Country Configuration” on page 325 for more details), each country has default dialing settings. However, you can override these values and define your own dialing settings.

You can use two types of configuration as described in “Default vs. Specific Configurations” on page 326.

▶ **To set the dialing settings:**

1. In the *telIfMIB*, locate the *countryCustomizationDialingGroup* folder.

2. Set the `defaultCountryCustomizationDialingOverride` variable to **enable**.

You can also use the following line in the CLI or a configuration script:

```
telIf.specificCountryCustomizationDialing.EnableConfig[InterfaceId="Interface"]=
"1"
```

where *Interface* is the name of the interface you want to configure (for instance, Slot2/Pri1).

This allows overriding the default country settings.

3. If you want to change the override status for one or more interfaces, set the following variables:

- `specificCountryCustomizationDialingEnableConfig` variable for the specific interface you want to configure to **enable**.
- `specificCountryCustomizationDialingOverride` variable for the specific interface you want to configure to **enable**.

You can also use the following lines in the CLI or a configuration script:

```
telIf.specificCountryCustomizationDialing.EnableConfig[InterfaceId="Interface"]=
"1"
telIf.specificCountryCustomizationDialing.Override[InterfaceId="Interface"]="1"
```

where *Interface* is the name of the interface you want to configure (for instance, Slot2/Pri1).

4. Set an inter-digit dial delay in the `defaultCountryCustomizationDialingInterDtmfDialDelay` variable.

You can also use the following line in the CLI or a configuration script:

```
telIf.defaultCountryCustomizationDialing.InterDtmfDialDelay="Value"
```

This is the delay, in milliseconds (ms), between two DTMFs when dialing the destination phone number. Values range from 50 ms to 600 ms.

5. If you want to set a different inter-digit dial delay for one or more interfaces, set the following variables:

- `specificCountryCustomizationDialingEnableConfig` variable for the specific interface you want to configure to **enable**.
- `specificCountryCustomizationDialingInterDtmfDialDelay` variable for the specific interface you want to configure.

You can also use the following lines in the CLI or a configuration script:

```
telIf.specificCountryCustomizationDialing.EnableConfig[InterfaceId="Interface"]=
"1"
telIf.specificCountryCustomizationDialing.InterDtmfDialDelay[InterfaceId="Slot3/
Bri3"]="Value"
```

where *Interface* is the name of the interface you want to configure (for instance, Slot2/Pri1).

6. Set the DTMF duration value in the `defaultCountryCustomizationDialingDtmfDuration` variable.

You can also use the following line in the CLI or a configuration script:

```
telIf.defaultCountryCustomizationDialing.DtmfDuration="Value"
```

This is the duration, in milliseconds (ms), a DTMF is played when dialing the destination phone number. Values range from 50 ms to 600 ms.

7. If you want to set a different DTMF duration value for one or more interfaces, set the following variables:

- `specificCountryCustomizationDialingEnableConfig` variable for the specific interface you want to configure to **enable**.
- `specificCountryCustomizationDialingDtmfDuration` variable for the specific interface you want to configure.

You can also use the following lines in the CLI or a configuration script:

```
telIf.specificCountryCustomizationDialing.EnableConfig[InterfaceId="Interface"]=
"1"
telIf.specificCountryCustomizationDialing.DtmfDuration[InterfaceId="Interface"]=
"Value"
```

8. Set the delay, in milliseconds, between two MFR1s when dialing on the interface in the `DefaultCountryCustomizationDialingInterMfR1DialDelay` variable.

See “Chapter 23 - E&M CAS Configuration” on page 253 for more details on MFR1 signalling.

You can also use the following line in the CLI or a configuration script:

9. Set the delay, in milliseconds, between two MFR1s when dialing on the interface by putting the following line in the configuration script:

```
telIf.defaultCountryCustomizationDialing.InterMfR1DialDelay="Value"
```

Values range from 50 ms to 600 ms.

10. If you want to set a different delay value for one or more interfaces, set the following variables:

```
telIf.specificCountryCustomizationDialing.EnableConfig[InterfaceId="Interface"]=
```

```
"1"
telIf.specificCountryCustomizationDialing.InterMfR1DialDelay[InterfaceId="Interf
ace"]="Value"
```

11. Set the duration, in milliseconds, of a MFR1 when dialling on the interface in the `DefaultCountryCustomizationDialingMfR1Duration` variable.

    See "Chapter 23 - E&M CAS Configuration" on page 253 for more details on MFR1 signalling.

    You can also use the following line in the CLI or a configuration script:

12. Set the duration, in milliseconds, of a MFR1 when dialing on the interface by putting the following line in the configuration script:

    ```
    telIf.DefaultCountryCustomizationDialing.MfR1Duration="Value"
    ```

    Values range from 50 ms to 600 ms.

13. If you want to set a different duration value for one or more interfaces, set the following variables:

    ```
    telIf.specificCountryCustomizationDialing.EnableConfig[InterfaceId="Interface"]=
    "1"
    telIf.specificCountryCustomizationDialing.MfR1Duration[InterfaceId="Interface"]=
    "Value"
    ```

14. Restart the *TelIf* service by accessing the *scmMIB* and setting the `serviceCommandsRestart` variable for the *TelIf* service to **restart**.

    You can also use the following line in the CLI or a configuration script:

    ```
    scm.serviceCommands.Restart[Name=TelIf]="10"
    ```

Fax Calling Tone Detection

You can enable the fax calling tone (CNG tone) detection.

You can use two types of configuration as described in "Default vs. Specific Configurations" on page 326.

▶ **To enable fax calling tone detection:**

1. In the *telIfMIB*, locate the *machineDetectionGroup* folder.
2. Set the `defaultMachineDetectionCngToneDetection` variable to **enable**.

   You can also use the following line in the CLI or a configuration script:

   ```
   telIf.defaultMachineDetection.CngToneDetection="1"
   ```

   Upon recognition of the CNG tone, the Aastra unit switches the communication from voice mode to fax mode and the CNG is transferred by using the preferred fax codec. This option allows for quicker fax detection, but it also increases the risk of false detection.

   If you do not want the Aastra unit to detect the fax calling tone, set the variable to **disable(0)**. In this case, the CNG tone does not trigger a transition from voice to data and the CNG is transferred in the voice channel. With this option, faxes are detected later, but the risk of false detection is reduced.

3. If you want to set a different calling tone detection setting for one or more interfaces, set the following variables:

   - `specificMachineDetectionEnableConfig` variable for the specific interface you want to configure to **enable**.
   - `specificMachineDetectionCngToneDetection` variable for the specific interface you want to configure.

   You can also use the following lines in the CLI or a configuration script:

   ```
   telIf.specificMachineDetection.EnableConfig[InterfaceId="Interface"]="1"
   telIf.specificMachineDetection.CngToneDetection[InterfaceId="Interface"]="Value"
   ```

CDR (Call Detail Record)

Call detail record (CDR) in VoIP contains information about recent system usage such as the identities of sources (points of origin), the identities of destinations (endpoints), the duration of each call, the total usage time in the billing period and many others.

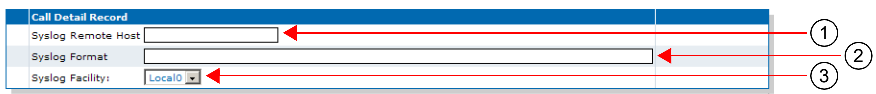
The *Misc* sub-page of the *Telephony* page allows you to configure the CDR parameters.

▶ **To set the CDR parameters:**

1. In the *Call Detail Record* section of the *Misc* page, set the host name and port number of the device that archives CDR log entries in the *Syslog Remote Host* field.

   Specifying no port (or port 0) sends notifications to port 514.

Figure 153: CDR Call Detail Record Section



2. Specify the format of the syslog Call Detail Record in the *Syslog Format* field.

   The formal syntax description of the protocol is as follows:

```
Precision=DIGIT
Width=DIGIT
MacroId=(ALPHA / "_")
Macro=%[Width]|[.Precision]|[Width.Precision]MacroId
```

The *Width* field is the minimum width of the converted argument. If the converted argument has fewer characters than the specified field width, then it is padded with spaces. If the converted argument has more characters than the specified field width, the field width is extended to whatever is required.

The *Precision* field specifies the maximum number of characters to be printed from a string. Examples :

```
sipid=SipUser001
CDR Log: %sipid      --> CDR Log : SipUser001
CDR Log: %15sipid    --> CDR Log : SipUser001
CDR Log: %15.5sipid --> CDR Log : SipUs
CDR Log: %.5sipid    --> CDR Log : SipUs
```

Call Detail Record predefined macros.

Control characters:

Table 242: Control Character

Character	Value
%%	%
\n	Split message

Call detail record macros:

Table 243: Call Detail Record Macros

Macro	Value
%id	CDR ID. The CDR ID is unique. The ID is incremented by one each time it is represented in a CDR record
%sipid	SIP call ID. Blank if no SIP interface was used during the call.
%ocgnum	Original calling number. Calling number as received by the unit.
%cgnum	Calling number. Calling number after manipulation by the call router.

Table 243: Call Detail Record Macros (Continued)

Macro	Value
%ocdnum	Original called number. Called number as received by the unit.
%cdnum	Called number. Called number after manipulation by the call router.
%oiname	Original Interface name. Interface on which the call was received. Ex. isdn-Slot2/ Pri1.
%diname	Destination interface name. Interface on which the call was relayed. Ex. SIP-Default
%chan	Channel number. Blank if no PRI/BRI interface was used during the call. If 2 PRI/ BRI interface were involved, display the originating interface.
%sipla	SIP local IP address.
%sipra	SIP remote IP address or FQDN (next hop).
%siprp	SIP remote port (next hop).
%mra	Media remote IP address. Source IP address of incoming media stream. If the stream was modified during the call, display the last stream.
%mrsp	Media remote port. Source port of incoming media stream. If the stream was modified during the call, display the last stream.
%mdrp	Media remote port. Destination port of outgoing media stream. If the stream was modified during the call, display the last stream.
%tz	Local time zone
%cd	Call duration (in seconds) (connect/disconnect).
%sd	Call duration (in seconds) (setup/connect).
%pdd	Post dial delay (in seconds) (setup/progress).
%css	Call setup second (local time)
%csm	Call setup minute (local time)
%csh	Call setup hour (local time)
%csd	Call setup day (local time)
%csmm	Call setup month (local time)
%csy	Call setup year (local time)
%ccs	Call connect second (local time)
%ccm	Call connect minute (local time)
%cch	Call connect hour (local time)
%ccd	Call connect day (local time)
%ccmm	Call connect month (local time)
%ccy	Call connect year (local time)
%cds	Call disconnect second (local time)
%cdm	Call disconnect minute (local time)
%cdh	Call disconnect hour (local time)
%cdd	Call disconnect day (local time)
%cdmm	Call disconnect month (local time)

Table 243: Call Detail Record Macros (Continued)

Macro	Value
%cdy	Call disconnect year (local time)
%miptxc	IP Media last transmitted codec
%miptxp	IP Media last transmitted p-time
%dr	Disconnect reason (ISDN reason codes with ISUP SIP mapping)
%rxp	Received media packets. Excluding T.38.
%txp	Transmitted media packets. Excluding T.38.
%rxpl	Received media packets lost. Excluding T.38.
%rxmd	Received packets mean playout delay (ms, 2 decimals). Excluding T.38.
%rxaj	Received packets average jitter (ms, 2 decimals). Excluding T.38.
%sipdr	SIP disconnect or rejection reason.

3. Set the Syslog facility used by the unit to route the Call Detail Record messages in the *Syslog Facility* field.

The application can use *Local0* through *Local7*.

4. Click *Submit* if you do not need to set other parameters.

Call Router Parameters

Page Left Intentionally Blank

CHAPTER
38

Call Router Configuration

This chapter describes the call router service.

- Introduction to the call router's parts and types supported.
- Routes parameters.
- Mappings parameters.
- Call signalling parameters.
- SIP headers translation parameters.
- Call properties translation parameters.
- Hunt table parameters.
- SIP Redirects parameters.

Standards Supported	• ITU-T Recommendation E.164: The international public telecommunication numbering plan. • ITU-T Recommendation F.69: List of Telex Destination Codes. • ITU-T Recommendation X.121: International numbering plan for public data networks.

Introduction

The Aastra unit's call router allows you to route calls between interfaces. Based on a set of routing criteria, the call router determines the destination (interface) for every incoming call. The forwarding decisions are based on the following tables:

Table 244: Call Router Table Types

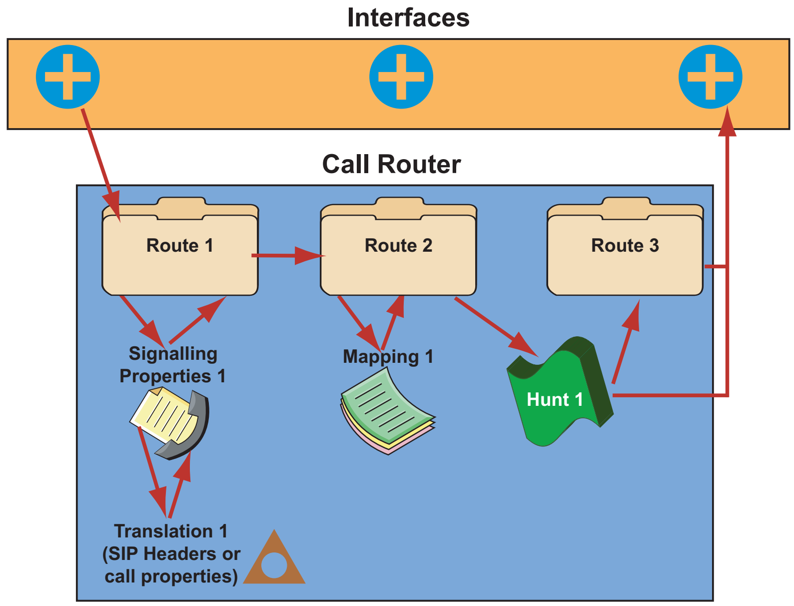
Table	Description
Routing	The routing table contains one or more routes. Each route associates a destination to a call that matches a set of criteria. See "Routes" on page 353 for more details.
Mapping	The mapping table contains one or more mapping types and expressions. A mapping modifies call properties such as the calling and called party numbers according to the network requirements. These mappings are specifically called within a route. See "Mappings" on page 358 for more details.
Call Signalling	Call signalling specifies how to set up a call to the destination Aastra unit or 3rd party equipment. Call signalling properties are assigned to a route and used to modify the behaviour of the call at the SIP protocol level. See "Signalling Properties" on page 368 for more details.
SIP Headers Translation	A SIP headers translation overrides the default value of SIP headers in an outgoing SIP message. See "SIP Headers Translations" on page 372 for more details.
Call Properties Translation	A call properties translation overrides the default value of call properties in an incoming SIP message. See "Call Properties Translations" on page 376 for more details.

Table 244: Call Router Table Types (Continued)

Table	Description
Hunt	The hunt table contains one or more hunt entries, each with a set of possible destinations. A hunt tries the destinations until one of the configured destinations accepts the call. See “Hunt Service” on page 379 for more details.
SIP Redirects	The SIP Redirects table allows configuring of SIP redirections that can be used as Route destinations. When the Route source is a SIP interface, incoming SIP Invites are replied with a 302 “Moved Temporarily” SIP response. See “SIP Redirects” on page 387 for more details.

When a new call comes from one of the Aastra unit interfaces, it is redirected to the routing table. The following figure illustrates the Aastra unit call router:

Figure 154: Call Routing



Limitations

The call routing service has the following limitations:

- A call coming from a SIP interface cannot be routed to another SIP interface. When that occurs, the call automatically fails.
- A call automatically fails if it is redirected to a route or hunt more than 10 times.
- Maximum number of Routes: 40
- Maximum number of Mapping Types: 40
- Maximum number of Mapping Expressions: 100
- Maximum number of Hunts: 40
- Maximum number of Signaling Properties: 40
- Maximum number of SIP Header Translations: 100
- Maxium number of Call Properties Translations: 100

Regular Expressions

Standards Supported	• IEEE Std 1003.1-2001: IEEE Standard for Information Technology---Portable Operating System Interface (POSIX®)

Some of the routing types described in “Routing Type” on page 338 require that you enter them following the regular expression syntax. A regular expression is a string used to find and replace strings in other large strings. The Aastra unit uses regular expressions to enter a value in several routing types, often by using wildcard characters. These characters provide additional flexibility in designing call routing and decrease the need for multiple entries in configuring number ranges.

The expression cannot begin by “^”, it is implicit in the expression. The following table shows some of the wildcard characters that are supported:

Table 245: Regular Expressions Wildcards

Character	Description
.	Single-digit place holder. For instance, `555 ....` matches any dialed number beginning with 555, plus at least four additional digits. Note that the number may be longer and still match.

*	Repeats the previous digit 0, 1, or more times. For instance, in the pattern:
	`1888*1`
	the pattern matches:
	`1881, 18881, 188881, 1888881`
	Note: If you are trying to handle the asterisk (*) as part of a dialed number, you must use `\*`.

[ ]	Range of digits. • A consecutive range is indicated with a hyphen (-), for instance, `[5-7]`. • A nonconsecutive range is indicated without a delimiter, for instance, `[58]`. • Both can be used in combination, for instance `[5-79]`, which is the same as `[5679]`. You may place a (^) symbol right after the opening bracket to indicate that the specified range is an exclude list. For instance, `[^01]` specifies the same range as `[2-9]`. **Note:** The call router only supports single-digit ranges. You cannot specify the range of numbers between 99 and 102 by using `[99-102]`.
( )	Indicates a pattern (also called group), for instance, `555(2525)`. It is used when replacing a number in a mapping. See “Groups” on page 337 for more details.
?	Matches 0 or 1 occurrence of the previous item. For instance, `123?4` matches both `124` and `1234`.
+	Repeats the previous digit one or more time. For instance `12+345` matches `12345`, `122345`, etc. (but not `1345`). If you use the + at the end of a number, it repeats the last number one or more times. For instance: `12345+` matches, `12345`, `123455`, `1234555`, etc.
|	Indicates a choice of matching expressions (OR).

The matching criterion implicitly matches from the beginning of the string, but not necessarily up to the end. For instance, `123` will match the criterion `1`, but it will not match the criterion `2`.

If you want to match the whole string, you must end the criterion with “$”. For instance, `123` will not match the criterion `1$` and will match the criterion `123$`.

Note: You can use the “<undefined>” string if you want to match a property that is not defined.

You can also use the macro “local_ip_port“ to replace the properties by the local IP address and port of the listening network of the SIP gateway used to send the INVITE.

Groups

A group is placed within parenthesis. It is used when replacing a string in a mapping. You can use up to nine groups (defined by “\1” to “\9”) and matching is not case sensitive. “\0” represents the whole string. Lets say for instance you have the following string:

```
9(123(45)6)
```

The following describes how the groups are replaced in a properties manipulation:

Table 246: Groups Replacement Example

Replacement	Result
\0	9123456
\1	123456
\2	45
\3	

Groups can only be used with the following routing types:

- Calling/Called E.164
- Calling/Called Name
- Calling/Called Host
- Calling/Called URI

Routing Type

Standards Supported	• ITU-T Recommendation Q.931: ISDN user-network interface layer 3 specification for basic call control

The following sub-sections list the available routing types of the call router and their supported values. The routing types that offer choices use the choices as defined in the Q.931 standard. Q.931 is ISDN’s connection control protocol, roughly comparable to TCP in the Internet protocol stack. The values may also be a special tag, as described in “Special Tags” on page 344.

Table 247: Routing Types Locations

Routing Type	Location
E164	“Called / Calling E164” on page 339
Type of Number (TON)	“Called / Calling TON” on page 339
Numbering Plan Indicator (NPI)	“Called / Calling NPI” on page 339
Name	“Called / Calling Name” on page 340
Host	“Called / Calling Host” on page 340
URI	“Called / Calling URI” on page 340
Presentation Indicator (PI)	“Calling PI” on page 340
Screening Indicator (SI)	“Calling SI” on page 340
Information Transfer Capability (ITC)	“Calling ITC” on page 341
Date and Time	“Date/Time” on page 341
Phone Context	“Called / Calling Phone Context” on page 342
SIP Username	“Called / Calling SIP Username” on page 342
Bearer Channel	“Called / Calling SIP Username” on page 342
Diverting Reason	“Last / Original Diverting Reason” on page 342
Diverting E.164	“Last / Original Diverting E.164” on page 343

Table 247: Routing Types Locations (Continued)

Routing Type	Location
Diverting Party Number Type	"Last / Original Diverting Party Number Type" on page 343
Diverting Public Type Of Number	"Last / Original Diverting Public Type Of Number" on page 343
Diverting Pivate Type Of Number	"Last / Original Diverting Private Type Of Number" on page 343
Diverting Number Presentation	"Last / Original Diverting Number Presentation" on page 344
SIP Privacy Type	"SIP Privacy Type" on page 344

Aastra recommends to carefully define the routing requirements and restrictions that apply to your installation before starting the routing configuration. This will help you determine the types of routing you need. When this is done, define the routes and mappings, as well as the hunts that you need to fulfil these requirements. You may need several entries of the same type to achieve your goals.

See also "Call Properties Parameters" on page 344 for a description of the parameters used by the various routing types and interfaces of the call router.

Called / Calling E164

This is the Called/Calling Party Number. You can enter a regular expression (called/calling party E.164 number in the call setup message) as per "Regular Expressions" on page 337. Note that:

- A PBX may insert or modify the calling party number. Sometimes there is no calling party number at all. This all depends on the equipment you connect to the device.
- The Aastra unit cannot filter the redirecting number information element of the SETUP message because it does not support the "calling-Redir-E164" and "Calling-Redir-Reason" routing properties criteria.

Called / Calling TON

Called or calling party type of number field in the ISDN setup message. The following values are available:

Table 248: Type of Number Values

Value	Description
unknown	Unknown number type.
international	International number.
national	National number.
network	Network specific number used to indicate an administration or service number specific to the serving network.
subscriber	Subscriber number.
abbreviated	Abbreviated number.

Note: The called type of number is set to **international** if the *To* username is an E.164 with the prefix "+". The calling type of number is set to **international** if the *From* username is an E.164 with the prefix "+".

Called / Calling NPI

Called or calling party numbering plan indicator field in the ISDN setup message. The following values are available:

Table 249: Numbering Plan Indicator Values

Value	Description
unknown	Unknown numbering plan.
isdn (E.164)	ISDN/Telephony numbering plan according to ITU-T Recommendation E.164.
data (X.121)	Data numbering plan according to ITU-T Recommendation X.121.
telex (F.69)	Telex numbering plan according to ITU-T Recommendation F.69.
national	Numbering plan according to a national standard.
private	A private numbering plan.

Called / Calling Name

Calling and called party name (display name). This is the human-readable name of the calling or called party. See “Regular Expressions” on page 337 for more details on how to enter a proper expression.

The Aastra unit does not support the sending of the calling name in the user-to-user information element.

Called / Calling Host

IP address or domain name of the called or calling host in the following format:

```
Fqdn[:port]
```

If `[:port]` is missing, the call router uses the well-known port of the signalling protocol. Note that:

- Incoming SIP calls use the calling party IP address property to store the IP address of the remote SIP user agent. Other interfaces such as ISDN set the IP address to 0.0.0.0.

  You can use a regular expression to enter an IP address or a range of IP addresses.

Called / Calling URI

Uniform Resource Identifier (URI) of:

- the called party, e.g., the *To-URI*.
- the originating VoIP peer, e.g., the *From-URI* of an incoming SIP call.

The URI follows the format described in RFC 3261.

Calling PI

Presentation indicator of the calling party number. The following values are available:

Table 250: Presentation Indicator Values

Value	Description
allowed	Presentation of the calling party number is allowed.
restricted	Presentation of the calling party number is restricted.
interworking	The calling party number is not available due to interworking.

You may want to remove the calling party number when the user sets the presentation indicator to **restricted**. To achieve this, route restricted calls to a mapping that sets the *Calling E164* to an empty string.

Calling SI

Screening indicator of the calling party number. The following values are available:

Table 251: Screening Indicator Values

Value	Description
not-screened	The user provides the calling party number but the number is not screened by the network. Thus the calling party possibly sends a number that it does not own.
passed	The calling party number is provided by the user and it passes screening.
failed	The calling party number is set by the user and verification of the number failed.
network	The originating network provides the number in the calling party number parameter.

You may want to remove the calling party number when it is not screened or screening failed. To do so, route these calls to a mapping that sets the *Calling E164* to an empty string. If you want to drop calls when the calling party number is not screened or screening failed, use the *Calling Si* as criteria for the route.

Calling ITC

The information transfer capability field of the bearer capability information element in the ISDN setup message. The following values are available:

Table 252: Information Transfer Capability Values

Value	Description
speech	Voice terminals (telephones).
unrestricted	Unrestricted digital information (64 kbps).
restricted	Restricted digital information (64 kbps).
3.1Khz	Transparent 3.1 kHz audio channel.
udi-ta	Unrestricted digital information with tones/announcements. **Note:** This was formerly transparent 7.1 kHz audio channel.
video	Video conference terminals.

The Aastra unit currently supports the following Information Transfer Capabilities when receiving calls to and from the ISDN (named as in Q.931, 05/98):

- Speech
- Unrestricted Digital Information
- 3.1 kHz Audio

Those are respectively referenced as *Speech*, *Unrestricted* and *3.1 kHz* in the call routing configuration.

When initiating calls towards the ISDN, the Aastra unit uses the calling ITC value if it is one of the three listed above. If none is set, it uses 3.1 kHz Audio. If the calling ITC set by the call router is different from the three listed above, the call is rejected.

> **Note:** Terminals connected to analog extensions (e.g. of a PBX) do not supply information transfer capability values in their call setup. The configuration of the analog port on the Terminal Adapter, NT or PBX is thus responsible to insert this value. The configuration of this value is however often omitted or wrong. The ITC value may therefore not be a reliable indication to differentiate between analogue speech, audio or Fax Group 3 connections. Furthermore, calls from SIP interfaces do not differentiate between bearer capabilities. They always set the information transfer capability property to **3.1Khz**.

Date/Time

Day of week and time period and/or date and time period. The following are the accepted formats:

Table 253: Date/Time Accepted Formats

Format	Description
Date/Time Period format	• 'DD.MM.YYYY/HH:MM:SS-DD.MM.YYYY/HH:MM:SS' • 'DD.MM.YYYY/HH:MM:SS-HH:MM:SS' • 'DD.MM.YYYY-DD.MM.YYYY' • 'DD.MM.YYYY' • 'HH:MM:SS-HH:MM:SS'
Week Day/Time Period format	• 'DDD' • 'DDD,DDD...' • 'DDD/HH:MM:SS-HH:MM:SS' • 'DDD,DDD.../HH:MM:SS-HH:MM:SS' DDD must be one of: SUN, MON, TUE, WED, THU, FRI, SAT.

Many of the formats above can be concatenated to form one expression. They must be separated by |. For instance: `25.12.2006 | SUN`.

Called / Calling Phone Context

This is a user parameter in a URI. For instance:

```
sip:1234;phone-context=1234@domain.com;user=phone
```

You can enter a regular expression (called/calling party phone context in the call setup message) as per "Regular Expressions" on page 337.

Called / Calling SIP Username

Calling and called party SIP username. See "Regular Expressions" on page 337 for more details on how to enter a proper expression.

Called / Calling Bearer Channel

Calling and called party bearer channel. See "Regular Expressions" on page 337 for more details on how to enter a proper expression.

Last / Original Diverting Reason

Standards Supported	• RFC 5806: Diversion Indication in SIP

This is the last or original diverting reason in ISDN setup and SIP INVITE messages. The following values are available:

Table 254: Diverting Reason Values

Value	Description
cfb	Call Forward on Busy – Allowed.
cfu	Call Forward on Unavailable – Restricted
cfnr	Call Forward on No Answer – Interworking
unknown	unknown

Refer to "You can set the SIP transfer method when an endpoint is acting as the transferor in a blind transfer scenario." on page 345 to select the SIP method used to receive/send call diversion information in an INVITE.

Last / Original Diverting E.164

Last or original party number to which the call was being routed when the first diversion occurred. You can enter a regular expression (called/calling party E.164 number in the call setup message) as per "Regular Expressions" on page 337. Note that:

- A PBX may insert or modify the calling party number. Sometimes there is no calling party number at all. This all depends on the equipment you connect to the device.
- The Aastra unit cannot filter the redirecting number information element of the SETUP message because it does not support the "calling-Redir-E164" and "Calling-Redir-Reason" routing properties criteria.

Last / Original Diverting Party Number Type

The following values are available:

Table 255: Diverting Party Number Type Values

Value	Description
unknown	Unknown number type.
public	Public number.
private	Private number.

Last / Original Diverting Public Type Of Number

Diverting or original called number public type of number field in the ISDN Setup message. Used only when the diverting or original called number type of number is 'public'. The following values are available:

Table 256: Diverting Public Type of Number Values

Value	Description
unknown	Unknown number type.
international	International number.
national	National number.
network-specific	Network specific number used to indicate an administration or service number specific to the serving network.
subscriber	Subscriber number.
abbreviated	Abbreviated number.

Last / Original Diverting Private Type Of Number

Diverting or original called number private type of number field in the ISDN Setup message. Used when the diverting or original called party number type is 'private'. The following values are available:

Table 257: Diverting Private Type of Number Values

Value	Description
unknown	Unknown.
leg2-reg	Leg2 reg.
leg1-reg	Leg1 reg.

Table 257: Diverting Private Type of Number Values (Continued)

Value	Description
pisn-specific	PISN Specific.
subscriber	Subscriber number.
abbreviated	Abbreviated number.

Last / Original Diverting Number Presentation

Diverting or original called number presentation. The following values are available:

Table 258: Diverting Presentation Values

Value	Description
allowed	Presentation of the party number is allowed.
restricted	Presentation of the party number is restricted.
interworking	The party number is not available due to interworking.
restricted-address	Restricted address.

SIP Privacy Type

Calling SIP privacy level of the call. The following values are available:

Table 259: SIP Privacy Values

Value	Description
disabled	No privacy is used.
none	Use P-Asserted Identity privacy.
id	Use P-Preferred Identity privacy.

Special Tags

You can use the following special tags as routing types values.

Table 260: Special Tags

Tag	Description
undefined	Matches if the property is not defined for the call.
default	Always matches. Generally used to set a default route if the previous criteria do not match.

Call Properties Parameters

The following sections describe the parameters used by the various call properties (routing types) and interfaces of the call router.

Call Properties to SIP

This section describes the information the call router uses for the various SIP fields.

Table 261: Call Properties to SIP

SIP Field	Description
To	The Aastra unit uses the calling URI to populate the *To* field if not undefined. Otherwise, the unit does the following: • Uses the called *Name* for the friendly name if not undefined. • Uses the called *SipUsername* for the user name if not empty or undefined; otherwise, uses the called *E164* for the username. If it is empty or undefined, the Aastra unit rather uses the value defined in the *Default Username Value* field of the *SIP* > *Interop* > *SIP Interop* parameters as username (see "SIP Interop" on page 312 for more details). The unit uses the called *Phone Context* for the user's 'phone-context' parameter if not empty. If a 'phone-context' parameter is added, the URI parameter 'user' is also automatically added. Its value is defined in the *SIP URI User Parameter Value* field of the *SIP* > *Interop* > *SIP Interop* parameters. If empty, then the value 'phone' is used • Uses the called *Host* for the host if not undefined, otherwise uses the configured home domain proxy host. • Prefixes the user name with "+" and adds the URI parameter "user" with the value "phone" if the called TON is "international". • If there is no URI parameter "user" yet and the *SIP URI User Parameter Value* field of the *SIP* > *Interop* > *SIP Interop* parameters is not empty, then the parameter is added with the value defined by the field.
From	The Aastra unit uses the called URI to populate the *From* field if not undefined. Otherwise, the unit does the following: • Uses the calling *Name* for the friendly name if not undefined. • Uses the calling *SipUsername* for the user name if not empty or undefined; otherwise, uses the calling *E164* for the username. If it is empty or undefined, the Aastra unit rather uses the value defined in the *Default Username Value* field of the *SIP* > *Interop* > *SIP Interop* parameters as username (see "SIP Interop" on page 312 for more details).The unit uses the calling *Phone Context* for the user's 'phone-context' parameter if not empty. If a 'phone-context' parameter is added, the URI parameter 'user' is also automatically added. Its value is defined in the *SIP URI User Parameter Value* field of the *SIP* > *Interop* > *SIP Interop* parameters. If empty, then the value 'phone' is used. • Uses the calling *Host* for the host if not undefined, otherwise uses the configured home domain proxy host. • Prefixes the user name with "+" and adds the URI parameter "user" with the value "phone" if the calling TON is "international". • If there is no URI parameter "user" yet and the *SIP URI User Parameter Value* field of the *SIP* > *Interop* > *SIP Interop* parameters is not empty, then the parameter is added with the value defined by the field.
Request URI	The Aastra unit uses the same information as the *To* field.
Contact	The Aastra unit uses the same information as the *From* field, but with the current IP address/port for the host.

Table 261: Call Properties to SIP (Continued)

SIP Field	Description

Diversion	A *Diversion* header is added if the *Last Diverting E.164* property is present and not empty. This *Diversion* header is constructed as follows:
	• The *username* of the URI is set to the value of the *Last Diverting E.164* property.
	• The *host* of the URI is set to the configured home domain proxy host.
	• The *reason* field is set according to value of the *Last Diverting Reason* property:
	    • cfu: "unconditional"
	    • cfb: "user-busy"
	    • cfnr: "no-answer"
	    • All other values or when undefined: "unknown'.
	• The field counter is set to the value of *DivertingCounter* if the *Original Diverting E.164* property is set to empty or undefined, otherwise it is set to DivertingCounter -1.
	A second *Diversion* header is added if the *Last Diverting E.164* and *Original Diverting E.164* properties are present and not empty. This *Diversion* header is constructed as follows:
	• The *username* of the URI is set to the value of the *Original Diverting E.164* property.
	• The *host* of the URI is set to the configured home domain proxy host.
	• The *reason* field is set according to the value of the *Original Diverting Reason* property:
	    • cfu: "unconditional"
	    • cfb: "user-busy"
	    • cfnr: "no-answer"
	    • All other values or when undefined: "unknown'.
	The field counter is set to 1.

SIP to Call Properties

This section describes the SIP information the call router uses for the various call properties.

Table 262: SIP to Call Properties

Property	SIP Information
Called URI	The URL of the *To* field.
Calling URI	The URL of the *From* field.
Called Name	The friendly name in the *To* field. The property is undefined if there is no friendly name.
Calling Name	The friendly name in the *From* field. The property is undefined if there is no friendly name.
Called E164	The user name of the *Request-Uri* field if the user name is a compatible E.164. The prefix “+” and separator “-” are removed. The property is undefined if there is no user name or if it is not compatible.
Calling E164	The user name of the *From* field if the user name is a compatible E.164. The prefix “+” and separator “-” are removed. The property is undefined if there is no user name or if it is not compatible.
Called Host	The host of the *To* field.

Table 262: SIP to Call Properties (Continued)

Property	SIP Information
Calling Host	The host of the *Contact* field.
Called TON	Set to “international” if the *To* user name is an E.164 with the prefix “+”; otherwise, the property is undefined.
Calling TON	Set to “international” if the *From* user name is an E.164 with the prefix “+”; otherwise the property is undefined.
Called Phone Context	Set to the parameter “phone-context” of the user name of the *To* if the user name is an E.164, otherwise the property is undefined.
Calling Phone Context	Set to the parameter “phone-context” of the user name of the *From* if the user name is an E.164, otherwise the property is undefined.
Called SIP Username	Set to the username of the *Request-Uri*. Note that this does not include the username parameter like the “phone-context”.
Calling SIP Username	Set to the username of the *From*. Note that this does not include the username parameter like the “phone-context”.
Last Diverting Reason	If the INVITE contains at least one *Diversion* header, this value is set according to the *reason* field value of the first *Diversion* header: • "user-busy": cfb • "unconditional":cfu • "no-answer": cfna • All other values: unknown Otherwise, the property is undefined. The *reason* field comparison is not case sensitive.
Original Diverting Reason	If the INVITE contains more than one *Diversion* header, this value is set according to the *reason* field value of the last *Diversion* header: • "user-busy": cfb • "unconditional":cfu • "no-answer": cfna • All other values: unknown Otherwise, the property is undefined. The *reason* field comparison is not case sensitive.
Last Diverting E.164	If the INVITE contains at least one *Diversion* header, this value is set to the *username* of the URI (can be a SIP URI, SIPS URI or TEL URI) of the first *Diversion* header converted into an E.164. It can be set to empty if there is no username or if the username is not an E.164. Otherwise, the property is undefined.
Original Diverting E.164	If the INVITE contains more than one *Diversion* header, this value is set to the *username* of the URI (can be a SIP URI, SIPS URI or TEL URI) of the last *Diversion* header converted into an E.164. It can be set to empty if there is no username or if the username is not an E.164. Otherwise, the property is undefined.
Diverting Counter	If the INVITE contains at least one *Diversion* header, this value is set to the sum of the *counter* field of all *Diversion* headers. If a diversion header does not contain the *counter* field, the value 1 is assumed for the header.
All others	The property is undefined.

Call Properties to ISDN

This section describes the information the call router uses for the various ISDN information elements.

Table 263: Call Properties to ISDN

Information Element	Description
Bearer Capabilities	If valid, the *calling ITC* is used to fill the “information transfer capability” (octet 3 [5:1]). Otherwise, the ITC is set to “3.1 kHz audio”. If more than one bearer capability information elements is provided in a prioritized list, they all receive the same ITC. This information element is included in the SETUP message only for outgoing calls.
Calling Party Number	Uses the *calling E164* to fill the field “number digits” (octet 4). Uses the *calling TON* to fill the field “type of number” (octet 3 [7:5]). Uses the *calling PI* to fill the field “presentation indicator” (octet 3a [7:6). Uses the *calling SI* to fill the field “screening indicator” (octet 3a [2:1]). Uses the *calling NPI* to fill the field “numbering plan identification” (octet 3 [4:1]).
Called Party Number	Uses the *called E164* to fill the field “number digits” (octet 4). Uses the *called TON* to fill the field “type of number” (octet 3 [7:5]). Uses the *called NPI* to fill the field “numbering plan identification” (octet 3 [4:1]).
Display	Uses the *calling E164* to fill the field “display information” (octet 3).
Called Bearer Channel	The called bearer channel is used to select a specific ISDN bearer channel for an outgoing ISDN call.

ISDN to Call Properties

This section describes the ISDN information the call router uses for the various call properties.

Table 264: ISDN to Call Properties

Property	ISDN Information
Calling Name	Field “display information” (octet 3) of the Display information element, if included in the SETUP Q.931 message.
Called E164	Field “number digits” (octet 4) of the called party information element included in the SETUP Q.931 message.
Calling E164	Field “number digits” (octet 4) of the calling party information element included in the SETUP Q.931 message.
Called TON	Field “type of number” (octet 3 [7:5]) of the called party information element included in the SETUP Q.931 message.
Calling TON	Field “type of number” (octet 3 [7:5]) of the calling party information element included in the SETUP Q.931 message.
Calling PI	Field “presentation indicator” (octet 3a [7:6) of the calling party information element included in the SETUP Q.931 message.
Calling SI	Field “screening indicator” (octet 3a [2:1]) of the calling party information element included in the SETUP Q.931 message.
Calling ITC	Field “information transfer capability” (octet 3 [5:1]) of the bearer capability information element included in the SETUP Q.931 message.
Called NPI	Field “numbering plan identification” (octet 3 [4:1]) of the called party information element included in the SETUP Q.931 message.
Calling NPI	Field “numbering plan identification” (octet 3 [4:1]) of the calling party information element included in the SETUP Q.931 message.

Table 264: ISDN to Call Properties (Continued)

Property	ISDN Information
Calling Bearer Channel	Represents the ISDN bearer channel on which the ISDN call is received.
All others	The property is undefined.

Call Properties to FXS

This section describes the information the call router uses for the various call properties to FXS.

Table 265: Call Properties to FXS

Caller ID	Description
Number	If the PI property is present and not set to "allowed", the number is "P". Otherwise, the number is set to the value of the *E164* property (truncated to the first 20 characters). See "Auto-Routing" on page 517 for details.
Name	If the PI property is present and not set to "allowed", the name is "Anonymous". Otherwise, the name is set to the value of the *Name* property (truncated to the first 50 characters). See "Auto-Routing" on page 517 for details.

FXS to Call Properties

This section describes the information the call router uses for the various FXS to call properties.

Table 266: FXS to Call Properties

Caller ID	Description
Calling E164	If the auto routing is enabled and the *E164* field of the *Call Router > Auto-routing* page is not empty (see "Auto-Routing" on page 517 for details), the value of the *E164* field. Otherwise, the property is not present.
Calling Name	If the auto routing is enabled and the *Name* field of the *Call Router > Auto-routing* page is not empty (see "Auto-Routing" on page 517 for details), the value of the *Name* field. Otherwise, the property is not present.
Calling SIP Username	If the auto routing is enabled and the *SIP Username* field of the *Call Router > Auto-routing* page is not empty (see "Auto-Routing" on page 517 for details), the value of the *SIP Username* field. Otherwise, the property is not present.
Called E164	For automatic calls, the E.164 defined in the *Automatic Call Target* field of the *Telephony > Services* page (see "Automatic Call" on page 419 for more details). For other calls, the dialed digit after the transformation defined in the *Transformation* field of the *Allowed DTMF Map* section (*Telephony > DTMF Maps* page – see "Allowed DTMF Maps" on page 405 for more details).
Called Name	For automatic calls, the name specified in the *Automatic Call Target* field of the *Telephony > Services* page (see "Automatic Call" on page 419 for more details). The property is not present if the target address does not contain a name. For other calls, the property is not present.

Table 266: FXS to Call Properties (Continued)

Caller ID	Description
Called Host	For automatic calls, the host specified in the the *Automatic Call Target* field of the *Telephony* > *Services* page (see "Automatic Call" on page 419 for more details). The property is not present if the target address does not contain a host. For other calls, the host defined in the *Target* field of the *Allowed DTMF Map* section (*Telephony* > *DTMF Maps* page – see "Allowed DTMF Maps" on page 405 for more details). The property is not present if the target host is not configured for the matching DTMF map.

Call Properties to FXO

This section describes the information the call router uses for the various call properties to FXO.

Table 267: Call Properties to FXO

Caller ID	Description
Dialled number	The *Called E164* property.

FXO to Call Properties

This section describes the information the call router uses for the various FXO to call properties.

Table 268: FXO to Call Properties

Caller ID	Description
Calling E164	If the caller ID is detected, the numbers provided by the caller ID. If the auto routing is enabled and the *E164* field of the *Call Router* > *Auto-routing* page is not empty (see "Auto-Routing" on page 517 for details), the value of the *E164* field. Otherwise, the property is not present.
Calling Name	If the caller ID is detected, the name provided by the caller ID. If the auto routing is enabled and the *Name* field of the *Call Router* > *Auto-routing* page is not empty (see "Auto-Routing" on page 517 for details), the value of the *Name* field. Otherwise, the property is not present.
Calling SIP Username	If the caller ID is detected, the property is not present. If the auto routing is enabled and the *SIP Username* field of the *Call Router* > *Auto-routing* page is not empty (see "Auto-Routing" on page 517 for details), the value of the *SIP Username* field. Otherwise, the property is not present.
Called E164	For automatic calls, the E.164 defined in the *Automatic Call Target* field of the *Telephony* > *Services* page (see "Automatic Call" on page 419 for more details). For other calls, the dialed digit after the transformation defined in the *Transformation* field of the *Allowed DTMF Map* section (*Telephony* > *DTMF Maps* page – see "Allowed DTMF Maps" on page 405 for more details).
Called Name	For automatic calls, the name specified in the *Automatic Call Target* field of the *Telephony* > *Services* page (see "Automatic Call" on page 419 for more details). The property is not present if the target address does not contain a name. For other calls, the property is not present.

Table 268: FXO to Call Properties (Continued)

Caller ID	Description
Called Host	For automatic calls, the host specified in the the *Automatic Call Target* field of the *Telephony > Services* page (see “Automatic Call” on page 419 for more details). The property is not present if the target address does not contain a host. For other calls, the host defined in the *Target* field of the *Allowed DTMF Map* section (*Telephony > DTMF Maps* page – see “Allowed DTMF Maps” on page 405 for more details). The property is not present if the target host is not configured for the matching DTMF map.

SIP/ISDN Call Default Values

When performing a call from SIP to ISDN or ISDN to SIP, some ISDN informations are missing from the SIP packet. The Dgw v2.0 Application sets the following default values when the information is missing. You cannot filter on these default values, but you can filter with the “<undefined>” or “<default>” values.

Table 269: SIP/ISDN Calls Default Values

Parameter	Default Value
SIP to ISDN Calls	
TON (calling)	**unknown**
TON (called)	**unknown**
NPI (calling and called)	**unknown**
SI (calling)	User-side: **not-screened** Network-side: **network**
ITC (calling)	**3.1 kHz audio**
PI (calling)	**1.** When the Calling Party Number E.164 is missing: **interworking**. In this case, this value overrides any value set by the call router. **2.** When CLIR is enabled (user-side only): **restricted**. In this case, this value overrides any value set by the call router. **3.** All other cases: **allowed**. This is the default value if the two cases above do not apply and no value has been set by the call router.
ISDN to SIP Calls	
SI (calling)	Network-side: The SI in the incoming Calling Party information element is ignored and replaced by one of the following: **1.** No calling IA5 digits received: **network**. **2.** NPI is not “unknown” nor “ISDN telephony”: **network**. **3.** TON is not “international” nor “national”: **network**, called IA5 digits are discarded. **4.** PI is set to “interworking”: **network**. **5.** Otherwise: **passed**. User-side: **not-screened**.

Table 269: SIP/ISDN Calls Default Values (Continued)

Parameter	Default Value
PI (calling)	Network-side: **1.** CLIR enabled: **restricted**. The PI is set to *restricted* no matter if a PI is present in the incoming Calling Party IE. **2.** CLIR disabled, no IA5 digits provided: **interworking**. **3.** CLIR disabled, IA5 digits provided: **allowed**. User-side: **1.** CLIR disabled, no IA5 digits provided: **interworking**. **2.** CLIR disabled, IA5 digits provided: **allowed**.
ITC (calling)	Must be provided in the incoming Bearer Capabilities information element provided by the ISDN peer that initiated the call. There is no default value, the call should be rejected if missing.
TON (called)	The Called TON must be provided by the ISDN peer that initiated the call.
TON (calling)	**unknown**
NPI (called	The Called NPI must be provided by the ISDN peer that initiated the call.
NPI (calling)	**unknown**

Note that the calling PI, SI, TON and NPI are present in Calling Party information elements in SETUP messages sent by the network-side only when CLIP is enabled. They should always be present in messages sent by the user-side. See “Chapter 21 - ISDN Configuration” on page 177 for more details on CLIP.

Call Routing Status

The routes, mappings, and hunts currently in use, as well as the available interfaces, are displayed in the *Call Router > Status* page.

Figure 155: Call Router – Status Web Page

Routes

The routing table contains one or more routes. These routes forward an incoming or outgoing call to another route, interface, or hunt based on a specific call property such as the called party number. It may also use a mapping to modify the call setup message of a call and a signalling property to modify the behaviour of the call at the SIP protocol level.

Once the call router finds a route that matches, it does not check the other routes, even if some of them may still match. The routes sequence is thus very important. The call router follows the routing table rows (routes) as they are entered in the web interface. If you want the call router to try to match one row before another one, you must put that row first.

When a call arrives, the call router proceeds as follows:

1. It examines the call property as specified with the routes.

   To select a route, the call must match all three of the *Source*, *Properties Criteria*, and *Expression Criteria* parameters.

2. It selects the first matching route in the list of routes.

3. It routes the call to the specified destination interface, hunt, or route.

> **Note:** You can revert back to the configuration displayed in the *Call Router > Status* web page at any time by clicking the **Rollback** button at the bottom of the page. All modified settings in the *Call Router > Route Config* page will be lost.

You can add up to 40 routes.

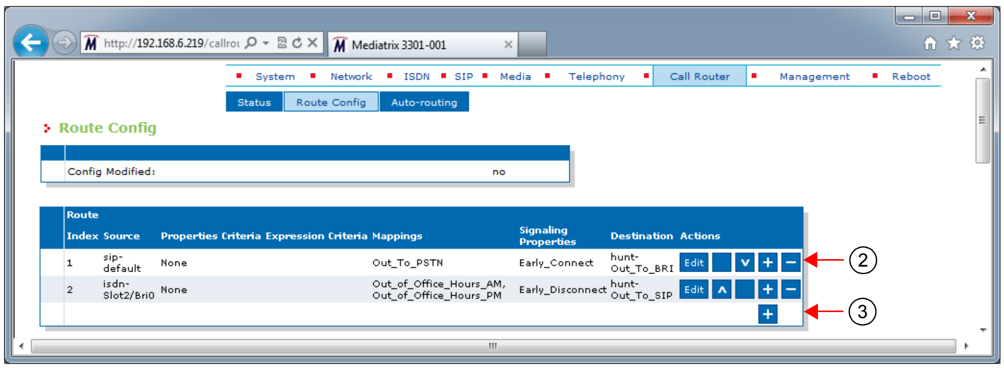
Creating/Editing a Route

The web interface allows you to create a route or modify the parameters of an existing one.

▶ To create or edit a route:

1. In the web interface, click the *Call Router* link, then the *Route Config* sub-link.

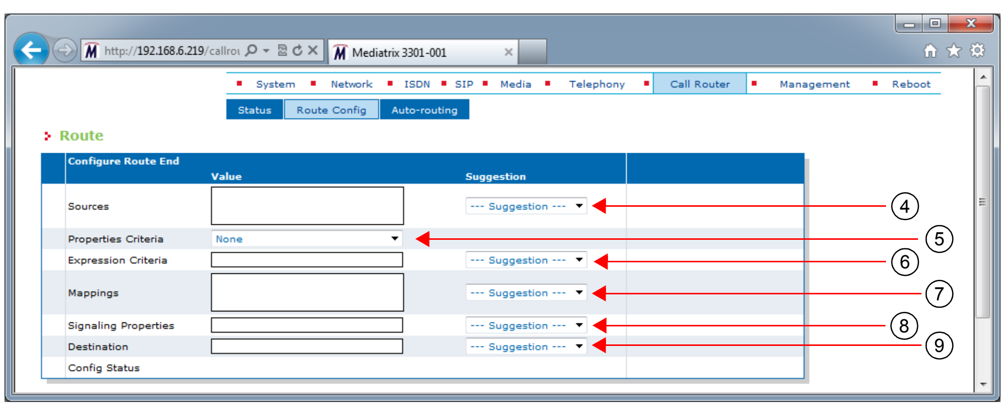
Figure 156: Call Router – Route Config Web Page



2. Locate the *Route* section.
3. Do one of the following:
   - If you want to add a route before an existing entry, locate the proper row in the table and click the + button of this row.
   - If you want to add a route at the end of the existing rows, click the + button at the bottom right of the *Route* section.
   - If you want to edit an existing route, locate the proper row in the table and click the Edit button.

   This brings you to the *Configure Route* panel.

Figure 157: Configure Route Panel



4. Enter one or more sources to compare with the call and match in order to select the route in the *Source* field.

   You can use the *Suggestion* column's drop-down menu to select between suggested values, if any. A source may be:

   - **route-***name*: The call uses the route *name*.
   - **sip-***name*: The call comes from the SIP interface *name*.
   - **isdn-***name*: The call comes from the ISDN interface *name*.
   - **r2-***name*: The call destination is set to the R2 interface *name*.
   - **e&m**-*name*: The call comes from the E&M interface name.
   - **fxs**-*name*: The call destination is set to the FXS interface *name*.
   - **fxo**-*name*: The call destination is set to the FXO interface *name*.

   If you want to use multiple sources, you must separate them by commas.

   For instance, if you want to route calls that come from the SIP interface "default", enter the following value:

   `sip-default`

   If you want to route calls that come from the SIP interfaces "default" and "other", enter the following value:

   `sip-default,sip-other`

   Keep in mind that to select a route, the call must match all three of the *Source*, *Properties Criteria*, and *Expression Criteria* parameters.

5. Select a call property to compare with the call and match in order to select the route in the *Properties Criteria* drop-down menu.

   The call router offers several different routing types. Each type specifies which call property the call router examines.

Table 270: Routing Types

Type	Description
Called E164	Routes calls based on the called party E.164 number.
Calling E164	Routes calls based on the calling party E.164 number.
Called TON	Routes calls based on the called party type of number.
Calling TON	Routes calls based on the calling party type of number.
Called NPI	Routes calls based on the called party numbering plan indicator.
Calling NPI	Routes calls based on the calling party numbering plan indicator.
Called Name	Routes calls based on the display name of the called party.
Calling Name	Routes calls based on the display name of the calling party.
Called Host	Routes calls based on the signalling IP address or domain name.
Calling Host	Routes calls based on the signalling IP address or domain name.
Called URI	Routes calls based on the *To-URI*.
Calling URI	Routes calls based on the *From-URI*.
Calling PI	Routes calls based on the presentation indicator.
Calling SI	Routes calls based on the screening indicator.
Calling ITC	Routes calls based on the information transfer capability.
Date/Time	Routes calls based on the date and/or time the call arrived at the call router. A link called **Time criteria editor** appears on the right of the *Expression criteria* field. Use it to easily configure the Date/Time type.

Table 270: Routing Types (Continued)

Type	Description
Called Phone Context	Routes calls based on the called party phone context.
Calling Phone Context	Routes calls based on the calling party phone context.
Called SIP Username	Routes calls based on the called party SIP username.
Calling SIP Username	Routes calls based on the calling SIP username.
Called Bearer Channel	Routes calls based on the called bearer channel properties.
Calling Bearer Channel	Routes calls based on the calling bearer channel properties.
Calling SIP Privacy	Routes calls based on the calling SIP privacy properties.

Keep in mind that to select a route, the call must match all three of the *Source*, *Properties Criteria*, and *Expression Criteria* parameters.

6. Enter the expression (related to the call properties selected in the previous step) to compare with the call and match in order to select the route in the *Expression Criteria* field.

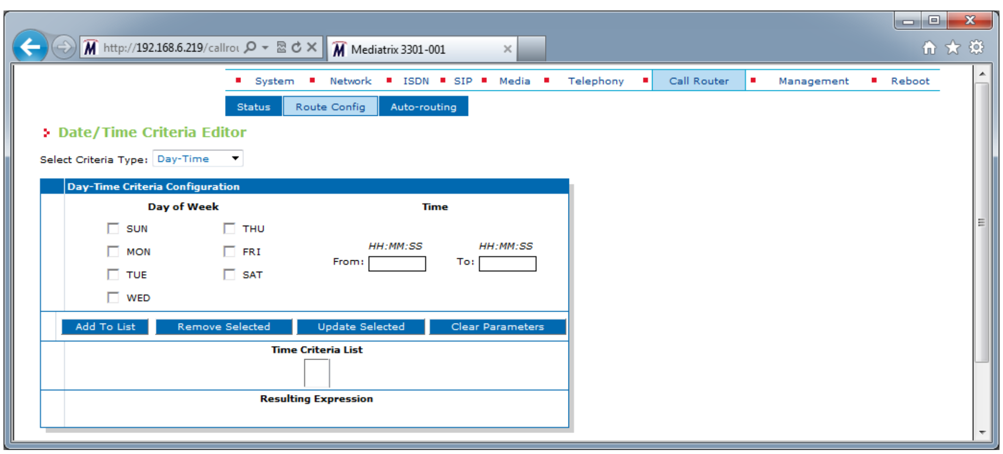
You can use the *Suggestion* column's drop-down menu to select between suggested values, if any. See "Routing Type" on page 338 for a list of available values for each call property.

For instance, if the property is *Calling TON*, you could instruct the call router to look for the following expression:

```
international
```

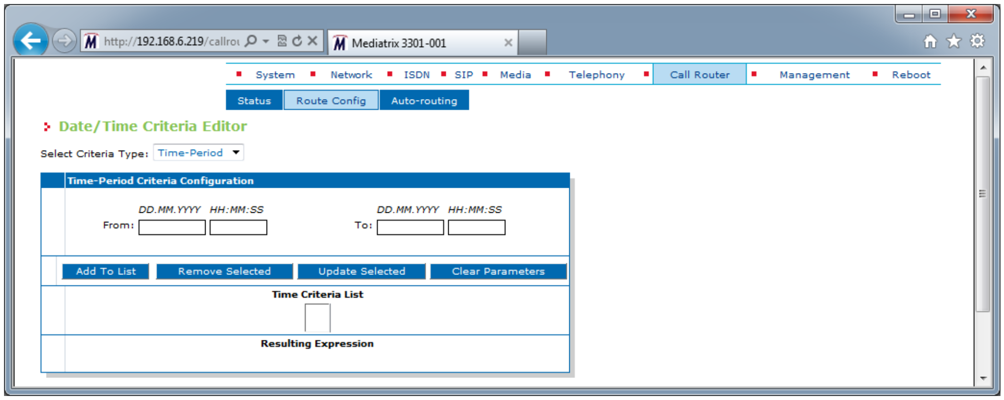
If you have selected the *Date/Time* property in the above step, you can click the **Time criteria editor** link and use the editor to easily configure the Date/Time parameters.

Figure 158: Date/Time Criteria Editor (Day Time)



- Select between the *Day-Time* or *Time-Period* settings in the *Select Criteria Type* drop-down menu. If you select *Time-Period*, the editor changes as follows:

Figure 159: Date/Time Criteria Editor (Time Period)



- Select or enter the parameters you want, then click the **Add to List** button. If a parameter is invalid (for instance, the end date is inferior to the start date), it is displayed in red in the *Time Criteria List* field.
- To remove an existing parameter, select it in the *Time Criteria List* field, then click the **Remove Selected** button.
- To update an existing parameter, select it in the *Time Criteria List* field, then click the **Update Selected** button.
- To remove all parameters, click the **Clear Parameters** button.
- When done, click the **Submit** button.

Keep in mind that to select a route, the call must match all three of the *Source*, *Properties Criteria*, and *Expression Criteria* parameters.

7. If applicable, enter the name of mappings to apply to the call in the *Mappings* field.

You can enter more than one mapping by separating them with commas. These mappings are executed in sequential order.

You can use the *Suggestion* column's drop-down menu to select an existing mapping, if any.

The manipulations are executed before sending the call to the new destination. See "Mappings" on page 358 for more details.

If you leave this field empty, no mapping is required.

8. Select the call signalling property of the route used to modify the behaviour of the call at the SIP protocol level in the *Call Signaling* drop-down menu.

You must set call signaling properties as defined in "Signalling Properties" on page 368. You can use the *Suggestion* column's drop-down menu to select between existing properties, if any.

9. Select the destination of the call when it matches in the *Destination* field.

You can use the *Suggestion* column's drop-down menu to select between suggested values, if any. The destination can be:

- **route-***name*: The call destination is set to the route *name*.
- **hunt-***name*: The call destination is set to the hunt *name*.
- **sip-***name*: The call destination is set to the SIP interface *name*.
- **isdn-***name*: The call destination is set to the ISDN interface *name*.
- **r2-***name*: The call destination is set to the R2 interface *name*.
- e&m-*name*: The call destination is set to the E&M interface *name*.
- **fxs**-*name*: The call destination is set to the FXS interface *name*.
- **fxo**-*name*: The call destination is set to the FXO interface *name*.
- **SipRedirect**-*name*: When the Route source is a SIP interface, incoming SIP Invites are replied with a 302 'Moved Temporarily' SIP response. See "SIP Redirects" on page 387 or more details.

For instance, if you want to route calls to the hunt “CallCenter”, enter the following:

`hunt-CallCenter`

10. Click the **Submit** button.

This brings you back to the main *Call Router* > *Route Config* web page.

You can see a yellow **Yes** in the *Config Modified* section at the top of the window. It warns you that the configuration has been modified but not applied (i.e., the *Call Router* > *Status* differs from the *Call Router* > *Route Config*). The *Route Config* sub-menu is a working area where you build up a Call Router configuration. While you work in this area, the configured parameters are saved but not applied (i.e., they are not used to process incoming calls). The yellow **Yes** flag warns you that the configuration has been modified but is not applied.

11. Click the **Apply** button to enable the route.

The current routes applied are displayed in the *Call Router* > *Status* web page. You can also see that the yellow Config Modified **Yes** flag is cleared.

Examples

The following are some examples of routes:

Figure 160: Routes Examples

Route					
Source	Properties Criteria	Expression Criteria	Mappings	Signaling Properties	Destination
sip-default	None		Out_To_PSTN	Early_Connect	hunt-Out_To_BRI
isdn-Slot2/Bri0	None		Out_of_Office_Hours_AM, Out_of_Office_Hours_PM	Early_Disconnect	hunt-Out_To_SIP

Moving a Route

Once the call router finds a routing entry that matches, it does not check the other entries, even if some of them may still match. The routes sequence is thus very important. The call router follows the routing table rows as they are entered in the web interface. If you want the call router to try to match one row before another one, you must put that row first.

► **To move a routing entry up or down:**

1. Either click the or arrow of the row you want to move until the entry is properly located.

2. Click the **Apply** button to update the *Call Router* > *Status* web page.

Deleting a Route

You can delete a routing row from the table in the web interface.

► **To delete a routing entry:**

1. Click the button of the row you want to delete.

2. Click the **Apply** button to update the *Call Router* > *Status* web page.

Mappings

Mapping entries modify the call setup message of a call. They thus influence the routing decision and/or the setup message leaving the call router. They are specifically called within a route.

Like the routing table, the mapping table finds the first matching entry. It then executes it by manipulating a call property. A mapping always examines one call property and changes another property.

The call router executes all mapping entries that match by following the mapping table rows as they are entered in the web interface. If you want the call router to try to match one row before another one, you must put that row first.

The mapping may work with three types of call properties:

- calling party properties
- called party properties
- generic properties

Generic properties are used for call properties that apply to both calling and called parties.

The web interface mapping configuration is separated in two parts: *Mapping Type* and *Mapping Expression*. You must properly configure both parts for the mapping to work as required.

When a call arrives at the mapping table, the call router proceeds as follows:

1. It examines the call property as specified in the *Criteria* (input) value of the *Mapping Type* part.
2. It selects the first matching entry.
3. It replaces the property specified in the *Transformation* (output) value of the *Mapping Expression* part with the value of the selected entry.

> **Note:** You can revert back to the configuration displayed in the *Call Router* > *Status* web page at any time by clicking the **Rollback** button at the bottom of the page. All modified settings in the *Call Router* > *Route Config* page will be lost.

Creating/Editing a Mapping Type

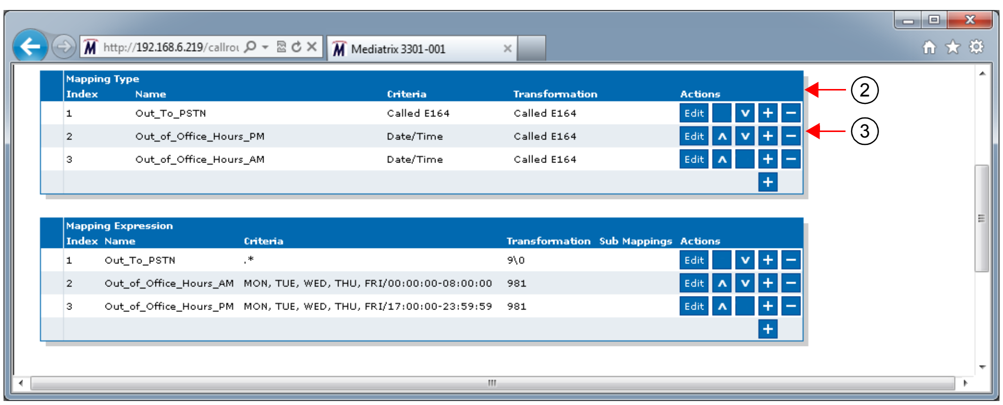
The *Mapping Type* part allows you to define the input call property to match and to define which call property to change. The mapping type then uses one or more corresponding mapping expressions that you can define in "Creating/Editing a Mapping Expression" on page 360.

You can add up to 40 Mapping Types.

▶ **To create or edit a mapping type:**

1. In the web interface, click the *Call Router* link, then the *Route Config* sub-link.

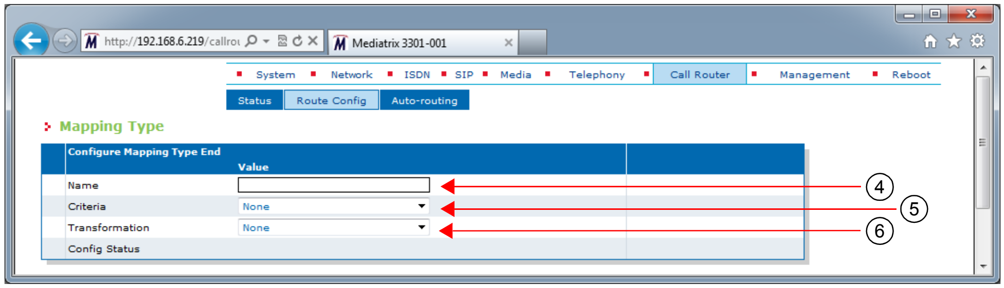
Figure 161: Call Router – Route Config Web Page



2. Locate the *Mapping Type* section.
3. Do one of the following:
   - If you want to add a mapping type entry before an existing entry, locate the proper row in the table and click the + button of this row.
   - If you want to add a mapping type entry at the end of the existing rows, click the + button at the bottom right of the *Mapping Type* section.
   - If you want to edit an existing entry, locate the proper row in the table and click the Edit button.

   This brings you to the *Configure Mapping Type* panel.

Figure 162: Configure Mapping Type Panel



4. Enter the name of the mapping in the *Name* field.

This is the name used in a route when calling a mapping. It must be unique. Aastra suggests to use the type as part of the name for ease of identification.

There must be at least one corresponding mapping expression in the *Mapping Expression* table with the exact same name. See "Creating/Editing a Mapping Expression" on page 360 for more details.

5. Select the input call property to compare with the call and match in order to select the mapping in the *Criteria* drop-down menu.

6. Select the call property to transform in the *Transformation* drop-down menu.

7. Do one of the following:

- Click the **Submit** button to go back to the main *Call Router* > *Route Config* web page. You can now define a corresponding mapping expression.
- Click the **Submit and Insert Expression** button to directly access the proper mapping expression dialog.

Creating/Editing a Mapping Expression

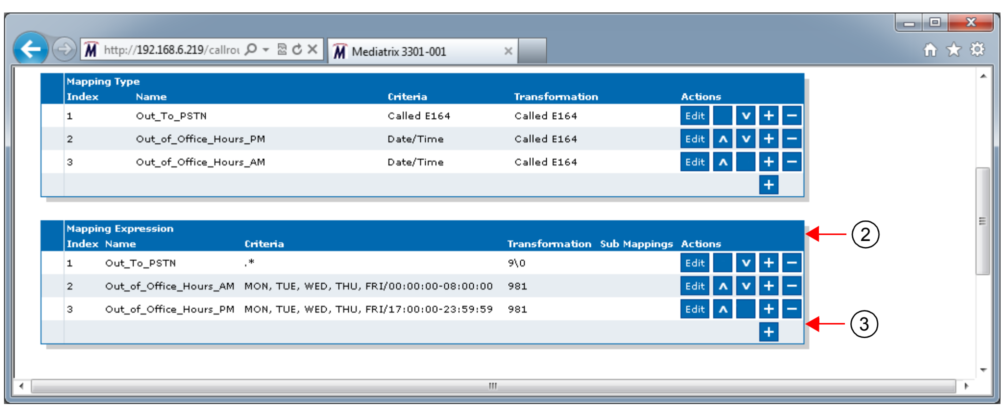
The *Mapping Expression* part defines the actual transformation to apply to the corresponding mapping type. Each mapping expression must match a mapping type as defined in "Creating/Editing a Mapping Type" on page 359.

You can add up to 100 Mapping Expressions.

▶ To create or edit a mapping expression:

1. In the web interface, click the *Call Router* link, then the *Route Config* sub-link.

Figure 163: Call Router – Route Config Web Page



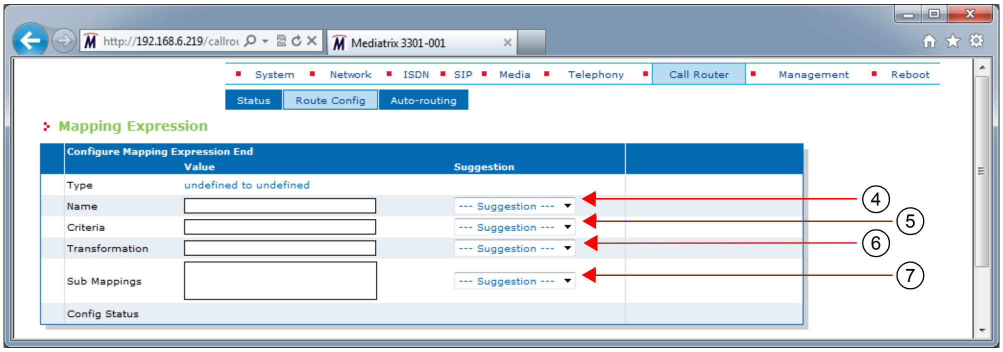
2. Locate the *Mapping Expression* section.

3. Do one of the following:

- If you want to add a mapping expression entry before an existing entry, locate the proper row in the table and click the button of this row.
- If you want to add a mapping expression entry at the end of the existing rows, click the button at the bottom right of the *Mapping Expression* section.
- If you want to edit an existing entry, locate the proper row in the table and click the Edit button.

This brings you to the *Configure Mapping Expression* panel.

Figure 164: Configure Mapping Expression Panel



4. Enter the name of the mapping expression in the *Name* field.

This name must match a mapping type as defined in "Creating/Editing a Mapping Type" on page 359. You can use the *Suggestion* column's drop-down menu to select an existing mapping type. When a name matches a mapping type, its type is displayed in the *Type* row as follows:

`input type to output type`

You can define several mapping expressions with the same name. In that case, the first row matching the call is used. The rows are used in ascending order.

5. Enter the expression (related to this specific input type) to compare with the call and match in order to select the mapping in the *Criteria* field.

This string differs depending on the input type selected in the *Mapping Type* part (*Criteria* drop-down menu). For instance, if your input type is *Calling TON*, you could instruct the call router to look for the following expression:

`international`

You can use the *Suggestion* column's drop-down menu to select between suggested values, if any. See "Routing Type" on page 338 for a list of available transformation values.

Table 271: Input Type Criteria

Input Type	Criteria
None	No criteria, always matches.
E164	If the *Transformation* value of the *Mapping Type* part is also a generic property, this is applied to both this *Calling E164* and *Called E164* property.
Called E164	Selects an entry based on the called party E.164 number. You can use wildcards to summarize entries as per "Called / Calling E164" on page 339.
Calling E164	Selects an entry based on the calling party E.164 number. You can use wildcards to summarize entries as per "Called / Calling E164" on page 339.
Name	If the *Transformation* value of the *Mapping Type* part is also a generic property, this is applied to both this *Calling Name* and *Called Name* property.
Called Name	Selects an entry based on the display name of the called party. You can use wildcards to summarize entries as per "Called / Calling Name" on page 340.

Table 271: Input Type Criteria (Continued)

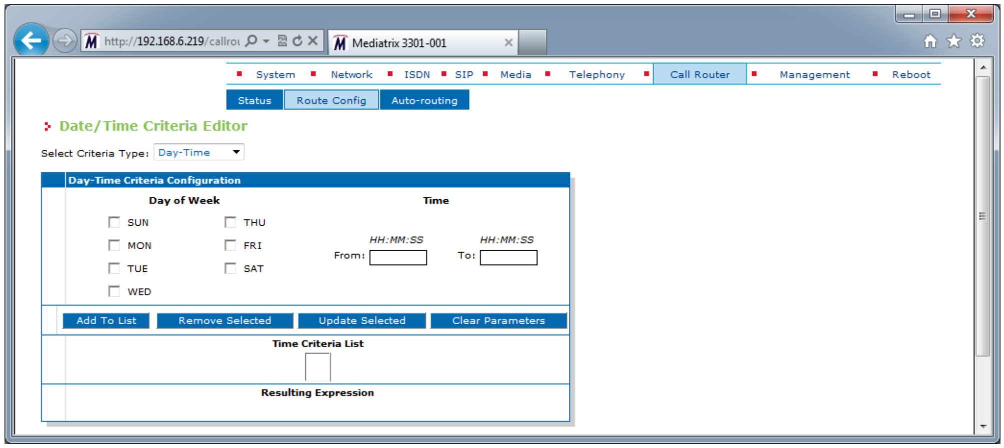
Input Type	Criteria
Calling Name	Selects an entry based on the display name of the calling party. You can use wildcards to summarize entries as per “Called / Calling Name” on page 340.
TON	If the *Transformation* value of the *Mapping Type* part is also a generic property, this is applied to both this *Calling TON* and *Called TON* property.
Called TON	Selects an entry based on the called party type of number as per “Called / Calling TON” on page 339.
Calling TON	Selects an entry based on the calling party type of number as per “Called / Calling TON” on page 339.
NPI	If the *Transformation* value of the *Mapping Type* part is also a generic property, this is applied to both this *Calling NPI* and *Called NPI* property.
Called NPI	Selects an entry based on the called party numbering plan indicator as per “Called / Calling NPI” on page 339.
Calling NPI	Selects an entry based on the calling party numbering plan indicator as per “Called / Calling NPI” on page 339.
Host	If the *Transformation* value of the *Mapping Type* part is also a generic property, this is applied to both this *Calling Host* and *Called Host* property.
Called Host	Selects an entry based on the remote signalling IP address or domain name of the destination VoIP peer. You can use wildcards to summarize entries as per “Called / Calling Host” on page 340.
Calling Host	Selects an entry based on the remote signalling IP address or domain name of the originating VoIP peer. You can use wildcards to summarize entries as per “Called / Calling Host” on page 340.
Calling PI	Selects an entry based on the presentation indicator as per “Calling PI” on page 340.
Calling SI	Selects an entry based on the screening indicator as per “Calling SI” on page 340.
Calling ITC	Selects an entry based on the information transfer capability as per “Calling ITC” on page 341.
URI	If the *Transformation* value of the *Mapping Type* part is also a generic property, this is applied to both this *Calling URI* and *Called URI* property.
Called URI	Selects an entry based on the called SIP URI properties. You can use wildcards to summarize entries as per “Called / Calling URI” on page 340.
Calling URI	Selects an entry based on the calling SIP URI properties. You can use wildcards to summarize entries as per “Called / Calling URI” on page 340.
Date/Time	Selects an entry based on the date and/or time the call arrived at the call router as per “Date/Time” on page 341.
Phone Context	Selects an entry based on the called or calling phone context properties as per “Called / Calling Phone Context” on page 342.
Called Phone Context	Selects an entry based on the called phone context properties as per “Called / Calling Phone Context” on page 342.
Calling Phone Context	Selects an entry based on the calling phone context properties as per “Called / Calling Phone Context” on page 342.
SIP Username	Selects an entry based on the called or calling SIP username properties as per “Called / Calling SIP Username” on page 342.

Table 271: Input Type Criteria (Continued)

Input Type	Criteria
Called SIP Username	Selects an entry based on the called SIP username properties as per “Called / Calling SIP Username” on page 342.
Calling SIP Username	Selects an entry based on the calling SIP username properties as per “Called / Calling SIP Username” on page 342.
Last Diverting Reason	Selects an entry based on the last diverting reason properties as per “Last / Original Diverting Reason” on page 342.
Last Diverting E164	Selects an entry based on the last diverting E.164 properties as per “Last / Original Diverting E.164” on page 343.
Last Diverting Party Number Type	Selects an entry based on the party number type of the last diverting number properties as per “Last / Original Diverting Party Number Type” on page 343.
Last Diverting Public Type Of Number	Selects an entry based on the public type of number of the last diverting number properties as per “Last / Original Diverting Public Type Of Number” on page 343.
Last Diverting Private Type Of Number	Selects an entry based on the private type of numbekr of the last diverting number properties as per “Last / Original Diverting Private Type Of Number” on page 343.
Last Diverting Number Presentation	Selects an entry based on the presentation of the last diverting number properties as per “Last / Original Diverting Number Presentation” on page 344.
OriginalDivertingReason	Selects an entry based on the original diverting reason properties as per “Last / Original Diverting Reason” on page 342.
OriginalDivertingE164	Selects an entry based on the original diverting E.164 properties as per “Last / Original Diverting E.164” on page 343.
Original Diverting Party Number Type	Selects an entry based on the party number type of the original diverting number properties as per “Last / Original Diverting Party Number Type” on page 343.
Original Diverting Public Type Of Number	Selects an entry based on the public type of number of the original diverting number properties as per “Last / Original Diverting Public Type Of Number” on page 343.
Called Bearer Channel	Selects an entry based on the called bearer channel properties as per “Called / Calling SIP Username” on page 342.
Calling Bearer Channel	Selects an entry based on the calling bearer channel properties as per “Called / Calling SIP Username” on page 342.
Calling SIP Privacyl	Selects an entry based on the calling SIP privacy properties as per “SIP Privacy Type” on page 344.

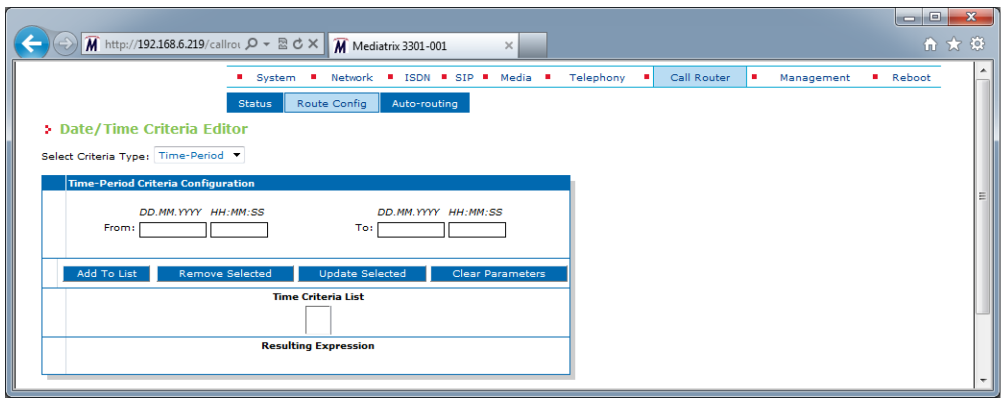
If you are editing a *Date/Time* property, you can click the **Time criteria editor** link and use the editor to easily configure the Date/Time parameters.

Figure 165: Date/Time Criteria Editor (Day Time)



- Select between the *Day-Time* or *Time-Period* settings in the *Select Criteria Type* drop-down menu. If you select *Time-Period*, the editor changes as follows:

Figure 166: Date/Time Criteria Editor (Time Period)



- Select or enter the parameters you want, then click the **Add to List** button. If a parameter is invalid (for instance, the end date is inferior to the start date), it is displayed in red in the *Time Criteria List* field.
- To remove an existing parameter, select it in the *Time Criteria List* field, then click the **Remove Selected** button.
- To update an existing parameter, select it in the *Time Criteria List* field, then click the **Update Selected** button.
- To remove all parameters, click the **Clear Parameters** button.
- When done, click the **Submit** button.

6. Enter the transformation (related to this specific output type) to apply in the *Transformation* field.

You can use the *Suggestion* column's drop-down menu to select between suggested values, if any.

If the transformation is to replace part of an expression, it can use the matched group of the criteria. "\0" will be replaced by the whole criteria capability and "\1" to "\9" by the matched group. See "Groups" on page 337 for more details.

See "Routing Type" on page 338 for a list of available transformation values.

Table 272: Output Type Transformation

Output Type	Transformation
None	No transformation is applied.

Table 272: Output Type Transformation (Continued)

Output Type	Transformation
E164	If the *Criteria* value of the *Mapping Type* part is also a generic property, this is applied to both the *Calling E164* and *Called E164* properties.
Called E164	Modifies the called party E.164 number as per "Called / Calling E164" on page 339.
Calling E164	Modifies the calling party E.164 number as per "Called / Calling E164" on page 339.
Name	If the *Criteria* value of the *Mapping Type* part is also a generic property, this is applied to both the *Calling Name* and *Called Name* properties.
Called Name	Sets the display name of the called party as per "Called / Calling Name" on page 340.
Calling Name	Sets the display name of the calling party as per "Called / Calling Name" on page 340.
TON	If the *Criteria* value of the *Mapping Type* part is also a generic property, this is applied to both the *Calling TON* and *Called TON* properties.
Called TON	Sets the called party type of number as per "Called / Calling TON" on page 339.
Calling TON	Sets the calling party type of number as per "Called / Calling TON" on page 339.
NPI	If the *Criteria* value of the *Mapping Type* part is also a generic property, this is applied to both the *Calling NPI* and *Called NPI* properties.
Called NPI	Sets the called party numbering plan indicator as per "Called / Calling NPI" on page 339.
Calling NPI	Sets the calling party numbering plan indicator as per "Called / Calling NPI" on page 339.
Host	If the *Criteria* value of the *Mapping Type* part is also a generic property, this is applied to both the *Calling Host* and *Called Host* properties.
Called Host	Sets the remote IP address or domain name of the destination VoIP peer as per "Called / Calling Host" on page 340.
Calling Host	Sets the remote IP address or domain name of the originating VoIP peer as per "Called / Calling Host" on page 340.
Calling PI	Sets the presentation indicator as per "Calling PI" on page 340.
Calling SI	Sets the screening indicator as per "Calling SI" on page 340.
Calling ITC	Sets the information transfer capability as per "Calling ITC" on page 341.
URI	If the *Criteria* value of the *Mapping Type* part is also a generic property, this is applied to both the *Calling URI* and *Called URI* properties.
Called URI	Sets the called URI as per "Called / Calling URI" on page 340.
Calling URI	Sets the calling URI as per "Called / Calling URI" on page 340.
Phone Context	If the *Criteria* value of the *Mapping Type* part is also a generic property, this is applied to both the *Calling Phone Context* and *Called Phone Context* properties.
Called Phone Context	Sets the called Phone Context as per "Called / Calling Phone Context" on page 342.
Calling Phone Context	Sets the calling Phone Context as per "Called / Calling Phone Context" on page 342.

Table 272: Output Type Transformation (Continued)

Output Type	Transformation
SIP Username	If the *Criteria* value of the *Mapping Type* part is also a generic property, this is applied to both the *Calling SIP Username* and *Called SIP Username* properties.
Called SIP Username	Sets the called SIP Username as per “Called / Calling SIP Username” on page 342.
Calling SIP Username	Sets the calling SIP Username as per “Called / Calling SIP Username” on page 342.
Last Diverting Reason	Sets the last diverting reason properties as per “Last / Original Diverting Reason” on page 342.
Last Diverting E164	Sets the last diverting E.164 properties as per “Last / Original Diverting E.164” on page 343.
Last Diverting Party Number Type	Sets the party number type of the last diverting number properties as per “Last / Original Diverting Party Number Type” on page 343.
Last Diverting Public Type Of Number	Sets the public type of number of the last diverting number properties as per “Last / Original Diverting Public Type Of Number” on page 343.
Last Diverting Private Type Of Number	Sets the private type of number of the last diverting number properties as per “Last / Original Diverting Private Type Of Number” on page 343.
Last Diverting Number Presentation	Sets the presentation of the last diverting number properties as per “Last / Original Diverting Number Presentation” on page 344.
Original Diverting Reason	Sets the original diverting reason properties as per “Last / Original Diverting Reason” on page 342.
Original Diverting E164	Sets the original diverting E.164 properties as per “Last / Original Diverting E.164” on page 343.
Original Diverting Party Number Type	Sets the party number type of the original diverting number properties as per “Last / Original Diverting Party Number Type” on page 343.
Original Diverting Public Type Of Number	Sets the public type of number of the original diverting number properties as per “Last / Original Diverting Public Type Of Number” on page 343.
Original Diverting Private Type Of Number	Sets the private type of number of the original diverting number properties as per “Last / Original Diverting Private Type Of Number” on page 343.

Table 272: Output Type Transformation (Continued)

Output Type	Transformation
Original Diverting Number Presentation	Sets the Presentation of the original diverting number properties as per "Last / Original Diverting Number Presentation" on page 344.
Called Bearer Channel	Sets the called bearer channel properties as per "Called / Calling SIP Username" on page 342.
Calling Bearer Channel	Sets the calling bearer channel properties as per "Called / Calling SIP Username" on page 342.
Debug	Reserved for debug configuration.

You cannot use Date/Time as an output type transformation.

7. If applicable, enter the name of one or more subsequent mappings to execute in the *Sub Mappings* field.

You can enter more than one mapping by separating them with commas. The mappings are executed in sequential order.

You can use the *Suggestion* column's drop-down menu to select between existing values, if any.

You may want to send the result of the first mapping to another one. Once the subsequent mapping is finished, the call router continues to check the mapping entries for matching entries. For instance, if the call router is checking the fourth mapping entry and that entry uses subsequent mapping, the call router executes the subsequent mapping, then resumes checking the fifth mapping entry, and so on.

The maximal number of subsequent interleaved mapping is 3.

8. Do one of the following:

- Click the **Submit** button to go back to the main *Call Router* > *Route Config* web page.

  You can see a yellow **Yes** in the *Config Modified* section at the top of the window. It warns you that the configuration has been modified but not applied (i.e., the *Call Router* > *Status* differs from the *Call Router* > *Route Config*). The *Route Config* sub-menu is a working area where you build up a Call Router configuration. While you work in this area, the configured parameters are saved but not applied (i.e., they are not used to process incoming calls). The yellow **Yes** flag warns you that the configuration has been modified but is not applied.

- Click the **Submit and Insert Expression** button to create another expression for the same type.

9. Click the **Apply** button to enable the mapping entry.

The current mappings applied are displayed in the *Call Router* > *Status* web page. You can also see that the yellow Config Modified **Yes** flag is cleared.

Examples

The following are some examples of mappings:

Figure 167: Mappings Examples

Mapping Out_To_PSTN (Called E164 to Called E164)		
Criteria	Transformation	Sub Mappings
.*	9\0	

Mapping Out_of_Office_Hours_PM (Date/Time to Called E164)		
Criteria	Transformation	Sub Mappings
MON, TUE, WED, THU, FRI/17:00:00-23:59:59	981	

Mapping Out_of_Office_Hours_AM (Date/Time to Called E164)		
Criteria	Transformation	Sub Mappings
MON, TUE, WED, THU, FRI/00:00:00-08:00:00	981	

Moving a Mapping Type or Expression Row

The mapping entries sequence is very important. The call router follows the mapping table rows as they are entered in the web interface. If you want the call router to try to match one row before another one, you must put that row first.

▶ **To move a mapping entry up or down:**

1. In the *Mapping Type* or *Mapping Expression* table, either click the ^ or v arrow of the row you want to move until the entry is properly located.
2. Click the **Apply** button to update the *Call Router* > *Status* web page.

Deleting a Mapping Type or Expression Row

You can delete a mapping row from the *Mapping Type* or *Mapping Expression* table in the web interface.

▶ **To delete a mapping entry:**

1. Click the − button of the row you want to delete.
2. Click the **Apply** button to update the *Call Router* > *Status* web page.

Signalling Properties

Standards Supported	• RFC 3323: A Privacy Mechanism for the Session Initiation Protocol (SIP) (only supports 'none' as Privacy level) • RFC 3325: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks (supports 'id' as Privacy level. Accept/send P-Asserted-Identity and P-Preferred-Identity.)

Call signalling specifies how to set up a call to the destination Aastra unit or 3rd party equipment. Call signalling properties are assigned to a route and used to modify the behaviour of the call at the SIP protocol level.

Signaling Properties are applied after mappings rules.

Like the routing table, the signalling properties table finds the first matching entry. It then executes it by modifying the behaviour of the call.

Note: You can revert back to the configuration displayed in the *Call Router* > *Status* web page at any time by clicking the **Rollback** button at the bottom of the page. All modified settings in the *Call Router* > *Route Config* page will be lost.

You can add up to 40 Signalling Properties.

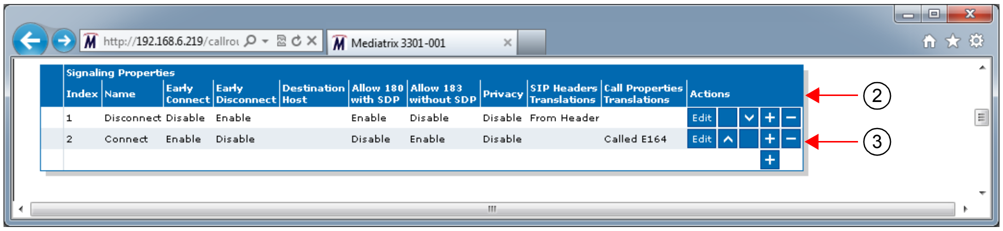
Creating/Editing a Signalling Property

The web interface allows you to create a signalling property or modify the parameters of an existing one. The signalling properties are called from a route as described in "Routes" on page 353.

▶ To create or edit a signalling property:

1. In the web interface, click the *Call Router* link, then the *Route Config* sub-link.

Figure 168: Call Router – Route Config Web Page



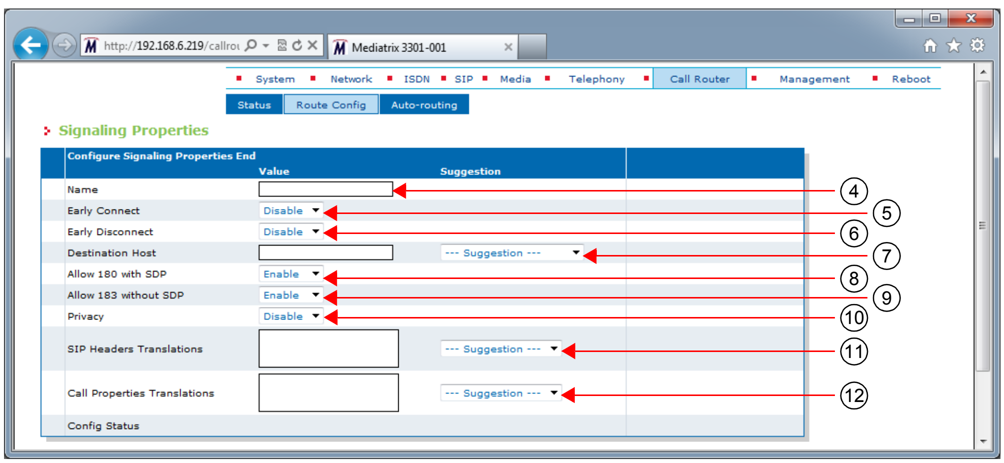
2. Locate the *Signaling Properties* section.

3. Do one of the following:

- If you want to add a signalling property entry before an existing entry, locate the proper row in the table and click the + button of this row.
- If you want to add a signalling property entry at the end of existing rows, click the + button at the bottom right of the *Signaling Properties* section.
- If you want to edit an existing entry, locate the proper row in the table and click the Edit button.

This brings you to the *Configure Signaling Properties* panel.

Figure 169: Configure Signaling Properties Panel



4. Enter the name of the signalling property in the *Name* field.

The name must be unique. It will be used in routes to call a specific signalling property as described in "Routes" on page 353.

5. Select whether or not the early connect feature is enabled in the *Early Connect* drop-down menu.

When early connect is enabled, the SIP call is connected by sending a 200 OK message instead of a 183 Session Progress message with early media, if the called party answers the call. It allows interoperability with units that do not support the 183 Session Progress with SDP message.

When early connect is disabled, call progress tones or announcements are transmitted in the early SIP dialog.

6. Select whether or not the early disconnect feature is enabled in the *Early Disconnect* drop-down menu.

This feature is useful to avoid hearing the end of call tone when the far end party terminates the call during a conference.

When early disconnect is:

- enabled, the SIP BYE message is sent upon receiving the ISDN “Disconnect” signal.
- disabled, the SIP BYE message is sent upon receiving the ISDN “Call release” signal.

If early disconnect is enabled but no ISDN “Disconnect” message is received, the SIP BYE message is sent upon receiving an ISDN “Call release” signal as if the early disconnect was disabled.

7. Define the SIP messages destination (where an INVITE is sent) in the *Destination Host* field.

It can override the *Called Host* property set by a mapping rule because signalling properties are applied after mappings.

You can also use the macro `local_ip_port` to replace the properties by the local IP address and port of the listening network of the SIP gateway used to send the INVITE.

8. Define whether or not to enable the 180 with SDP allowed feature in the *Allow 180 SDP* drop-down menu.

Table 273: 180 with SDP Parameters

Parameter	Description
Enable	The unit can send a SDP in the provisional response 180. Thus when the ISDN peer sends an alerting with indication to open the voice (or if the voice is already opened), the unit sends a 180 with SDP. This is the default value.
Disable	A SIP 183 with SDP is sent instead of a 180 with SDP. This does not affect the 180 without SDP. This is useful if your proxy has issues receiving 180 with SDP messages. The SIP 183 with SDP replacing the SIP 180 with SDP is not sent if a 183 with SDP has already been sent.

9. Define whether or not to enable the 183 without SDP allowed feature in the *Allow 183 No SDP* drop-down menu.

Table 274: 183 without SDP Parameters

Parameter	Description
Enable	When enabled, the unit sends a 183 without SDP upon receiving an ISDN progress indicator without any indication to open a voice stream. This is the default value.
Disable	When disabled, nothing is sent instead of a 183 without SDP. This does not affect the 183 with SDP. This is useful if your proxy has issues receiving 183 without SDP messages.

10. Set the privacy level of the call in the *Privacy* drop-down menu.

Table 275: Privacy Levels

Level	Description	Effects on incoming SIP call	Effects on outgoing SIP call
Disable	No privacy is used.	None	None

Table 275: Privacy Levels (Continued)

Level	Description	Effects on incoming SIP call	Effects on outgoing SIP call
None	Use P-Asserted Identity privacy.	None	Adds two headers: • **Privacy**: none • **P-Asserted-Identity**: p_asserted_identity_value *p_asserted_identity_value* is the call's From URI unless a SIP header translation has been added to the Signaling Properties for the *Identity-header*.
Id	Use P-Preferred Identity privacy.	The *calling-name* is empty and the PI is set to **restricted**.	Always adds one header: • **P-Preferred-Identity**: p_preferred_identity_value *p_ preferred _identity_value* is the call's From URI unless a SIP header translation has been added to the Signaling Properties for the *Identity-header*. If the incoming call's PI property is *restricted*, another header is added: • **Privacy**: id
Rpid	Use Remote-Party-ID privacy.	None	One header always added : • **Remote-Party-ID**: remote_party_id_value "*Optional Friendly Name*"<sip:410202@10.4.125.12>;party=calling Where *remote_party_id_value* should be set by the SIP Headers Translation. It consists of an optional friendly name followed by the SIP URI and the party direction. Example: `Remote-Party-ID: "John Doe"<sip:410202@10.4.125.12>;party=calling`

11. Enter the name of one or more SIP headers translation to apply to the call in the *SIP Headers Translations* field.

You must define SIP headers translations as defined in "SIP Headers Translations" on page 372. You can use the *Suggestion* column's drop-down menu to select between existing translations, if any.

You can enter more than one translation. In that case, the translations are separated with "," and are executed in sequential order.

12. Enter the name of one or more call properties translation to apply to the call in the *Call Properties Translations* field.

You must set call properties translations as defined in “Call Properties Translations” on page 376. You can use the *Suggestion* column’s drop-down menu to select between existing translations, if any.

You can enter more than one translation. In that case, the translations are separated with “,” and are executed in sequential order.

13. Click the **Submit** button.

This brings you back to the main *Call Router* > *Route Config* web page.

You can see a yellow **Yes** in the *Config Modified* section at the top of the window. It warns you that the configuration has been modified but not applied (i.e., the *Call Router* > *Status* differs from the *Call Router* > *Route Config*). The *Route Config* sub-menu is a working area where you build up a Call Router configuration. While you work in this area, the configured parameters are saved but not applied (i.e., they are not used to process incoming calls). The yellow **Yes** flag warns you that the configuration has been modified but is not applied.

14. Click the **Apply** button to enable the signalling property entry.

The current properties applied are displayed in the *Call Router* > *Status* web page. You can also see that the yellow Config Modified **Yes** flag is cleared.

Examples

The following are some examples of signalling properties:

Figure 170: Signalling Properties Examples

Signaling Properties								
Name	Early Connect	Early Disconnect	Destination Host	Allow 180 with SDP	Allow 183 without SDP	Privacy	SIP Headers Translations	Call Properties Translations
Disconnect	Disable	Enable		Enable		Disable	From Header	
Connect	Enable	Disable		Disable		Disable		Called E164

Moving a Signalling Property Row

The signalling properties entries sequence is very important. The call router follows the signalling properties table rows as they are entered in the web interface. If you want the call router to try to match one row before another one, you must put that row first.

▶ **To move a signalling property entry up or down:**

1. Either click the ^ or v arrow of the row you want to move until the entry is properly located.
2. Click the **Apply** button to update the *Call Router* > *Status* web page.

Deleting a Signalling Property Row

You can delete a signalling property row from the table in the web interface.

▶ **To delete a signalling property entry:**

1. Click the − button of the row you want to delete.
2. Click the **Apply** button to update the *Call Router* > *Status* web page.

SIP Headers Translations

A SIP Headers Translation overrides the default value of SIP headers in an outgoing SIP message. It modifies the SIP headers before the call is sent to its destination.

Like the routing table, the SIP headers translation table finds the first matching entry. It then executes it by modifying the behaviour of the call.

> **Note:** You can revert back to the configuration displayed in the *Call Router > Status* web page at any time by clicking the **Rollback** button at the bottom of the page. All modified settings in the *Call Router > Route Config* page will be lost.

You can add up to 100 SIP Headers Translations.

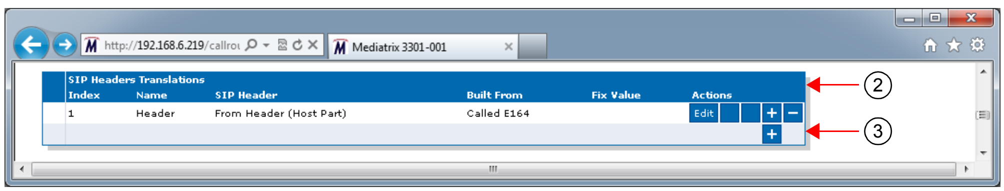
Creating/Editing a SIP Headers Translation

The web interface allows you to create a SIP header translation or modify the parameters of an existing one. The SIP headers translations are called from a signalling property as described in “Signalling Properties” on page 368.

► To create or edit a SIP headers translation:

1. In the web interface, click the *Call Router* link, then the *Route Config* sub-link.

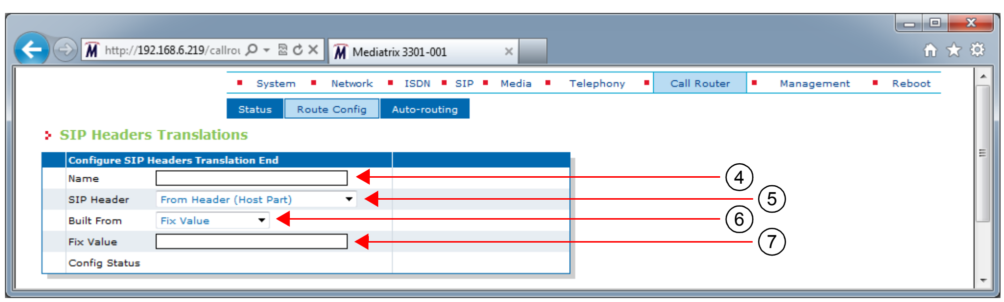
Figure 171: Call Router – Route Config Web Page



2. Locate the *SIP Headers Translations* section.
3. Do one of the following:
   - If you want to add a SIP headers translation before an existing entry, locate the proper row in the table and click the + button of this row.
   - If you want to add a SIP headers translation at the end of existing rows, click the + button at the bottom right of the *SIP Headers Translations* section.
   - If you want to edit an existing entry, locate the proper row in the table and click the Edit button.

This brings you to the *Configure SIP Headers Translation* panel.

Figure 172: Configure SIP Headers Translation Panel



4. Enter the name of the SIP headers translation in the *Name* field.
5. Set which SIP header is modified by this translation in the *SIP Header* drop-down menu.

Table 276: SIP Headers

SIP Header	Description
From Header (Host Part)	Host part of the *From* header's URI.

Table 276: SIP Headers (Continued)

SIP Header	Description
From Header (User Part)	User part of the *From* header's URI.
Identity Header (Host Part)	Host part of the *Identity* header's URI.
Identity Header (User Part)	User part of the *Identity* header's URI.
Identity Header (Phone Number)	Phone number in the *Identity* header's tel URL.
Request Line (Host Part)	Host part of the Request line's URI.
Request Line (User Part)	User part of the Request line's URI.
To Header (Host Part)	Host part of the *To* header's URI.
To Header (User Part)	User part of the *To* header's URI.

6. Set what information is used to build the selected SIP header in the *Built From* drop-down menu.

Table 277: Built From Information

Built From	Description
Called E164	Use the called party E.164 property.
Destination Host	Use the destination host configured in the signalling properties of which this translation is part.
Domain	Use the domain name configured in the unit.
Fix Value	Use a fix value as defined in the *Fix Value* field (see Step 7).
Host Name	Use the host name configured in the unit.
Local Ip	Use the local IP address.
Calling Bearer Channel	Use the calling bearer channel.
SIP Endpoint Username	Use the SIP username associated with the endpoint.
Calling Name	Use the calling party name property.
Calling E164	Use the calling party E.164 property.

7. If you have selected **Fix Value** in the *Built From* drop-down menu, enter a fix value to be inserted in the SIP header in the *Fix Value* field.

For instance, you could hide the caller's name in a SIP message by using the *From Header (User Part)* SIP header and entering "anonymous" in the *Fix Value* field.

8. Click the **Submit** button.

This brings you back to the main *Call Router* > *Route Config* web page.

You can see a yellow **Yes** in the *Config Modified* section at the top of the window. It warns you that the configuration has been modified but not applied (i.e., the *Call Router* > *Status* differs from the *Call Router* > *Route Config*). The *Route Config* sub-menu is a working area where you build up a Call Router configuration. While you work in this area, the configured parameters are saved but not applied (i.e., they are not used to process incoming calls). The yellow **Yes** flag warns you that the configuration has been modified but is not applied.

9. Click the **Apply** button to enable the SIP headers translation entry.

The current properties applied are displayed in the *Call Router* > *Status* web page. You can also see that the yellow Config Modified **Yes** flag is cleared.

Example

The following is an example of SIP headers translations:

Figure 173: SIP Headers Translations Example

SIP Headers Translations

Index	Name	SIP Header	Built From	Fix Value
1	Header	From Header (Host Part)	Called E164	

Moving a SIP Headers Translation Row

The SIP headers translation entries sequence is very important. The signalling properties table follows the SIP headers translation table rows as they are entered in the web interface. If you want the signalling properties table to try to match one row before another one, you must put that row first.

▶ **To move a SIP headers translation entry up or down:**

1. Either click the or arrow of the row you want to move until the entry is properly located.
2. Click the **Apply** button to update the *Call Router* > *Status* web page.

Deleting a SIP Headers Translation Row

You can delete a SIP headers translation row from the table in the web interface.

▶ **To delete a SIP headers translation entry:**

1. Click the button of the row you want to delete.
2. Click the **Apply** button to update the *Call Router* > *Status* web page.

Call Properties Translations

A Call Properties Translation overrides the default value of call properties in an incoming SIP message. It modifies the call properties before the call is sent to its destination.

Like the routing table, the call properties translation table finds the first matching entry. It then executes it by modifying the behaviour of the call.

> **Note:** You can revert back to the configuration displayed in the *Call Router* > *Status* web page at any time by clicking the **Rollback** button at the bottom of the page. All modified settings in the *Call Router* > *Route Config* page will be lost.

You can add up to 100 Call Properties Translations.

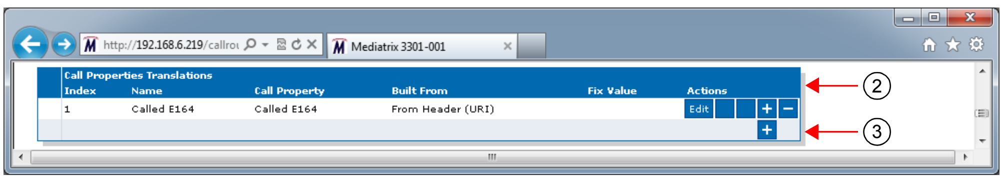
Creating/Editing a Call Properties Translation

The web interface allows you to create a call properties translation or modify the parameters of an existing one. The call properties translations are called from a signalling property as described in "Signalling Properties" on page 368.

▶ **To create or edit a call properties translation:**

1. In the web interface, click the *Call Router* link, then the *Route Config* sub-link.

Figure 174: Call Router – Route Config Web Page



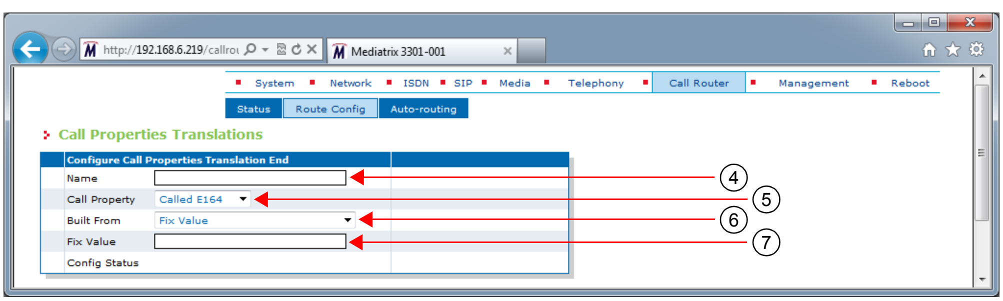
2. Locate the *Call Properties Translations* section.

3. Do one of the following:

- If you want to add a call properties translation before an existing entry, locate the proper row in the table and click the  button of this row.
- If you want to add a call properties translation at the end of existing rows, click the  button at the bottom right of the *Call Properties Translations* section.
- If you want to edit an existing entry, locate the proper row in the table and click the  button.

This brings you to the *Configure Call Properties Translation* panel.

Figure 175: Configure Call Properties Translation Panel



4. Enter the name of the call properties translation in the *Name* field.

5. Set which call property is modified by this translation in the *Call Property* drop-down menu.

Table 278: Call Properties

Call Property	Description
Called E164	Called party E.164 property.
Calling E164	Calling party E.164 property.
Called Name	Called party name property.
Calling Name	Calling party name property.
Called Uri	Called URI name property.
Calling Uri	Calling URI name property.
Called Bearer Channel	Called bearer channel property.

6. Set what information is used to build the selected call property in the *Built From* drop-down menu.

Table 279: Built From Information

Built From	Description
Domain	Use the domain name configured in the unit.
Fix Value	Use a fix value as defined in the *Fix Value* field (see Step 7).
From Header (Uri)	Use the *From* header's URI.
From Header (Friendly Name)	Use the friendly name part of the *From* header.
From Header (User Part)	Use the user part of the *From* header's URI.
Identity Header (Uri)	Use the *Identity* header's URI.
Identity Header (User Part)	Use the user part of the *Identity* header's URI.
Identity Header (Phone Number)	Use the phone number in the *Identity* header's tel URL. The phone number is not retrieved if the received tel URL is invalid. Only the phone number part is retrieved. Examples: • Received header: `P-Preferred-Identity: <tel:8298749;phone-context=819>` Retrieved phone number: 8298749 • Received header: `P-Preferred-Identity: <tel:+8298749>` Retrieved phone number: 8298749 • Received header: `P-Preferred-Identity: <tel:8298749>` Retrieved phone number: None, the received header is invalid.
Identity Header (Friendly Name)	Use the friendly name in the Identity header's URI.
Local Ip	Use the local IP address.
Request Line (Uri)	Use the Request line's URI.
Request Line (User Part)	Use the user part of the Request line's URI.
To Header (Uri)	Use the *To* header's URI.
To Header (Friendly Name)	Use the friendly name part of the *To* header.
To Header (User Part)	Use the user part of the *To* header's URI.

7. If you have selected **Fix Value** in the *Built From* drop-down menu, enter a fix value to be inserted in the call property in the *Fix Value* field.

   For instance, you could hide the callee's name in a SIP message by using the *From Header (User Part)* SIP header and entering "anonymous" in the *Fix Value* field.

8. Click the **Submit** button.

   This brings you back to the main *Call Router > Route Config* web page.

   You can see a yellow **Yes** in the *Config Modified* section at the top of the window. It warns you that the configuration has been modified but not applied (i.e., the *Call Router > Status* differs from the *Call Router > Route Config*). The *Route Config* sub-menu is a working area where you build up a Call Router configuration. While you work in this area, the configured parameters are saved but not applied (i.e., they are not used to process incoming calls). The yellow **Yes** flag warns you that the configuration has been modified but is not applied.

9. Click the **Apply** button to enable the call properties translation entry.

   The current properties applied are displayed in the *Call Router > Status* web page. You can also see that the yellow Config Modified **Yes** flag is cleared.

Example

The following is an example of call properties translations:

Figure 176: Call Properties Translations Example

Call Properties Translations

Index	Name	Call Property	Built From	Fix Value
1	Called E164	Called E164	From Header (URI)	

Moving a Call Properties Translation Row

The call properties translation entries sequence is very important. The signalling properties table follows the call properties translation table rows as they are entered in the web interface. If you want the signalling properties table to try to match one row before another one, you must put that row first.

▶ **To move a call properties translation entry up or down:**

1. Either click the or arrow of the row you want to move until the entry is properly located.
2. Click the **Apply** button to update the *Call Router > Status* web page.

Deleting a Call Properties Translation Row

You can delete a call properties translation row from the table in the web interface.

▶ **To delete a SIP headers translation entry:**

1. Click the button of the row you want to delete.
2. Click the **Apply** button to update the *Call Router > Status* web page.

Hunt Service

Routes and mappings only manipulate address properties of a call. The hunt service hunts an incoming call to multiple interfaces. It accepts a call routed to it by a route or directly from an interface and creates another call that is offered to one of the configured destination interfaces. If this destination cannot be reached, the hunt tries another destination until one of the configured destinations accepts the call. When an interface accepts a call, the interface hunting is complete and the hunt service merges the original call with the new call to the interface that accepted the call.

The hunt sequence is very important. The call router follows the hunt rows as they are entered in the web interface. If you want the call router to try to match one row before another one, you must put that row first.

> **Note:** You can revert back to the configuration displayed in the *Call Router > Status* web page at any time by clicking the **Rollback** button at the bottom of the page. All modified settings in the *Call Router > Route Config* page will be lost.

You can add up to 40 Hunts.

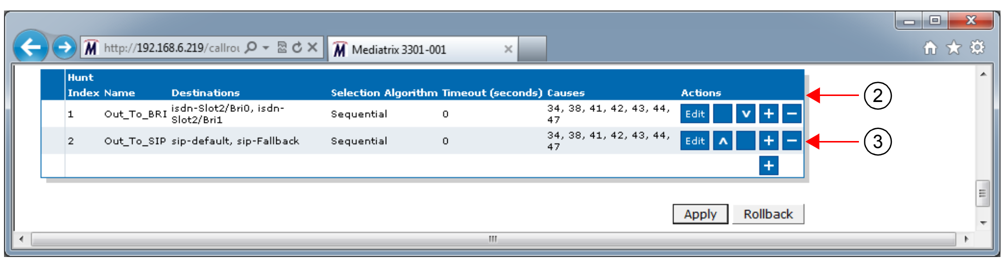
Creating/Editing a Hunt

The web interface allows you to create a hunt or modify the parameters of an existing one.

▶ **To create or edit a hunt:**

1. In the web interface, click the *Call Router* link, then the *Route Config* sub-link.

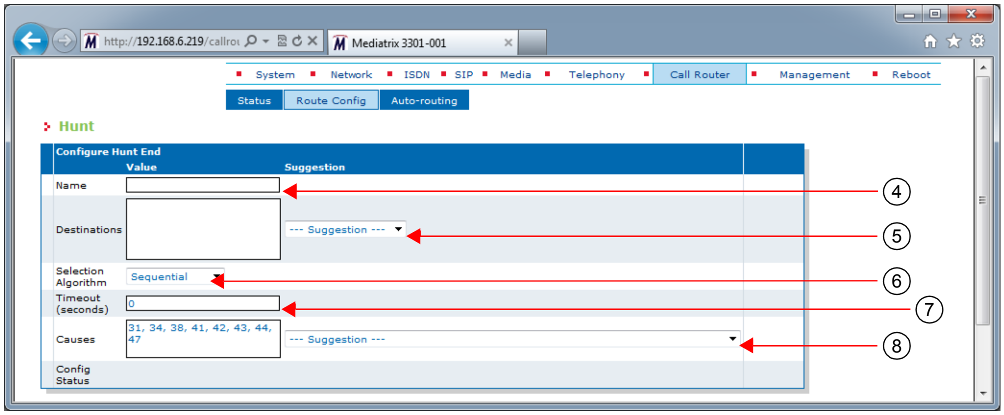
Figure 177: *Call Router* – Route Config Web Page



2. Locate the *Hunt* section.
3. Do one of the following:
   - If you want to add a hunt entry before an existing entry, locate the proper row in the table and click the + button of this row.
   - If you want to add a hunt entry at the end of existing rows, click the + button at the bottom right of the *Hunt* section.
   - If you want to edit an existing entry, locate the proper row in the table and click the Edit button.

This brings you to the *Configure Hunt* panel.

Figure 178: Configure Hunt Panel



4. Enter the name of the hunt in the *Name* field.

The name must be unique. If more than one hunt have the same name, only the first hunt is used.

5. Define a list of hunt destinations separated by commas in the *Destinations* field.

This is the interface, route, or hunt that is tried during the hunt's interface hunting. The destination can either be:

- **route-***name*: The call destination is the route *name*.
- **hunt-***name*: The call destination is the hunt *name*.
- **sip-***name*: The call destination is the SIP interface *name*.
- **isdn-***name*: The call destination is the ISDN interface *name*.
- **r2-***name*: The call destination is the R2 interface *name*.
- **e&m-***name*: The call destination is the E&M interface *name*.
- **fxs-***name*: The call destination is the FXS interface *name*.
- **fxo-***name*: The call destination is the FXO interface *name*.

Only FXS interfaces are supported if the selection algorithm **Simultaneous** is used (see Step 6).

You can use the *Suggestion* column's drop-down menu to select between suggested values, if any.

6. Select the algorithm used to select the order of the destination in the *Selection Algorithm* drop-down menu.

The algorithm can be:

- Sequential: The hunt tries the destination in the same order as listed. The first destination hunted is the first listed.
- Cyclic: The Aastra unit starts from the destination that follows the destination used for the last hunt. Subsequent calls try another first destination in a round-robin method. For instance, if the destination is set to 'x, y, z', the destination the hunt tries is in the following order:

  1. x,y,z

  2. y,z,x

  3. z,x,y

  4. x,y,z
- Simultaneous: The hunt tries every available destination at the same time. The first destination to pick up has the call. Other destinations stop ringing. This method can only have FXS endpoints as destinations.

7. Set the maximal time, in seconds (s), allowed to an interface to handle the call in the *Timeout* field.

After this timeout has elapsed, the next destination is tried when the current destination does not answer. This feature is useful to ensure a minimal time of response and fallback to other destinations. Some interfaces (e.g. SIP, which has a default timeout of 32 seconds) may wait an arbitrary long time until an answer is returned.

> **Note:** This parameter is not applicable if the selection algorithm **Simultaneous** is used (see Step 6).

Setting the field to **0** disables the timeout, which means that the call router waits indefinitely for the interface to respond. This does not affect the internal interface timeouts (the ISDN timeout as defined in ITU norms or the SIP transmission timeout) that will eventually stop the call and the call router will try another destination.

Example:

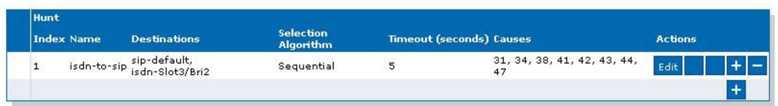
You want a call from ISDN to SIP to fallback to another ISDN interface when the SIP destination cannot be contacted within 5 seconds.

You thus create a hunt with the following destinations in order:

`sip-[gateway name], isdn-[fallback interface]`

and set the timeout to 5. The *Selection Algorithm* drop-down menu must be set to **Sequential** to always try the SIP destination first.

Figure 179: Hunt Timeout Example



The Aastra unit has the following behaviour if the SIP transmission timeout has the default value (32 seconds):

a. A new call comes from an ISDN interface and the call router sets the destination of the call to the `isdn-to-sip` hunt.

b. The call router starts the hunt timeout (5 s) and tries the first destination `sip-default`.

c. The SIP interface performs a DNS query to resolve the server name. The DNS result returns server A and server B.

d. The SIP interface sends an INVITE to the server A.

e. The hunt timeout elapses, so the call router cancels the call to the SIP interface and tries the second destination `isdn-Slot3/Bri2`. The hunt timeout is restarted.

f. The SIP interface continues to send the INVITE retransmission until the SIP transmission timeout elapses. RFC 3261 states that an INVITE request cannot be cancelled until the destination sends a response. If the destination responds before the SIP transmission timeout elapses, a CANCEL or BYE request is sent. The SIP interface will not try to use the server B location.

The Aastra unit has the following behaviour if the SIP transmission timeout is set to 3 seconds:

a. A new call comes from an ISDN interface and the call router sets the destination of the call to the `isdn-to-sip` hunt.

b. The call router starts the hunt timeout (5 s) and tries the first destination `sip-default`.

c. The SIP interface performs a DNS query to resolve the server name. The DNS result returns server A and server B.

d. The SIP interface sends an INVITE to the server A.

e. A SIP transmission timeout occurs after 4 seconds and the SIP interface sends an INVITE to the server B.

f. The hunt timeout elapses, so the call router cancels the call to the SIP interface and tries the second destination `isdn-Slot3/Bri2`. The hunt timeout is restarted.

g. The SIP interface continues to send the INVITE retransmission until the SIP transmission timeout elapses. RFC 3261 states that an INVITE request cannot be cancelled until the destination sends a response. If the destination responds before the SIP transmission timeout elapses, a CANCEL or BYE request is sent.

> **Note:** The maximal response time of a SIP interface is the transmission timeout total of all SIP destination locations + the DNS query time.

The SIP transmission timeout can be set in the *Transmission Timeout* field of the *SIP Interop* section, *SIP* > *Interop* page ("SIP Interop" on page 312).

8. Select call rejection causes to continue the hunt in the *Causes* field.

When an interface has a problem placing a call to the final destination, it drops the call by specifying a drop cause based on Q.850 ISUP drop causes. Separate the causes with commas.

See "Call Rejection (Drop) Causes" on page 382 for a list of drop causes.

You can use the *Suggestion* column's drop-down menu to select between suggested values, if any.

> **Note:** This parameter is not applicable if the selection algorithm **Simultaneous** is used (see Step 6).

9. Click the **Submit** button.

This brings you back to the main *Call Router* > *Route Config* web page.

You can see a yellow **Yes** in the *Config Modified* section at the top of the window. It warns you that the configuration has been modified but not applied (i.e., the *Call Router* > *Status* differs from the *Call Router* > *Route Config*). The *Route Config* sub-menu is a working area where you build up a Call Router configuration. While you work in this area, the configured parameters are saved but not applied (i.e., they are not used to process incoming calls). The yellow **Yes** flag warns you that the configuration has been modified but is not applied.

10. In the main *Call Routing Config* web page, click the **Apply** button to enable the hunt.

The current hunts applied are displayed in the *Call Router* > *Status* web page. You can also see that the yellow Config Modified **Yes** flag is cleared.

Examples

The following are some examples of hunts:

Figure 180: Hunt Example

Hunt Name	Destinations	Selection Algorithm	Timeout (seconds)	Causes
Out_To_BRI	isdn-Slot2/Bri0, isdn-Slot2/Bri1	Sequential	0	34, 38, 41, 42, 43, 44, 47
Out_To_SIP	sip-default, sip-Fallback	Sequential	0	34, 38, 41, 42, 43, 44, 47

Call Rejection (Drop) Causes

When a destination interface drops the call, the hunt service must supply a call rejection cause based on Q.850 ISUP drop causes. The Aastra unit offers the following drop causes categories:

- Normal Event
- Resource Unavailable
- Service or Option Not Available
- Service or Option Not Implemented
- Invalid Message
- Protocol Error
- Interworking

> **Note:** You can use any custom code between 1 and 127.

Normal Event

The following table lists all normal events drop causes. These causes are used to drop the original call.

Table 280: Normal Event Drop Causes

#	Cause	Description
1	Unassigned (unallocated) number	The calling user requested a destination that cannot be reached because the number is unassigned.
2	No route to specified transit network	The destination is asked to route the call through an unrecognized network. This may mean that: • The wrong transit network code was dialed. • The transit network does not serve this equipment. • The transit network does not exist.
3	No route to destination	The called party cannot be reached because the network through which the call has been routed does not serve the destination address.
6	Channel unacceptable	The sending entity cannot accept the channel most recently identified for use in this call.
7	Call awarded and being delivered in an established channel	The user has been awarded the incoming call, which is being connected to a channel already established to that user for similar calls.
16	Normal call clearing	The call is being cleared because one of the users involved with the call has requested that the call be cleared (usually, a call participant hung up).
17	User busy	The called party is unable to accept another call because all channels are in use. It is noted that the user equipment is compatible with the call.
18	No user responding	The called party does not respond to a call establishment message with either an alerting or connect indication within the time allotted. The number that is being dialed has an active D-channel, but the far end chooses not to answer.
19	User alerting, no answer	The called party has been alerted but does not respond with a connect indication within the time allotted.
21	Call rejected	The remote equipment can accept the call but rejects it for an unknown reason, although it could have accepted it because the equipment sending this cause is neither busy nor incompatible.
22	Number changed	The called number indicated by the calling party is no longer assigned.
26	Non-selected user clearing	The user has not been awarded the incoming call.
27	Destination out of order	The destination indicated by the user cannot be reached because the destination's interface is not functioning correctly. This can be a temporary condition, but it could last for an extended period.
28	Invalid number format (incomplete number)	The called party cannot be reached because the called party number is not in a valid format or is not complete.
29	Facility rejected	The network cannot provide the facility requested by the user.
30	Response to STATUS ENQUIRY	The STATUS message is generated in direct response to receiving a STATUS ENQUIRY message.
31	Normal, unspecified	Reports a normal event only when no other cause in the normal class applies.

Resource Unavailable

The following table lists all resource unavailable drop causes. These causes are used to hunt the next destination.

Table 281: Resource Unavailable Drop Causes

#	Cause	Description
34	No circuit/channel available	There is no appropriate circuit or channel presently available to handle the call (usually, no B-channels are available to make the selected call).
38	Network out of order	The network is not functioning properly and the condition is likely to last for an extended period.
41	Temporary failure	The network is not functioning properly and the condition should be resolved quickly.
42	Switching equipment congestion	Cannot reach the destination because the network switching equipment is temporary experiencing high traffic.
43	Access information discarded	The network could not deliver access information to the remote user as requested.
44	Requested circuit/ channel not available	The other side of the interface cannot provide the circuit or channel indicated by the requested entity.
47	Resource unavailable, unspecified	The requested channel or service is unavailable for an unknown reason.

Service or Option Not Available

The following table lists all service or option not available drop causes. These causes are used to drop the original call.

Table 282: Service or Option Not Available Drop Causes

#	Cause	Description
57	Bearer capability not authorized	The user has requested a bearer capability that is implemented on the equipment but the user is not authorized to use it.
58	Bearer capability not presently available	The user has requested a bearer capability that is implemented by the equipment and is currently unavailable.
63	Service or option not available, unspecified	The network or remote equipment cannot provide the requested service option for an unspecified reason.

Service or Option Not Implemented

The following table lists all service or option not implemented drop causes. These causes are used to drop the original call.

Table 283: Service or Option Not Implemented Drop Causes

#	Cause	Description
65	Bearer capability not implemented	The remote equipment does not support the requested bearer capability.
66	Channel type not implemented	The remote equipment does not support the requested channel type.
69	Requested facility not implemented	The remote equipment does not support the requested supplementary service.

Table 283: Service or Option Not Implemented Drop Causes (Continued)

#	Cause	Description
70	Only restricted digital information bearer capability is available	The calling party has requested an unrestricted bearer service but the remote equipment only supports the restricted version of the requested bearer capacity.
79	Service or option not implemented, unspecified	The network or remote equipment cannot provide the requested service option for an unspecified reason. This can be a subscription problem.

Invalid Message

The following table lists all invalid message drop causes. These causes are used to drop the original call.

Table 284: Invalid Message Drop Causes

#	Cause	Description
81	Invalid call reference value	The remote equipment has received a message with a call reference that is not currently in use on the user-network interface.
82	Identified channel does not exist	Indicates a call attempt on a channel that is not configured.
83	A suspended call exists, but this call identity does not	Attempted to resume a call with a call identity that differs from the one in use for any presently suspended calls.
84	Call identity in use	The network has received a call suspended request containing a call identity that is already in use for a suspended call.
85	No call suspended	The network has received a call resume request containing a call identity information element that does not indicate any suspended call.
86	Call having the requested call identity has been cleared	The network has received a call identity information element indicating a suspended call that has in the meantime been cleared while suspended.
88	Incompatible destination	The remote equipment has received a request to establish a call with compatibility attributes that cannot be accommodated.
91	Invalid transit network selection	Received a transit network identification of an incorrect format was received.
95	Invalid message, unspecified	Received an invalid message event.

Protocol Error

The following table lists all protocol error drop causes. These causes are used to drop the original call.

Table 285: Protocol Error Drop Causes

#	Cause	Description
96	Mandatory information element is missing	The remote equipment has received a message that is missing an information element (IE). This IE must be present in the message before the message can be processed.
97	Message type non-existent or not implemented	The remote equipment has received a message with a missing information element that must be present in the message before the message can be processed.

Table 285: Protocol Error Drop Causes (Continued)

#	Cause	Description
98	Message not compatible with call state or message type non-existent or not implemented	The remote equipment has received a message that is not allowed while in the current call state.
99	Information element non-existent or not implemented	The remote equipment has received a message that includes information elements or parameters that are not recognized.
100	Invalid information element contents	The remote equipment has received a message that includes invalid information in the information element or call property.
101	Message not compatible with call state	Received an unexpected message that is incompatible with the call state.
102	Recovery on time expiry	A procedure has been initiated by the expiration of a timer in association with error handling procedures.
111	Protocol error, unspecified	An unspecified protocol error with no other standard cause occurred.

Interworking

The following table lists all interworking drop causes. These causes are used to drop the original call.

Table 286: Interworking Drop Causes

#	Cause	Description
127	Interworking, unspecified	An event occurs, but the network does not provide causes for the action it takes. The precise problem is unknown.

Moving a Hunt

The hunt sequence is very important. The call router follows the hunt rows as they are entered in the web interface. If you want the call router to try to match one row before another one, you must put that row first.

▶ **To move a hunt entry up or down:**

1. Either click the ^ or v arrow of the row you want to move until the entry is properly located.
2. Click the **Apply** button to update the *Call Router* > *Status* web page.

Deleting a Hunt

You can delete a hunt row from the table in the web interface.

▶ **To delete a hunt entry:**

1. Click the − button of the row you want to move.
2. Click the **Apply** button to update the *Call Router* > *Status* web page.

SIP Redirects

The SIP Redirect allows SIP redirections to be configured. These SIP Redirect entries can be used as destinations in route rules. This type of destination is valid only when the Source of the route rule is a SIP interface.

When a route rule is configured with a SIP Redirect destination, incoming SIP Invites are replied with a 302 "Moved Temporarily" SIP response.

> **Note:** You can revert back to the configuration displayed in the *Call Router* > *Status* web page at any time by clicking the **Rollback** button at the bottom of the page. All modified settings in the *Call Router* > *Route Config* page will be lost.

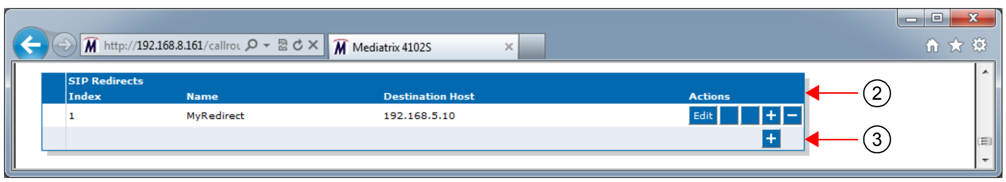
Creating/Editing a SIP Redirect

The web interface allows you to create a SIP Redirect or modify the parameters of an existing one.

▶ **To create or edit a SIP Redirect:**

1. In the web interface, click the *Call Router* link, then the *Route Config* sub-link.

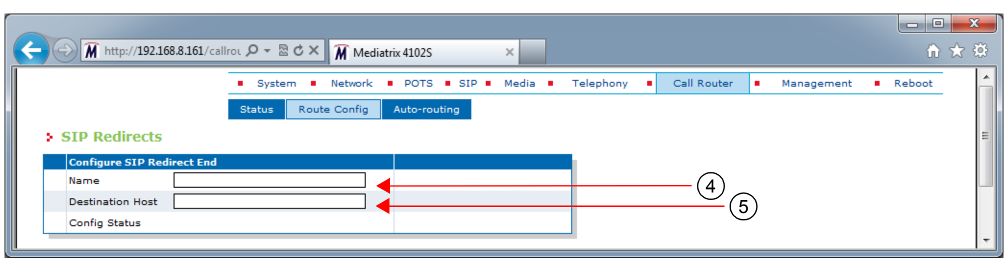
Figure 181: *Call Router* – Route Config Web Page



2. Locate the *SIP Redirects* section.
3. Do one of the following:
   - If you want to add a SIP Redirect entry before an existing entry, locate the proper row in the table and click the + button of this row.
   - If you want to add a SIP Redirect entry at the end of existing rows, click the + button at the bottom right of the *SIP Redirects* section.
   - If you want to edit an existing entry, locate the proper row in the table and click the Edit button.

   This brings you to the *Configure SIP Redirect* panel.

Figure 182: Configure SIP Redirect Panel



4. Enter the name of the SIP Redirect in the *Name* field.

   The name must be unique. If more than one SIP Redirect have the same name, only the first SIP Redirect is used.
5. Set the *Destination Host* field with the host address inserted in the Moved Temporarily response.
6. Click the **Submit** button.

This brings you back to the main *Call Router* > *Route Config* web page.

You can see a yellow **Yes** in the *Config Modified* section at the top of the window. It warns you that the configuration has been modified but not applied (i.e., the *Call Router* > *Status* differs from the *Call Router* > *Route Config*). The *Route Config* sub-menu is a working area where you build up a Call Router configuration. While you work in this area, the configured parameters are saved but not applied (i.e., they are not used to process incoming calls). The yellow **Yes** flag warns you that the configuration has been modified but is not applied.

7. In the main *Call Routing Config* web page, click the **Apply** button to enable the SIP Redirect.

The current SIP Redirects applied are displayed in the *Call Router* > *Status* web page. You can also see that the yellow Config Modified **Yes** flag is cleared.

Examples

The following are some examples of SIP Redirects:

Figure 183: SIP Redirects Example

SIP Redirects		
Index	Name	Destination Host
1	MyRedirect	192.168.5.10

Moving a SIP Redirect

The SIP Redirect sequence is very important. The call router follows the SIP Redirect rows as they are entered in the web interface. If you want the call router to try to match one row before another one, you must put that row first.

▶ **To move a SIP Redirect entry up or down:**

1. Either click the or arrow of the row you want to move until the entry is properly located.

2. Click the **Apply** button to update the *Call Router* > *Status* web page.

Deleting a SIP Redirect

You can delete a SIP Redirect row from the table in the web interface.

▶ **To delete a SIP Redirect entry:**

1. Click the button of the row you want to move.

2. Click the **Apply** button to update the *Call Router* > *Status* web page.

Configuration Examples

The following are examples of configuration you could do with the call router.

Figure 184: Configuration Examples

Route

Index	Source	Properties Criteria	Expression Criteria	Mappings	Signaling Properties	Destination	Actions
1	sip-default	None		Out_To_PSTN	Early_Connect	hunt-Out_To_BRI	Edit
2	isdn-Slot2/Bri0	None		Out_of_Office_Hours_AM, Out_of_Office_Hours_PM	Early_Disconnect	hunt-Out_To_SIP	Edit

Mapping Type

Index	Name	Criteria	Transformation	Actions
1	Out_To_PSTN	Called E164	Called E164	Edit
2	Out_of_Office_Hours_PM	Date/Time	Called E164	Edit
3	Out_of_Office_Hours_AM	Date/Time	Called E164	Edit

Mapping Expression

Index	Name	Criteria	Transformation	Sub Mappings	Actions
1	Out_To_PSTN	.*	9\0		Edit
2	Out_of_Office_Hours_AM	MON, TUE, WED, THU, FRI/00:00:00-08:00:00	981		Edit
3	Out_of_Office_Hours_PM	MON, TUE, WED, THU, FRI/17:00:00-23:59:59	981		Edit

Signaling Properties

Index	Name	Early Connect	Early Disconnect	Destination Host	Allow 180 with SDP	Allow 183 without SDP	Privacy	SIP Headers Translations	Call Properties Translations	Actions
1	Disconnect	Disable	Enable		Enable	Disable	Disable	From Header		Edit
2	Connect	Enable	Disable		Disable	Enable	Disable		Called E164	Edit

SIP Headers Translations

Index	Name	SIP Header	Built From	Fix Value	Actions
1	From Header	From Header (Host Part)	Called E164		Edit

Call Properties Translations

Index	Name	Call Property	Built From	Fix Value	Actions
1	Called E164	Called E164	From Header (URI)		Edit

Hunt

Index	Name	Destinations	Selection Algorithm	Timeout (seconds)	Causes	Actions
1	Out_To_BRI	isdn-Slot2/Bri0, isdn-Slot2/Bri1	Sequential	0	34, 38, 41, 42, 43, 44, 47	Edit
2	Out_To_SIP	sip-default, sip-Fallback	Sequential	0	34, 38, 41, 42, 43, 44, 47	Edit

SIP Redirects

Index	Name	Destination Host	Actions
1	MyRedirect	192.168.5.10	Edit

CHAPTER 39

Auto-Routing Configuration

This chapter describes the auto-routing feature.

Auto-Routing

The auto-routing feature is an aid to call routing configuration. When this feature is enabled, routing rules are automatically generated for all endpoints marked as "Auto-routable". For each auto-routable endpoint, two rules are generated and added to the Call Router: one directing incoming calls from the associated auto-routing SIP gateway to the endpoint, and one sending outgoing calls from the endpoint to the associated auto-routing SIP gateway.

The auto-routing routes are not displayed in the *Route Configuration* page because you cannot edit them. They are however listed in the *Status* page and are attributed a type:

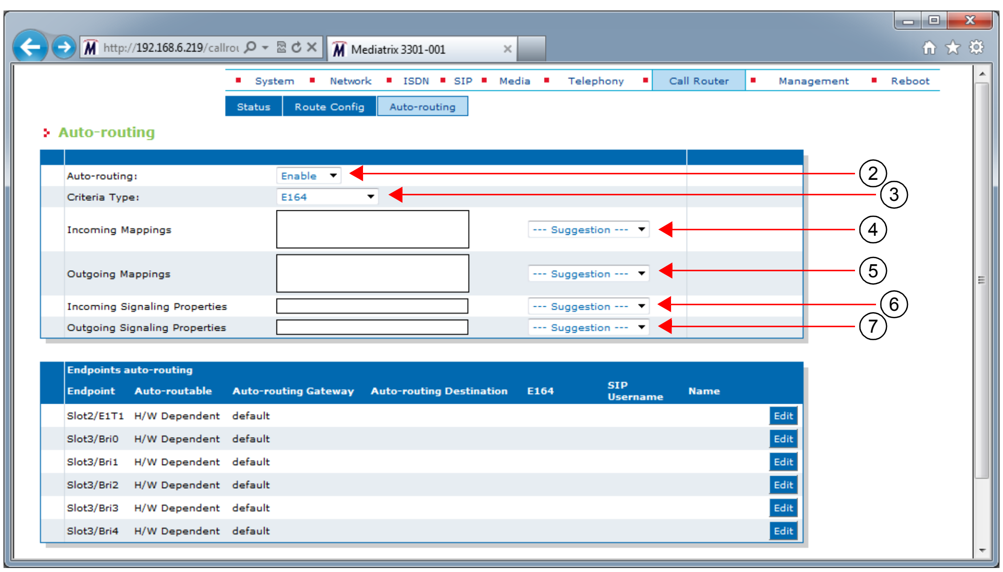
- User: the route has been manually entered by the user.
- Auto: this is an auto-routing route.

> **Note:** Auto-routing can only be used if the username of the endpoint is an E.164 string and the username part of the request-URI of the received INVITE can be converted into an E.164. See “Manual Routing” on page 394 for more details.

To activate auto-routing:

1. In the web interface, click the *Call Router* link, then the *Auto-routing* sub-link.

Figure 185: Call Router – Auto-Routing Web Page



2. In the top section, set the *Auto-routing* drop-down menu with the proper behaviour.

   If you select **Enable**, routes are automatically added to the Route Table in order to connect the endpoints marked as eligible for auto-routing (see Step 3) and the designated SIP gateway (see Step 4). These automatic routes are displayed in the *Call Router* > *Status* page, but do not show up in the *Call Router* > *Route Configuration* page.

3. Select the type of criteria to use to create automatic rules from SIP to the telephony endpoints in the *Criteria Type* drop-down menu.

Table 287: Criteria Types

Parameter	Description
E164	The E.164 associated with the endpoint is used as criterion.
Sip Username	The SIP username associated with the endpoint is used as criterion.

4. Set the *Incoming Mappings* field with the name of the properties manipulations associated with the route from the SIP gateway to the endpoint.

   You can specify more than one mapping by separating them with ','. They are executed in sequential order. See “Mappings” on page 484 for more details.

   You can use the *Suggestion* column’s drop-down menu to select between suggested values, if any.

5. Set the *Outgoing Mappings* field with the name of the properties manipulations associated with the route from the endpoint to the SIP gateway.

   You can specify more than one mapping by separating them with ','. They are executed in sequential order. See “Mappings” on page 484 for more details.

   You can use the *Suggestion* column’s drop-down menu to select between suggested values, if any.

6. Set the *Incoming Signaling Properties* field with the name of the signaling properties associated with the route from the SIP gateway to the endpoint.

   See “Signalling Properties” on page 494 for more details.

   You can use the *Suggestion* column’s drop-down menu to select between suggested values, if any.

7. Set the *Outgoing Signaling Properties* field with the name of the signaling properties associated with the route from the endpoint to the SIP gateway.

   See “Signalling Properties” on page 494 for more details.

   You can use the *Suggestion* column’s drop-down menu to select between suggested values, if any.

8. Click the **Submit** button to enable auto-routing.

   The current routes applied are displayed in the *Call Router* > *Status* web page. They are added at the end of the routes that are already present, if any. This ensures that the user-defined routes always have precedence over the automatic routes when both types of routes apply to the same endpoint.

Endpoints Auto-Routing

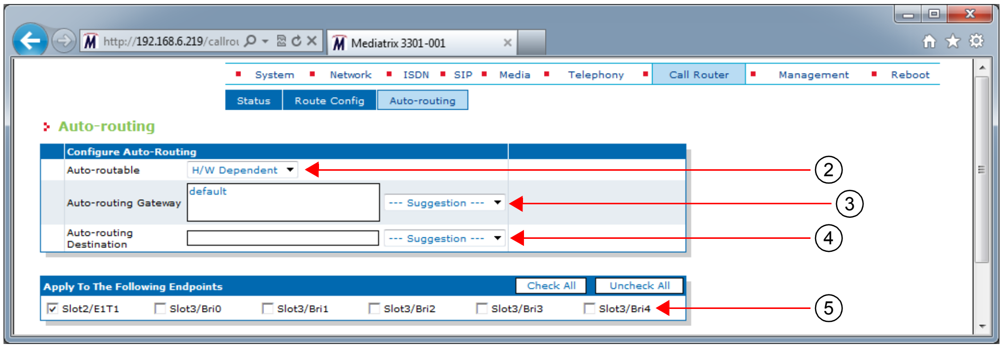
This section allows you to link an endpoint to several SIP gateways.

▶ **To set Endpoints auto-routing parameters:**

1. In the *Endpoints auto-routing* section of the *Auto-routing* page, locate the proper endpoint in the table and click the Edit button.

   The Configure Auto-Routing page displays:

Figure 186: Configure Auto-Routing Section



2. Select whether or not automatic routes are generated for the endpoint when auto-routing is enabled in the *Auto-routable* drop-down menu.

Table 288: Auto-routable Parameters

Parameter	Description
Enable	Automatic routes allowing incoming and outgoing calls to and from the endpoint are added to the Route Table when auto-routing is enabled.
Disable	Automatic route generation is turned off for this endpoint.
HardwareDependent	Automatic routes are generated if the endpoint belongs to an FXS interface.

3. Select the SIP gateways to use as the destination of outgoing calls and the source of incoming calls when generating auto-routing rules in the *Auto-routing Gateway* drop-down menu.

You can use the *Suggestion* column's drop-down menu to select between suggested values, if any.

If you leave the field blank, it is the same as disabling the auto-routing feature.

More than one SIP gateway can be defined. The SIP gateways names are separated by comas. Example:

```
gw1,gw2,gw3
```

When one SIP gateway is defined:

- A route is automatically created from the SIP gateway to the telephony interface.
- A route is automatically created from the telephony interface to the SIP gateway if the *Auto-routing Destination* field is empty. Otherwise, the destination of the route uses the destination defined in the *Auto-routing Destination* field.

When several SIP gateways are defined:

- Routes are automatically created from each defined SIP gateway to the telephony interface.
- A route is automatically created from the telephony interface to the destination defined in the *Auto-routing Destination* field. No route is created if the destination is left empty.

If available, two additional parameters are displayed:

- If an endpoint has a telephone number that is associated with it, it is displayed in the corresponding *E164* column. This is the *User Name* field as configured in the *SIP > Registration* page as long as the name follows the E.164 syntax.
- If an endpoint has a friendly name that is associated with it, it is displayed in the corresponding *Name* column. This is the *Friendly Name* field as configured in the *SIP > Registration* page.

Pleas note that routes are created only if a user name is associated with the telephony endpoint in the registration table. See "Endpoints Registration" on page 289 for more details.

4. Set the destination to use for the routes from the telephony interface in the *Auto-routing Destination* field.

   You can use the *Suggestion* column's drop-down menu to select between suggested values, if any. The destination can be:

   - **route**-*name*: The route destination is set to the route *name*.
   - **hunt**-*name*: The route destination is set to the hunt *name*.
   - **sip**-*name*: The route destination is set to the SIP interface *name*.
   - **isdn**-*name*: The route destination is set to the ISDN interface *name*.
   - **r2**-*name*: The route destination is set to the R2 interface *name*.
   - **e&m**-*name*: The route destination is set to the E&M interface *name*.
   - **fxs**-*name*: The route destination is set to the FXS interface *name*.
   - **fxo**-*name*: The route destination is set to the FXO interface *name*.

5. You can copy the configuration of the selected endpoint to one or more endpoints of the Aastra unit in the *Apply to the Following Endpoints* section at the bottom of the page. You can select specific endpoints by checking them, as well as use the *Check All* or *Uncheck All* buttons.

6. When you are finished, you have the choice to:

   - Click the **Submit** button to enable auto-routing.

     The current routes applied are displayed in the *Call Router* > *Status* web page. They are added at the end of the routes that are already present, if any. This ensures that the user-defined routes always have precedence over the automatic routes when both types of routes apply to the same endpoint.

   - Click the **Submit & Create Hunt** button to perform a submit action and go to the hunt creation page. This option is available only if the destination is set to an unexisting hunt.
   - Click the **Submit & Edit Hunt** button to perform a submit action and go to the hunt edition page. This option is available only if the destination is set to an existing hunt.
   - Click the **Submit & Create Route** button to perform a submit action and go to the route creation page. This option is available only if the destination is set to an unexisting route.
   - Click the **Submit & Edit Route** button to perform a submit action and go to the route edition page. This option is available only if the destination is set to an existing route.

Manual Routing

Auto-routing can only be used if the username of the endpoint is an E.164 string and the username part of the request-URI of the received INVITE can be converted into an E.164.

The conversion of a username into an E.164 follows these rules:

- The prefix "+" is removed. Note that if the *Map Plus To TON International* drop-down menu is set to **Enable**, the call property 'type of number' is set to 'international'. See "Misc Interop" on page 319 for more details.
- The visual separator "-" is removed.
- The username parameter is removed. The username parameter is a suffix beginning with ";".
- All remaining characters need to be "0123456789*#abcdABCD".

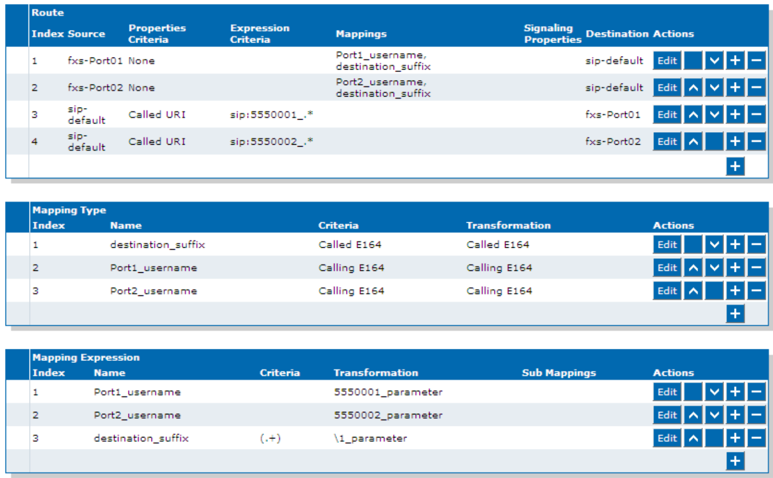
Examples of conversion:

```
5551234 --> 5551234
#20 --> #20
555-1234 --> 5551234
+1-819-555-1234 --> 18195551234
5551234;parameter --> 5551234
5551234_parameter --> cannot convert
```

To use a username not compatible with E.164, you must disable the auto-routing and use manual routes.

Figure 187 gives an example of manual routes for an endpoint using "5550001_paramter" as user.

Figure 187: Manual Routes Example



Route							
Index	**Source**	**Properties Criteria**	**Expression Criteria**	**Mappings**	**Signaling Properties**	**Destination**	**Actions**
1	fxs-Port01	None		Port1_username, destination_suffix		sip-default	Edit
2	fxs-Port02	None		Port2_username, destination_suffix		sip-default	Edit
3	sip-default	Called URI	sip:5550001_.*			fxs-Port01	Edit
4	sip-default	Called URI	sip:5550002_.*			fxs-Port02	Edit

Mapping Type				
Index	**Name**	**Criteria**	**Transformation**	**Actions**
1	destination_suffix	Called E164	Called E164	Edit
2	Port1_username	Calling E164	Calling E164	Edit
3	Port2_username	Calling E164	Calling E164	Edit

Mapping Expression					
Index	**Name**	**Criteria**	**Transformation**	**Sub Mappings**	**Actions**
1	Port1_username		5550001_parameter		Edit
2	Port2_username		5550002_parameter		Edit
3	destination_suffix	(.+)	\1_parameter		Edit

Management Parameters

Page Left Intentionally Blank

CHAPTER

40 Configuration Script

This chapter describes the configuration script download feature, which allows updating the Aastra unit configuration by transferring a configuration script from a remote server or from the local file system. The Aastra unit is the session initiator, which allows NAT traversal. You can also configure the Aastra unit to automatically update its configuration.

You can also generate a configuration script from the running configuration of the Aastra unit.

Configuration scripts are files containing textual commands that are sent over the network to a Aastra unit. Upon receiving the file, the unit executes each command line in sequence. Script commands can assign values to configuration variables, or execute configuration commands. See "Creating a Configuration Script" on page 414 for more details on how to create a configuration script.

Scripts are written by the system administrator and can be used to accomplish various tasks, such as automating recurrent configuration tasks or batch-applying configuration settings to multiple devices. Scripts can be executed once or periodically at a specified interval. They can also be scheduled to execute when the Aastra unit restarts.

This chapter describes the following:

- Configuration script server setup.
- Configuration script server parameters.
- Configuration download procedure.
- Generating a configuration script from the running configuration.
- Automatic configuration update parameters.
- How to create a configuration script from scratch.

Standards Supported	• RFC 959: File Transfer Protocol (client-side only) • RFC 1350: The TFTP Protocol (Revision 2) (client-side only) • RFC 2616: Hypertext Transfer Protocol - HTTP/1.1 (client-side only) • RFC 2617: HTTP Authentication: Basic and Digest Access Authentication • RFC 3617: Uniform Resource Identifier (URI) Scheme for the Trivial File Transfer Protocol • draft-ietf-http-authentication-03

Configuration Script Server

To download a configuration script, you may need to setup the following applications on your computer:

- TFTP server with proper root path
- SNTP server properly configured
- HTTP server with proper root path
- HTTPS server with proper root path

Configuring the TFTP Server

When you perform a configuration script download by using the TFTP (Trivial File Transfer Protocol) protocol, you must install a TFTP server running on the PC designated as the TFTP server host. It is assumed that you know how to set the TFTP root path. If not, refer to your TFTP server's documentation.

Configuring the SNTP Server

When you use the automatic configuration script update feature (see “Automatic Configuration Update” on page 410 for more details) or the HTTPS protocol, you need to have a time server SNTP that is accessible and properly configured. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server’s documentation. You can also refer to “SNTP Configuration” on page 93 for more details on how to configure the Aastra unit for a SNTP server.

Note: The Aastra unit hardware does not include a real time clock. The unit uses the SNTP client to get and set its clock. As certain services need correct time to work properly (such as HTTPS), you should configure your SNTP client with an available SNTP server in order to update and synchronise the local clock at boot time.

Configuring the HTTP Server

When you to perform a configuration script download by using the HTTP protocol, you must install a HTTP server running on the PC designated as the server host. It is assumed that you know how to set the root path. If not, refer to your HTTP server’s documentation.

Configuring the HTTPS Server

Standards Supported	• RFC 2246: The TLS Protocol Version 1.0 • RFC 2459: X.509 Digital Certificates • RFC 2818: HTTP Over TLS (client side only) • RFC 3268: Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS) • RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

When you perform a configuration script download that requires authentication or privacy by using the HTTP over the Transport Layer Security (TLS) protocol (HTTPS), you must install a HTTPS server running on the PC designated as the server host. It is assumed that you know how to set the root path and SSL/TLS security configuration. If not, refer to your HTTPS server’s documentation.

Caution: You must have a time server SNTP that is accessible and properly configured, or the automatic configuration update feature may not work properly. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server’s documentation. You can also refer to “SNTP Configuration” on page 93 for more details on how to configure the Aastra unit for a SNTP server.

When two peers establish a HTTPS connection, they negotiate and decide on a cipher suite to use for data encryption. The client suggests a list of cipher suites and the server selects one that it supports. Some cipher suites are more secured than others. The Aastra unit acts as a client.

The Aastra unit suggests a wide range of cypher suites, which includes cipher suites that are not very secure. The final choice rests with the server and it is thus possible that the transfer uses a SSL/TLS link that is not very secure.

Aastra recommends to use cipher suites based on the RSA key exchange mechanism, because the Diffie-Hellman key exchange mechanism introduces a noticeable delay in the HTTPS session establishment. Furthermore, Aastra recommends using cipher suites based on the following SSL/TLS algorithms:

Table 289: Suggested Secure Parameters

Suggested Parameter	Description
Key Exchange Mechanism	• RSA • Diffie-Hellman
Ciphers	• AES (128 and 256 bits) • 3DES (168 bits)

Table 289: Suggested Secure Parameters (Continued)

Suggested Parameter	Description
Message Digests	• SHA-1

The following six recommended cipher suites are based on the algorithms of Table 289:

Table 290: Recommended Cipher Suites

ID	Name
0x0035	TLS_RSA_WITH_AES_256_CBC_SHA
0x0039	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
0x000a	TLS_RSA_WITH_3DES_EDE_CBC_SHA
0x0016	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
0x002f	TLS_RSA_WITH_AES_128_CBC_SHA
0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Certificates

The Aastra unit contains embedded security certificates formatted as per ITU x.509 and RFC 3280. The certificates are factory-installed. You can also add new certificates as described in “Chapter 46 - Certificates Management” on page 557.

When contacting a HTTPS server, the Aastra unit establishes a TLS connection by (among others):

- negotiating cipher suites
- checking the server certificates validity (dates)

The Aastra unit then checks the server’s identity by validating the host name used to contact it against the information found in the server’s certificate, as described in RFC 2818, section 3.1.

If any of the above does not succeed, the Aastra unit refuses the secure connection. To help detect such errors, you can increase the syslog messages level.

Generating a Configuration Script from the Running Configuration

You can generate a configuration script from the running configuration of the Aastra unit and export it.

You can export the configuration in two ways:

- To a URL you specify with one of the supported transfer protocols.
- By directly downloading the exported script via your web browser. This option uses the protection provided by your web browser (it is protected if you log on to the unit via HTTPS).

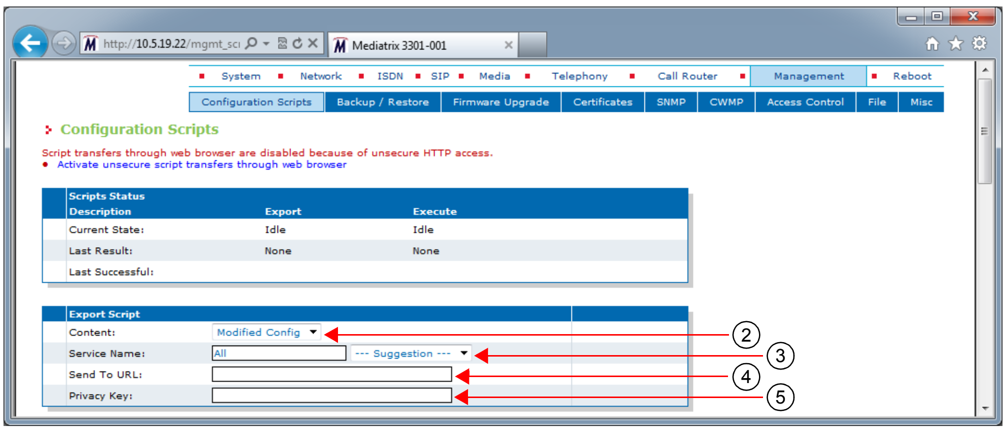
Exporting a Configuration to a URL

The *Export Script* section allows you to generate a configuration script from the running configuration of the Aastra unit and export it.

To export a configuration to a URL:

1. In the web interface, click the *Management* link, then the *Configuration Scripts* sub-link.

Figure 188: Management – Configuration Scripts Web Page



2. Select the content to export in the generated configuration script in the *Content* drop-down menu.

Table 291: Exported Configuration Script Content

Parameter	Description
All Config	Exports everything.
Modified Config	Export only the configuration that has been modified (differs from the default values).

3. Set the *Service Name* field with the name of the service from which to export configuration.

   You can use the *Suggestion* drop-down menu to select one of the available services. You can use the special value **All** to export the configuration of all services.

4. Set the *Send To URL field* with the URL where to send the exported configuration script.

   The URL should follow this format:

   `protocol://[user[:password]@]hostname[:port]/[path/]filename`

   The brackets [ ] denote an optional parameter.

   The filename may contain a %mac% macro that is substituted by the MAC address of the unit at the moment of sending the configuration script. For instance, the “%mac%.cfg” value for a Aastra unit with MAC address “0090f12345ab” will be “0090f12345ab.xml”.

   The filename may contain macros that are substituted at the moment of sending the configuration script. The supported macros are:

- %mac% - the MAC address of the unit
- %version% - the MFP version of the unit

For instance, the "%mac%.cfg" value for a Aastra unit with MAC address "0090f12345ab" will be "0090f12345ab.xml".

The transfer protocols supported are:

- TFTP
- FTP
- FILE

Examples of valid URLs:

- tftp://tftpserver.com:69/folder/script.cfg
- ftp://guest@ftpserver.com/script.cfg
- ftp://username:password@ftpserver.com/script.cfg
- file://script.cfg

The protocol's default port is used if none is specified.

5. Set the *Privacy Key* field with the key used to encrypt the configuration script to export.

> **Caution:** The *Privacy Key* field is not accessible if you have the User or Observer access right. See "Users" on page 591 for more details.

The key is encoded in hexadecimal notation. You can thus use characters in the range 0-9, A-F, and a-f. All other characters are not supported.

The maximum key length is 64 characters, which gives a binary key of 32 bytes (256 bits). It is the maximum key size supported by the MxCryptFile application.

For instance, a 32-bit key could look like the following: `A36CB299`.

If the field is empty, the configuration script is not encrypted.

To decrypt the exported configuration script, you must use the MxCryptFile application. MxCryptFile is a command line tool that encrypts or decrypts files to be exchanged with the Aastra unit. Contact your sales representative for more details.

6. Initiate the configuration scripts exportation by clicking the **Submit & Export Now** button at the bottom of the page.

The Aastra unit immediately generates and transfers a configuration script based on the export settings set in the previous steps.

Exporting a Configuration Script to your PC

This section describes how to export the configuration of a Aastra unit to the PC.

If you are currently using an unsecure HTTP access, script transfers through web browser are disabled. This is to avoid transferring the configuration in clear text. To enable the section, you can:

- Access the secure site (recommended) by clicking the corresponding link at the top of the window. This is the recommended way to proceed.
- Activate unsecure certificate transfer by clicking the corresponding link at the top of the window. This is not recommended.

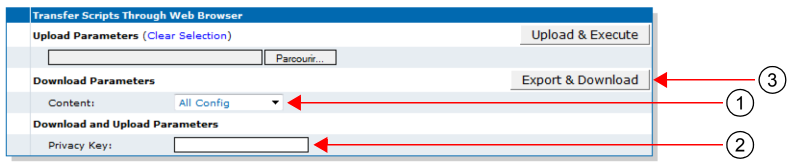
▶ To export a configuration script to the PC:

1. In the *Transfer Scripts Through Web Browser* section of the *Configuration Scripts* page, select the content to export in the generated configuration script in the *Content* drop-down menu.

Table 292: Exported Configuration Script Content

Parameter	Description
All Config	Exports everything.
Modified Config	Export only the configuration that has been modified (differs from the default values).

Figure 189: Transfer Scripts Through Web Browser Section



2. If required, set the *Privacy Key* field with the key used to encrypt the configuration script to export.

Caution: The *Privacy Key* field is not accessible if you have the User or Observer access right. See "Users" on page 591 for more details.

The key is encoded in hexadecimal notation. You can thus use characters in the range 0-9, A-F, and a-f. All other characters are not supported.

The maximum key length is 64 characters, which gives a binary key of 32 bytes (256 bits). It is the maximum key size supported by the MxCryptFile application.

For instance, a 32-bit key could look like the following: `A36CB299`.

If the field is empty, the configuration script is not encrypted.

To decrypt the exported configuration script, you must use the MxCryptFile application. MxCryptFile is a command line tool that encrypts or decrypts files to be exchanged with the Aastra unit. Contact your sales representative for more details.

3. Click the **Export & Download** button.

Executing Configuration Scripts Settings

You can execute the configuration in two ways:

- From the configuration script server URL that you specify with one of the supported transfer protocols.
- By directly executing the script via your web browser. This option uses the protection provided by your web browser (it is protected if you log on to the unit via HTTPS).

Executing a Script from the Configuration Script Server

This section describes how to configure the IP address and port number of the configuration script server. This server contains the configuration scripts the Aastra unit will download.

When performing a configuration script download, you can download two different scripts:

- A generic configuration script that should be used to update a large number of units with the same configuration.
- A specific configuration script that contains the configuration for a single unit, for instance the telephone numbers of its endpoints.

You can use a specific configuration script but no generic configuration script or vice-versa. You can also use both generic and specific configuration scripts. When both the generic and specific configuration scripts are downloaded, settings from the specific configuration script always override the settings from the generic configuration script. These scripts must be located in the same directory.

Each script is executed independently from the other one. A script that is empty, cannot be found or has an invalid syntax does not prevent the execution of the other script. If one or both scripts fail, error messages are sent.

To set the configuration scripts server parameters:

1. In the *Configuration Scripts* section of the *Configuration Scripts* page, set the name of the generic configuration script to download in the *Generic File Name* field.

   This script should be used to update a large number of units with the same configuration. The script name is case sensitive hence it must be entered properly.

   If you select **File** in the Transfer Protocol drop-down menu (Step 4), this means that you can select a script located in the unit's persistent file system. You can use the *Suggestion* drop-down menu to select one of the available scripts in the file system.

   To see the content of the unit's file system persistent memory, go to the File Manager ("Chapter 50 - File Manager" on page 597). All installed configuration scripts/images are listed.

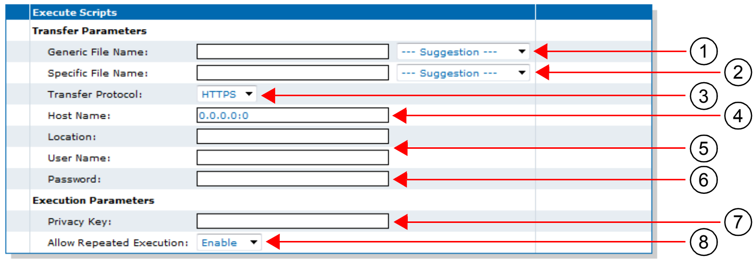
   This field may contain some macros that are substituted by the actual value at the moment of fetching the configuration script. The supported macros are:

   - %mac% - the MAC address of the unit
   - %version% - the MFP version of the unit
   - %product% - the Product name of the unit.
   - %productseries% - the Product series name of the unit.

   For instance, the "%mac%.xml" value for a Aastra unit with MAC address "0090f12345ab" will be "0090f12345ab.xml".

   If you leave the field empty, the Aastra unit does not download the generic configuration script.

Figure 190: Execute Scripts Section



2. Set the name of the specific configuration script to download in the *Specific File Name* field.

This script should be used to update the configuration of a single unit. The script name is case sensitive hence it must be entered properly.

If you select **File** in the Transfer Protocol drop-down menu (Step 4), this means that you can select a script located in the unit's persistent file system. You can use the *Suggestion* drop-down menu to select one of the available scripts in the file system.

To see the content of the unit's file system persistent memory, go to the File Manager ("Chapter 50 - File Manager" on page 597). All installed configuration scripts/images are listed.

This field may contain a macro that is substituted by the actual value when downloading the configuration script. The Aastra unit supports the %mac% macro, which will be substituted by the MAC address of the unit. For instance, the "%mac%.xml" value for a Aastra unit with MAC address "0090f12345ab" will be "0090f12345ab.xml".

This field may contain some macros that are substituted by the actual value when downloading the configuration script. The supported macros are:

- %mac% - the MAC address of the unit
- %version% - the MFP version of the unit
- %product% - the Product name of the unit.
- %productseries% - the Product series name of the unit.

For instance, the "%mac%.xml" value for a Aastra unit with MAC address "0090f12345ab" will be "0090f12345ab.xml".

If the variable is empty (after macro substitution), the Aastra unit does not download the specific configuration script.

3. Set the path of the directory where the configuration scripts are located in the *Location* field.

The path is case sensitive hence it must be entered properly. It is relative to the root of the configuration scripts server. Use the "/" character when defining the path to indicate sub-directories.

This field may contain some macros that are substituted by the actual value when downloading the configuration script. The supported macros are:

- %mac% - the MAC address of the unit
- %version% - the MFP version of the unit
- %product% - the Product name of the unit.
- %productseries% - the Product series name of the unit.

For instance, the "%mac%.xml" value for a Aastra unit with MAC address "0090f12345ab" will be "0090f12345ab.xml".

The path differs depending on the transfer protocol selected (see Step 5).

Example: All Transfer Protocols Except File

Let's consider the following example for all protocols except File:

- The directory that contains the configuration script is called: **Config_Script**.

- This directory is under **C:/Root/Download**.

Table 293: Path Configurations Example

Root Path	Corresponding Path Name
c:/root/download	Config_Script
c:/	root/download/Config_Script
c:/root	download/Config_Script

The following are some tips to help your download process:

- Use the "/" character when defining the path to indicate sub-directories. For instance, *root/download*.
- If you are using the TFTP protocol to download the software, note that some TFTP servers on Windows do not recognize the "/" character and produce an error. In this case, use the "\" character.
- Use basic directory names, without spaces or special characters such as "~", "@", etc., which may cause problems.
- Cut and paste the path and/or name of the directory that contains the extracted scripts into the configuration download path of the Aastra unit (you may have to convert "\" into "/") to eliminate typographical errors.

Note that you can define the **C:/Root/Download** part as you want. The script names may also differ from the example shown above.

When the Transfer Protocol is set to **File**, you may prefix the path by one of the following to indicate storage media:

- ***Persistent***: for onboard persistent storage. The configuration script is saved into the persistent file system of the Aastra unit (in flash memory). This is the default value.
- ***Volatile***: for onboard non-persistent storage. The configuration script is saved into the non-persistent RAM memory of the Aastra unit. All information is lost the next time the unit restarts.

Table 294: Path Configurations Example (File)

Location	Corresponding Path Name
Onboard persistent storage of the Aastra unit under the directory "Script-1"	Persistent:Script-1 or Script-1

4. Set the transfer protocol to transfer the configuration scripts in the *Transfer Protocol* field.

You can select from five different transfer protocols:

- HTTP: HyperText Transfer Protocol.
- HTTPS: HyperText Transfer Protocol over Transport Layer Security.
- TFTP: Trivial File Transfer Protocol.
- FTP: File Transfer Protocol. Note that the Aastra unit FTP client does not support the EPSV command.

Note: The configuration script download via TFTP can only traverse NATs of types "Full Cone" or "Restricted Cone". If the NAT you are using is of type "Port Restricted Cone" or "Symmetric", the script transfer will not work.

- File: Complete path to a configuration image in a storage device. You can view and manage all files created with the File transfer protocol by using the File Manager. See "File Manager" on page 597 for more details.

HTTP and HTTPS support basic or digest authentication mode as described in RFC 2617. HTTPS requires a valid certificate.

If you have selected HTTP or HTTPS, please note that your server may activate some caching mechanism for the script download. This mechanism caches the initial script download for later processing, thus preventing changes or update of the original script. This can cause strange problems if you want to edit a configuration script to modify values and upload it immediately. The result will still return the original script and not the new one.

5. If your server requires authentication when downloading the configuration script, set the following:

- The user name in the *User Name* field.
- The password in the *Password* field.

Caution: The *User Name* and *Password* fields are not accessible if you have the User or Observer access right. See "Users" on page 591 for more details.

6. Set the static configuration scripts server IP address or domain name and port number in the *Host Name* field.

This is the current address of the PC that hosts the configuration scripts.

Use the special port value zero to indicate the protocol default. For instance, the TFTP default port is 69, the HTTP default port is 80, and the HTTPS default port is 443.

The default value is 0.0.0.0:0.

7. Set the key used to decrypt configuration scripts when they are encrypted in the *Privacy key* field.

Caution: The *Privacy Key* field is not accessible if you have the User or Observer access right. See "Users" on page 591 for more details.

You can secure the exchange of configuration scripts between the server and the Aastra unit. A privacy key allows the unit to decrypt a previously encrypted configuration script.

To encrypt a configuration script, you must use the MxCryptFile application. MxCryptFile is a command line tool that encrypts files before sending them to the Aastra unit. Contact your sales representative for more details.

The key is encoded in hexadecimal notation. You can thus use characters in the range 0-9, A-F, and a-f. All other characters are not supported.

Each character encodes 4 bits and the maximum key length is 112 characters, which gives a binary key of 56 bytes. It is the maximum supported by the MxCryptFile application.

For instance, a 32-bit key could look like the following: `A36CB299`.

This key must match the key used for the encryption of the relevant configuration script.

If the field is empty, the configuration script is not decrypted by the unit and the configuration update fails.

Encryption is auto-detected.

8. Define whether or not to allow the execution of a script even if it is identical to the last executed script in the *Allow Repeated Execution* drop-down menu.

Table 295: Allow Repeated Execution Parameters

Parameter	Description
Auto	Uses the configured value of ScriptsAllowRepeatedExecution.
Enable	Allows repeated execution of the same script.
Disable	Does not allow repeated execution of the same script.

The script retry mechanism is not enabled for the DHCP triggered scripts (see "DHCPv4 Auto-Provisioning" on page 412 for more details).

9. Do one of the following:

- Click **Submit** if you do not need to set other parameters.
- Click **Submit & Execute Now** to execute the script.

Executing a Script from your PC

This section describes how to execute a script located on the PC.

If you are currently using an unsecure HTTP access, script transfers through web browser are disabled. This is to avoid transferring the configuration in clear text. To enable the section, you can:

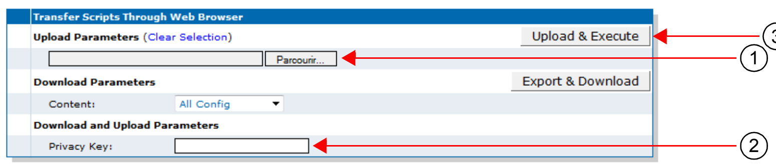
- Access the secure site (recommended) by clicking the corresponding link at the top of the window. This is the recommended way to proceed.
- Activate unsecure certificate transfer by clicking the corresponding link at the top of the window. This is not recommended.

To execute a script from the PC:

1. In the *Transfer Scripts Through Web Browser* section of the *Configuration Scripts* page, type the name of a script in the *Upload Parameters* field or select an existing one on the PC with the **Browse** button.

   When a script is executed, it is not installed in the unit's file system persistent memory. You can click the *Clear Selection* link to empty the field and enter another name.

Figure 191: Transfer Scripts Through Web Browser Section



2. If required, set the key used to decrypt configuration scripts when they are encrypted in the *Privacy key* field.

   You can secure the exchange of configuration scripts between the server and the Aastra unit. A privacy key allows the unit to decrypt a previously encrypted configuration script.

   To encrypt a configuration script, you must use the MxCryptFile application. MxCryptFile is a command line tool that encrypts files before sending them to the Aastra unit. Contact your sales representative for more details.

   The key is encoded in hexadecimal notation. You can thus use characters in the range 0-9, A-F, and a-f. All other characters are not supported.

   Each character encodes 4 bits and the maximum key length is 112 characters, which gives a binary key of 56 bytes. It is the maximum supported by the MxCryptFile application.

   For instance, a 32-bit key could look like the following: `A36CB299`.

   This key must match the key used for the encryption of the relevant configuration script.

   If the field is empty, the configuration script is not decrypted by the unit and the configuration update fails.

   Encryption is auto-detected.

3. Click the **Upload & Execute** button.

Configuration Download Procedure

The following steps explain how to download configuration scripts from the web interface.

Note: The configuration download via TFTP can only traverse NATs of types "Full Cone" or "Restricted Cone". If the NAT you are using is of type "Port Restricted Cone" or "Symmetric", the file transfer will not work.

▶ **To download configuration scripts:**

1. Place the configuration scripts to download on the computer hosting the configuration scripts server.

   These scripts must be in a directory under the server's root path.

2. Initiate the configuration scripts download by clicking the **Submit & Execute Now** button at the bottom of the page.

   The Aastra unit immediately downloads the configuration scripts.

Automatic Configuration Update

This section describes how to configure the Aastra unit to automatically update its configuration. This update can be done:

- Every time the Aastra unit restarts.
- At a specific time interval you can define.

Automatic Update on Restart

The Aastra unit may download new configuration scripts each time it restarts.

NAT Variations

NAT treatment of UDP varies among implementations. The four treatments are:

- Full Cone: All requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host by sending a packet to the mapped external address.
- Restricted Cone: All requests from the same internal IP address and port are mapped to the same external IP address and port. Unlike a full cone NAT, an external host (with IP address X) can send a packet to the internal host only if the internal host had previously sent a packet to IP address X.
- Port Restricted Cone: Similar to a restricted cone NAT, but the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P.
- Symmetric: All requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port. If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used. Furthermore, only the external host that receives a packet can send a UDP packet back to the internal host.

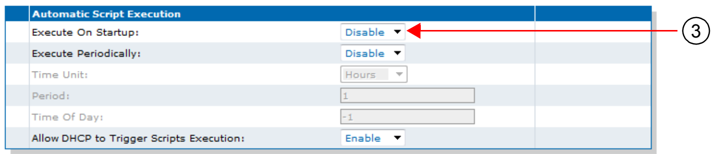
For more details on NAT treatments, refer to RFC 3489.

▶ **To set the automatic update every time the** Aastra unit **restarts:**

1. Set the configuration scripts parameters as defined in "Executing Configuration Scripts Settings" on page 405.
2. Place the configuration scripts to download on the computer hosting the configuration scripts server.

   These scripts must be in a directory under the root path.
3. In the *Automatic Script Execution* section of the *Configuration Scripts* page, select **Enable** in the *Execute on Startup* drop-down menu.

   Figure 192: Automatically Update Scripts Section

   The automatic configuration update will be performed each time the Aastra unit restarts.

   The unit configuration is only updated if at least one parameter value defined in the downloaded configuration scripts is different from the actual unit configuration.
4. Click **Submit** if you do not need to set other parameters.

Automatic Update at a Specific Time Interval

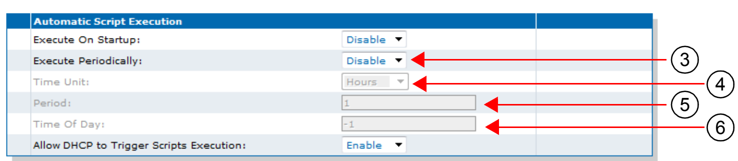
You can configure the Aastra unit to download new configuration scripts at a specific day and/or time.

▶ **To set the automatic update at a specific time interval:**

1. Set the configuration scripts parameters as defined in "Executing Configuration Scripts Settings" on page 405.
2. Place the configuration scripts to download on the computer hosting the configuration scripts server.

   These scripts must be in a directory under the root path.
3. In the *Automatic Script Execution* section of the *Configuration Scripts* page, select **Enable** in the *Execute Periodically* drop-down menu.

   Figure 193: Automatically Update Scripts Section

4. Select the time base for configuration updates in the *Time Unit* drop-down menu.

   Table 296: Time Unit Parameters

Parameter	Description
Minutes	Updates the unit's configuration every *x* minutes.
Hours	Updates the unit's configuration every *x* hours.
Days	Updates the unit's configuration every *x* days. You can define the time of day when to perform the update in the *Time of Day* field (see Step 6).

   You can specify the *x* value in the *Period* field (see Step 5).
5. Set the waiting period between each configuration update in the *Period* field.

Available values are from 1 to 60. The time unit for the period is specified in the *Time Unit* field (see Step 4).

6. If you have selected **Days** in Step 4, set the time of the day when to initiate a configuration update in the *Time of Day* field.

The time of the day is based on the *Static Time Zone* field of the *Network - Host* page (see "Time Configuration" on page 94 for more details).

You must have a time server SNTP that is accessible and properly configured or the automatic configuration update feature may not work properly. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server's documentation.

> **Note:** The Aastra unit hardware does not include a real time clock. The unit uses the SNTP client to get and set its clock. As certain services need correct time to work properly (such as HTTPS), you should configure your SNTP client with an available SNTP server in order to update and synchronise the local clock at boot time.

The configuration scripts are downloaded at the first occurrence of this value and thereafter at the period defined by the *Period* field. Let's say for instance the automatic unit configuration update is set with the time of day at 14h00 and the update period at every 2 days.

- If the automatic update is enabled before 14h00, the first update will take place the same day at 14h00, the second update two days later at the same hour, and so on.
- If the automatic update is enabled after 14h00, the first update will take place the day after at 14h00, the second download two days later at the same hour, and so on.

Available values are -1, and from 0 to 23.

When setting the variable to **-1**, the time of the day at which the Aastra unit first downloads the configuration scripts is randomly selected.

7. Click **Submit** if you do not need to set other parameters.

DHCPv4 Auto-Provisioning

> **Note:** This feature does not support IPv6. See "IPv4 vs. IPv6 Availability" on page 85 for more details.

You can configure the Aastra unit to automatically download new configuration scripts upon receiving options 66 (tftp-server) or 67 (bootfile) in a DHCPv4 answer. A DHCP answer includes both Bound and Renew.

The contents of the option 66 or 67 defines which script to download. The unit's configuration is not used to download the script. This allows the unit, for instance, to download a script from a server after a factory reset and to reconfigure itself without a specific profile.

The syntax of options 66 and 67 is as follows:

```
[FileType] = [protocol]://[username] :[password]@[fqdn server]/[path]
```

For instance:

```
Script=https://admin :adminpw@script-server.aastra.com/Mx3000config/%mac%.cfg
```

The Aastra unit supports only the Script file type for now.

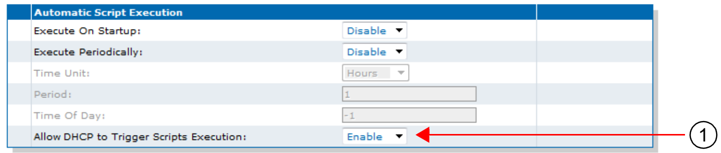
The following is an example of a valid option 67 (Bootfile):

```
Option: (t=67, l=53) Bootfile name = "Script=http://192.168.50.1/digest/
%mac%__2.0.6.84.cfg"
Option: (67) Bootfile name
Length: 53
Value: 5363726970743D687474703A2F2F3139322E31136382E3530...
```

▶ To set DHCPv4 auto-provisioning:

1. In the *Automatic Script Execution* section of the *Configuration Scripts* page, set the *Allow DHCP to Trigger Scripts Execution* drop-down menu with the proper behaviour.

Figure 194: Automatically Update Scripts Section



When enabled, the DHCPv4 options *tftp-server* (option 66) and *bootfile* (option 67) are used to download a configuration script. If this configuration script is identical to the last executed script, it will not be run again. The script retry mechanism is not enabled for the DHCPv4 triggered scripts (see "Executing Configuration Scripts Settings" on page 405 for more details).

If the two options are received, both scripts are executed independently. The script defined by the *tftp-server* (option 66) option is executed first.

If you are using HTTPS to transfer scripts, you must have a time server SNTP that is accessible and properly configured. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server's documentation.

Note: The Aastra unit hardware does not include a real time clock. The unit uses the SNTP client to get and set its clock. As certain services need correct time to work properly (such as HTTPS), you should configure your SNTP client with an available SNTP server in order to update and synchronise the local clock at boot time.

When a DHCPv4 download script is configured in HTTPS, the script execution is deferred and a 30 seconds timer is started to let enough time for the NTP synchronization.

This timer is independent for each HTTPS script launched. If, for instance, a DHCPv4 answer has both option 66 and 67 configured in HTTPS and if the Update on Restart feature is used, up to 1 min 30 seconds can pass before any other operation such as backup, restore, script execution can be processed.

Once the NTP synchronization is established, the deferred scripts are started immediately one after the other, ending the timer.

When synchronization is already established, there is no timer, even in HTTPS.

2. Click **Submit** if you do not need to set other parameters.

Number of Retries

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

When using the automatic configuration update (on restart or at a specific interval), the Aastra unit may encounter a problem upon restarting the unit (such as a DHCP server problem) that prevents the update to succeed. You can define a maximum number of attempts to retry a script transfer until it succeeds when it fails upon an automatic transfer on restart or automatic periodic transfer. The retries are only attempted if the server is unreachable. Unreachable port or file not found errors don't trigger the retry mechanism.The time interval between each retry is 30 seconds.

▶ To set the number of retries:

1. In the *confMIB*, set the number of retries in the `scriptsTransferRetriesNumber` variable.

   You can also use the following line in the CLI or a configuration script:

   `conf.scriptsTransferRetriesNumber="Value"` where *Value* may be as follows

- -1 means a retry to infinity.
- 0 means no retry.

The maximum number of retries is 100.

Creating a Configuration Script

Configuration scripts are text files that contain command lines interpreted by the Aastra unit. Most commands contained in a script assign values to configuration variables. Script commands can also execute configuration commands. This configuration script can then be downloaded into the Aastra unit as described in the current chapter.

Writing configuration scripts requires a bit of knowledge about the Aastra unit's configuration variables tree structure. Each parameter that is accessed via the unit's web interface maps to a variable in the configuration tree. For detailed information on these mappings, please refer to "Appendix D - Web Interface – SNMP Variables Mapping" on page 641.

Configuration scripts use the Aastra proprietary scripting language, as described in "Appendix B - Scripting Language" on page 627.

Refer to "Appendix B - Scripting Language" on page 627 for samples of configurations you can use in a configuration script. The samples include the configuration required to perform a basic call between an ISDN telephone and an analog telephone. These samples may also be used in the Aastra unit Command Line Interface.

CHAPTER

41 Configuration Backup/Restore

This chapter describes the configuration backup/restore feature, which allows you to backup (upload) all the SNMP (MIB) and Web configuration of the Aastra unit into a configuration image file located on a remote server or to the local file system.

This chapter describes the following:

- Configuration backup download server setup.
- Backup/restore configuration parameters.

Standards Supported	• RFC 959: File Transfer Protocol (client-side only) • RFC 1350: The TFTP Protocol (Revision 2) (client-side only) • RFC 2616: Hypertext Transfer Protocol - HTTP/1.1 (client-side only) • RFC 2617: HTTP Authentication: Basic and Digest Access Authentication • RFC 3617: Uniform Resource Identifier (URI) Scheme for the Trivial File Transfer Protocol • draft-ietf-http-authentication-03

Configuration Backup Download Server

To backup/restore a configuration image, you may need to setup the following applications on your computer:

- TFTP server with proper root path
- SNTP server properly configured
- HTTP server with proper root path
- HTTPS server with proper root path

Configuring the TFTP Server

When you perform a configuration backup/restore by using the TFTP (Trivial File Transfer Protocol) protocol, you must install a TFTP server running on the PC designated as the TFTP server host. It is assumed that you know how to set the TFTP root path. If not, refer to your TFTP server's documentation.

Configuring the SNTP Server

When you use the HTTPS protocol, you need to have a time server SNTP that is accessible and properly configured. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server's documentation. You can also refer to "SNTP Configuration" on page 93 for more details on how to configure the Aastra unit for a SNTP server.

Note: The Aastra unit hardware does not include a real time clock. The unit uses the SNTP client to get and set its clock. As certain services need correct time to work properly (such as HTTPS), you should configure your SNTP client with an available SNTP server in order to update and synchronise the local clock at boot time.

Configuring the HTTP Server

When you to perform a configuration backup/restore by using the HTTP protocol, you must install a HTTP server running on the PC designated as the server host. It is assumed that you know how to set the root path. If not, refer to your HTTP server's documentation.

Configuring the HTTPS Server

Standards Supported	• RFC 2246: The TLS Protocol Version 1.0 • RFC 2459: X.509 Digital Certificates • RFC 2818: HTTP Over TLS (client side only) • RFC 3268: Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS) • RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

When you perform a configuration backup/restore that requires authentication or privacy by using the HTTP over the Transport Layer Security (TLS) protocol (HTTPS), you must install a HTTPS server running on the PC designated as the server host. It is assumed that you know how to set the root path and SSL/TLS security configuration. If not, refer to your HTTPS server's documentation.

When two peers establish a HTTPS connection, they negotiate and decide on a cipher suite to use for data encryption. The client suggests a list of cipher suites and the server selects one that it supports. Some cipher suites are more secured than others. The Aastra unit acts as a client.

The Aastra unit suggests a wide range of cypher suites, which includes cipher suites that are not very secure. The final choice rests with the server and it is thus possible that the transfer uses a SSL/TLS link that is not very secure.

Aastra recommends to use cipher suites based on the RSA key exchange mechanism, because the Diffie-Hellman key exchange mechanism introduces a noticeable delay in the HTTPS session establishment. Furthermore, Aastra recommends using cipher suites based on the following SSL/TLS algorithms:

Table 297: Suggested Secure Parameters

Suggested Parameter	Description
Key Exchange Mechanism	• RSA • Diffie-Hellman
Ciphers	• AES (128 and 256 bits) • 3DES (168 bits)
Message Digests	• SHA-1

The following six recommended cipher suites are based on the algorithms of Table 297:

Table 298: Recommended Cipher Suites

ID	Name
0x0035	TLS_RSA_WITH_AES_256_CBC_SHA
0x0039	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
0x000a	TLS_RSA_WITH_3DES_EDE_CBC_SHA
0x0016	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
0x002f	TLS_RSA_WITH_AES_128_CBC_SHA
0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Certificates

The Aastra unit contains embedded security certificates formatted as per ITU x.509 and RFC 3280. The certificates are factory-installed. You can also add new certificates as described in "Chapter 46 - Certificates Management" on page 557.

When contacting a HTTPS server, the Aastra unit establishes a TLS connection by (among others):

- negotiating cipher suites
- checking the server certificates validity (dates)

The Aastra unit then checks the server's identity by validating the host name used to contact it against the information found in the server's certificate, as described in RFC 2818, section 3.1.

If any of the above does not succeed, the Aastra unit refuses the secure connection. To help detect such errors, you can increase the syslog messages level.

Backup/Restore Configuration

This section describes how to set the backup/restore configuration parameters and some related files (e.g. certificates). You can restore this configuration in case the Aastra unit loses it for any reason or to clone a unit with the configuration of another unit. The configuration backup images are in XML format and may be encrypted or in clear text.

Note: The files under the File service are not included in the backup process. In the same way, the restore process will not remove any file under the File service.

Please note that you can use a backup file from an older firmware version and use it in a unit with a more recent firmware version. However, a backup file from a newer firmware version than the one actually in the unit cannot be used for a restore operation on the unit. For instance, let's say you perform the following backups:

- In firmware v1.1r4.1, you make the backup "Backup_X1".
- In firmware v1.1r4.2 you make the backup "Backup_X2"

Application v1.1r4.2 is more recent than v1.1r4.1. The following table describes the various scenarios possible.

Table 299: Backup Matrix

Scenario	Supported	Not Supported
Apply the backup "Backup_X1" in a unit with firmware v1.1r4.1.	✓	
Apply the backup "Backup_X1" in a unit with firmware v1.1r4.2.	✓	
Apply the backup "Backup_X2" in a unit with firmware v1.1r4.2.	✓	
Apply the backup "Backup_X2" in a unit with firmware v1.1r4.1.		✓

You can backup or restore the configuration to/from two sources:

- To/from an image located on an image server
- To/from an image located on your PC (transfer images through the web browser)

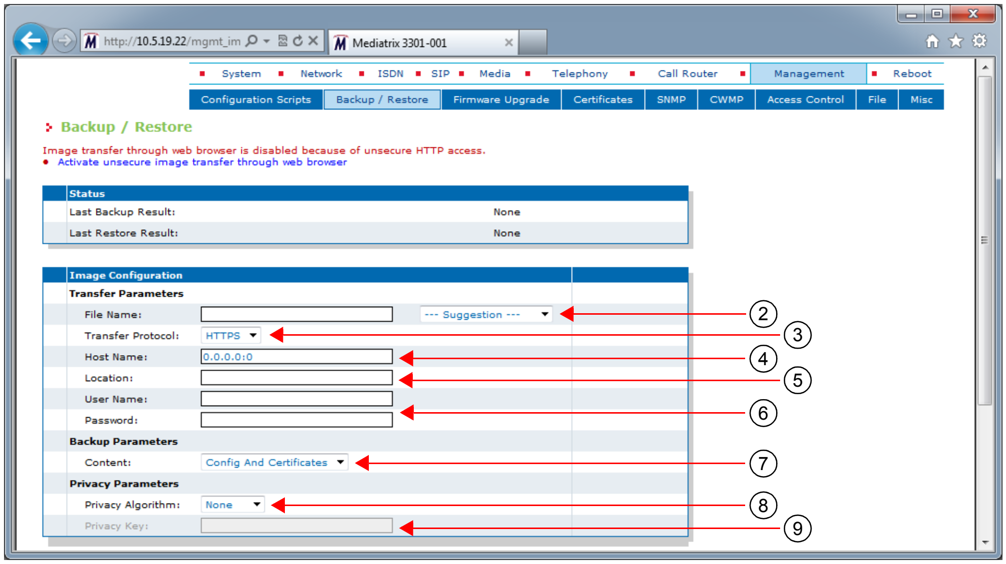
This section explains both methods.

Performing a Backup/Restore to/from on an Image Server or File System

▶ **To set the configuration backup/restore parameters:**

1. In the web interface, click the *Management* link, then the *Backup / Restore* sub-link.

Figure 195: Management – Backup / Restore Web Page



2. Set the name of the configuration image in which you want to backup or from which you want to restore the Aastra unit configuration in the *File Name* field.

The file name is case sensitive hence it must be entered properly. Make sure to write the file extension.

If you select **File** in the Transfer Protocol drop-down menu (Step 5), this means that you can select an image located in the unit's persistent file system. You can use the *Suggestion* drop-down menu to select one of the available images in the file system.

To see the content of the unit's file system persistent memory, go to the File Manager ("Chapter 50 - File Manager" on page 597). All installed configuration scripts/images are listed.

This field may contain a macro that is substituted by the actual value when backing up or restoring the unit's configuration. The Aastra unit supports the *%mac%* macro, which will be substituted by the MAC address of the unit. For instance, the "%mac%.bkp" value for a Aastra unit with MAC address "0090F12345AB" will be "0090F12345AB.bkp".

This field may contain macros that are substituted by the actual value when backing up or restoring the unit's configuration. The supported macros are:

- %mac% - the MAC address of the unit.
- %version% - the MFP version of the unit.
- %product% - the Product name of the unit.
- %productseries% - the Product series name of the unit.

For instance, the "%mac%.bkp" value for a Aastra unit with MAC address "0090F12345AB" will be "0090F12345AB.bkp".

3. Select a transfer protocol to transfer a configuration image in the *Transfer Protocol* drop-down menu.

You can select from five different transfer protocols:

- HTTP: HyperText Transfer Protocol.
- HTTPS: HyperText Transfer Protocol over Transport Layer Security.
- TFTP: Trivial File Transfer Protocol.
- FTP: File Transfer Protocol. Note that the Aastra unit FTP client does not support the EPSV command.
- File: Complete path to a configuration image in the Aastra unit's onboard storage space. You can view and manage all files created with the File transfer protocol by using the File Manager. See "File Manager" on page 597 for more details.

Note: The configuration image backup via TFTP can only traverse NATs of types "Full Cone" or "Restricted Cone". If the NAT you are using is of type "Port Restricted Cone" or "Symmetric", the transfer will not work.

HTTP and HTTPS support basic or digest authentication mode as described in RFC 2617. HTTPS requires a valid certificate.

The backup operation currently supports the following protocols:

- TFTP
- FTP
- File

The restore operation supports all the transfer protocols.

If you have selected HTTP or HTTPS, please note that your server may activate some caching mechanism for the configuration image transfer. This mechanism caches the initial configuration image transfer for later processing, thus preventing changes or update of the original image. This can cause strange problems if you want to edit a configuration image to modify values and upload it immediately. The result will still return the original image and not the new one.

4. Set the configuration backup/restore server hostname or FQDN and IP port in the *Host Name* field.

This is the current address and port number of the PC that hosts the configuration image file. Use the special port value 0 to indicate the protocol default. For instance, the TFTP default port is 69 and the HTTP default port is 80.

The default value is **0.0.0.0:0**.

NAT Variations

NAT treatment of UDP varies among implementations. The four treatments are:

- Full Cone: All requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host by sending a packet to the mapped external address.
- Restricted Cone: All requests from the same internal IP address and port are mapped to the same external IP address and port. Unlike a full cone NAT, an external host (with IP address X) can send a packet to the internal host only if the internal host had previously sent a packet to IP address X.
- Port Restricted Cone: Similar to a restricted cone NAT, but the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P.
- Symmetric: All requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port. If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used. Furthermore, only the external host that receives a packet can send a UDP packet back to the internal host.

For more details on NAT treatments, refer to RFC 3489.

5. Set the path of the directory where the configuration image is located in the *Location* field.

The path is case sensitive hence it must be entered properly. It is relative to the root of the configuration transfer server. Use the “/” character when defining the path to indicate sub-directories.

This field may contain some macros that are substituted by the actual value when downloading the configuration script. The supported macros are:

- %mac% - the MAC address of the unit
- %version% - the MFP version of the unit
- %product% - the Product name of the unit.
- %productseries% - the Product series name of the unit.

For instance, the “%mac%.xml” value for a Aastra unit with MAC address “0090f12345ab” will be “0090f12345ab.xml”.

The path differs depending on the transfer protocol selected (see Step 4).

Example: All Transfer Protocols Except File

Let’s consider the following example for all protocols except File:

- The directory that contains the configuration image is called: **Config_Image**.
- This directory is under **C:/Root/Download**.

Table 300: Path Configurations Example

Root Path	Corresponding Path Name
c:/root/download	Config_Image
c:/	root/download/Config_Image
c:/root	download/Config_Image

The following are some tips to help your process:

- Use the “/” character when defining the path to indicate sub-directories. For instance, *root/download*.
- If you are using the TFTP protocol to download the software, note that some TFTP servers on Windows do not recognize the “/” character and produce an error. In this case, use the “\” character.
- Use basic directory names, without spaces or special characters such as “~”, “@”, etc., which may cause problems.
- Cut and paste the path and/or name of the directory that contains the file into the configuration download path of the Aastra unit (you may have to convert “\” into “/”) to eliminate typographical errors.

Note that you can define the **C:/Root/Download** part as you want. The file name may also differ from the example shown above.

Example: Transfer Protocol is File

When the Transfer Protocol is set to **File**, you may prefix the path by one of the following to indicate storage media:

- ***Persistent***: for onboard persistent storage. The configuration image is saved into the persistent file system of the Aastra unit (in flash memory). This is the default value.

- ***Volatile***: for onboard non-persistent storage. The configuration image is saved into the non-persistent RAM memory of the Aastra unit. All information is lost the next time the unit restarts.

Table 301: Path Configurations Example (File)

Location	Corresponding Path Name
Onboard persistent storage of the Aastra unit under the directory "Backup-1"	Persistent:Backup-1 or Backup-1

6. If your server requires authentication, set the following:

- The user name in the *User Name* field.
- The password in the *Password* field.

Caution: The *User Name* and *Password* fields are not accessible if you have the User or Observer access right. See "Users" on page 591 for more details.

7. Define the *Backup Content* drop-down menu with the information to include in the backup.

Table 302: Backup Content Parameters

Parameter	Description
Config	Only the unit's configuration is included in the backup image.
Config And Certificates	The unit's configuration and certificates are included in the backup image. Aastra strongly recommends to activate encryption when including certificates in the backup image because host certificates include the private key (see Steps 9-10).

8. Set the privacy algorithm in the *Privacy Algorithm* field.

This defines the encryption method to use for backup operations. This parameter is not used for restore operations.

You can secure the exchange of configuration image between the server and the Aastra unit. A privacy key allows the unit to decrypt a previously encrypted configuration image. During a restore of the backup image, the encryption is auto-detected.

The configuration image must have been encrypted before use.

Table 303: Privacy Algorithm

Parameter	Description
None	Backup images are not encrypted.
DefaultAlgo	Backup images are encrypted with the default algorithm.

9. Set the decryption key in the *Privacy key* field.

Caution: The *Privacy key* field is not accessible if you have the User or Observer access right. See "Users" on page 591 for more details.

This is the key used for:

- backup operations to encrypt backup images
- restore operations to decrypt backup images when encrypted (encryption is auto-detected).

The key is encoded in hexadecimal notation. You can thus use characters in the range 0-9, A-F. All other characters are not supported.

Each character encodes 4 bits of the key. For instance, a 32-bit key requires 8 characters.

- If you enter too many bits, the key is truncated to the first 448 bits.
- If you do not enter enough bits, the key is padded with zeros.

For instance, a 32-bit key could look like the following: `A36CB299`.

This key must match the key used for the encryption of the configuration image. If the variable is empty, the configuration image is not decrypted.

10. Do one of the following:

- To save your settings without performing a backup/restore, click **Submit**.
- To save your settings and perform a backup now, click **Submit & Backup Now**.
- To save your settings and perform a restore now, click **Submit & Restore Now**.

Transferring Images Through the Web Browser

This section describes how to perform a backup to or restore from an image located on the PC.

To see the content of the unit's file system persistent memory, go to the File Manager ("Chapter 50 - File Manager" on page 597). All installed configuration scripts/images are listed.

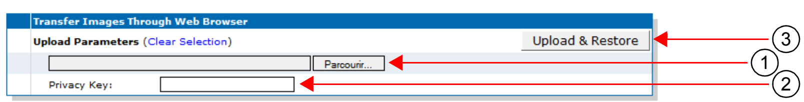
► **To perform a backup to or restore from an image on the PC:**

1. In the *Transfer Images Through Web Browser* section of the Backup / Restore page, type the name of an image in the *Upload Parameters* field or select an existing one on the PC with the **Browse** button.

If you are currently using an unsecure HTTP access, the *Transfer Images Through Web Browser* section is disabled. This is to avoid transferring an image in clear text. To enable the section, access the secure site by clicking the *Activate unsecure image transfer through web browser* link at the top of the window.

When an image is run, it is not installed in the unit's file system persistent memory. You can click the *Clear Selection* link to empty the field and enter another name.

Figure 196: Transfer Images Through Web Browser Section



2. Set the decryption key in the *Privacy key* field.

This is the key used for:

- backup operations to encrypt backup images
- restore operations to decrypt backup images when encrypted (encryption is auto-detected).

The key is encoded in hexadecimal notation. You can thus use characters in the range 0-9, A-F. All other characters are not supported.

Each character encodes 4 bits of the key. For instance, a 32-bit key requires 8 characters.

- If you enter too many bits, the key is truncated to the first 448 bits.
- If you do not enter enough bits, the key is padded with zeros.

For instance, a 32-bit key could look like the following: `A36CB299`.

This key must match the key used for the encryption of the configuration image. If the variable is empty, the configuration image is not decrypted.

3. Click the **Upload Now** button.

CHAPTER

42

Firmware Download

This chapter describes how to install, uninstall and update software components on the Aastra unit by using the web interface, according to a supplied Firmware Pack selection.

> **Note:** If you have backed up the configuration of your unit, Aastra recommends that you perform a new backup every time you upgrade the firmware pack of the unit to avoid restore issues.

This chapter describes the following:

- What is a firmware pack?
- Firmware pack server setup.
- Firmware pack version and name to download.
- Transfer parameters.
- Firmware pack update procedure.

Standards Supported	• RFC 959: File Transfer Protocol (client-side only) • RFC 1350: The TFTP Protocol (Revision 2) (client-side only) • RFC 2616: Hypertext Transfer Protocol - HTTP/1.1 (client-side only) • RFC 2617: HTTP Authentication: Basic and Digest Access Authentication • RFC 3617: Uniform Resource Identifier (URI) Scheme for the Trivial File Transfer Protocol • draft-ietf-http-authentication-03

What is a Firmware Pack?

A firmware pack file is a regular zip file that contains the modules and features to install on the Aastra unit.

When unzipping a firmware pack, the contents is extracted according to a pre-defined tree architecture. This creates a directory that contains the files required for the Aastra unit to properly update its firmware. The firmware pack contains all the modules to install. When performing the upgrade operation, the Aastra unit checks the modules versions of the firmware pack against its own modules versions and installs only the modules that have changed.

> **Note:** The currently installed firmware pack is only required when downgrading.

Before Performing a Firmware Upgrade or Downgrade

To download a firmware pack, you may need to setup the following applications on your computer:

- TFTP server with proper root path
- SNTP server properly configured
- MIB browser (with the current Aastra unit MIB tree)
- Firmware pack zip file
- HTTP server with proper root path

- HTTPS server with proper root path
- Syslog daemon (optional)

Configuring the TFTP Server

When you perform a firmware pack update by using the TFTP Trivial File Transfer Protocol) protocol, you must install a TFTP (server running on the PC designated as the update files server. This PC must not have a firewall running. Aastra also recommends to place the PC and the Aastra unit in the same subnet.

It is assumed that you know how to set the TFTP root path. If not, refer to your TFTP server's documentation.

Configuring the SNTP Server

When you use the HTTPS protocol, you need to have a time server SNTP that is accessible and properly configured. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server's documentation. You can also refer to "SNTP Configuration" on page 93 for more details on how to configure the Aastra unit for a SNTP server.

Note: The Aastra unit hardware does not include a real time clock. The unit uses the SNTP client to get and set its clock. As certain services need correct time to work properly (such as HTTPS), you should configure your SNTP client with an available SNTP server in order to update and synchronise the local clock at boot time.

Configuring the HTTP Server

When you perform a firmware pack update by using the HTTP protocol, you must install a HTTP server running on the PC designated as the update files server. This PC must not have a firewall running. Aastra also recommends to place the PC and the Aastra unit in the same subnet.

It is assumed that you know how to set the root path. If not, refer to your HTTP server's documentation.

Configuring the HTTPS Server

Standards Supported	• RFC 2246: The TLS Protocol Version 1.0 • RFC 2459: X.509 Digital Certificates • RFC 2818: HTTP Over TLS (client side only) • RFC 3268: Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS) • RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

When you perform a firmware pack update that requires authentication or privacy by using the HTTP over the Transport Layer Security (TLS) protocol (HTTPS), you must install a HTTPS server running on the PC designated as the update files server. It is assumed that you know how to set the root path and set the SSL/ TLS security configuration. If not, refer to your HTTPS server's documentation.

When two peers establish a HTTPS connection, they negotiate and decide on a cipher suite to use for data encryption. The client suggests a list of cipher suites and the server selects one that it supports. Some cipher suites are more secured than others. The Aastra unit acts as a client.

The Aastra unit suggests a wide range of cypher suites, which includes cipher suites that are not very secure. The final choice rests with the server and it is thus possible that the transfer uses a SSL/TLS link that is not very secure.

Aastra recommends to use cipher suites based on the RSA key exchange mechanism, because the Diffie-Hellman key exchange mechanism introduces a noticeable delay in the HTTPS session establishment. Furthermore, Aastra recommends using cipher suites based on the following SSL/TLS algorithms:

Table 304: Suggested Secure Parameters

Suggested Parameter	Description
Key Exchange Mechanism	• RSA • Diffie-Hellman
Ciphers	• AES (128 and 256 bits) • 3DES (168 bits)
Message Digests	• SHA-1

The following six recommended cipher suites are based on the algorithms of Table 304:

Table 305: Recommended Cipher Suites

ID	Name
0x0035	TLS_RSA_WITH_AES_256_CBC_SHA
0x0039	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
0x000a	TLS_RSA_WITH_3DES_EDE_CBC_SHA
0x0016	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
0x002f	TLS_RSA_WITH_AES_128_CBC_SHA
0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Certificates

The Aastra unit contains embedded security certificates formatted as per ITU x.509 and RFC 3280. The certificates are factory-installed. You can also add new certificates as described in "Chapter 46 - Certificates Management" on page 557.

When contacting a HTTPS server, the Aastra unit establishes a TLS connection by (among others):

- negotiating cipher suites
- checking the server certificates validity (dates)

Caution: You must have a time server SNTP that is accessible and properly configured. It is assumed that you know how to configure your SNTP server. If not, refer to your SNTP server's documentation. You can also refer to "SNTP Configuration" on page 93 for more details on how to configure the Aastra unit SNTP client.

The Aastra unit then checks the server's identity by validating the host name used to contact it against the information found in the server's certificate, as described in RFC 2818, section 3.1.

If any of the above does not succeed, the Aastra unit refuses the secure connection. To help detect such errors, you can increase the syslog messages level.

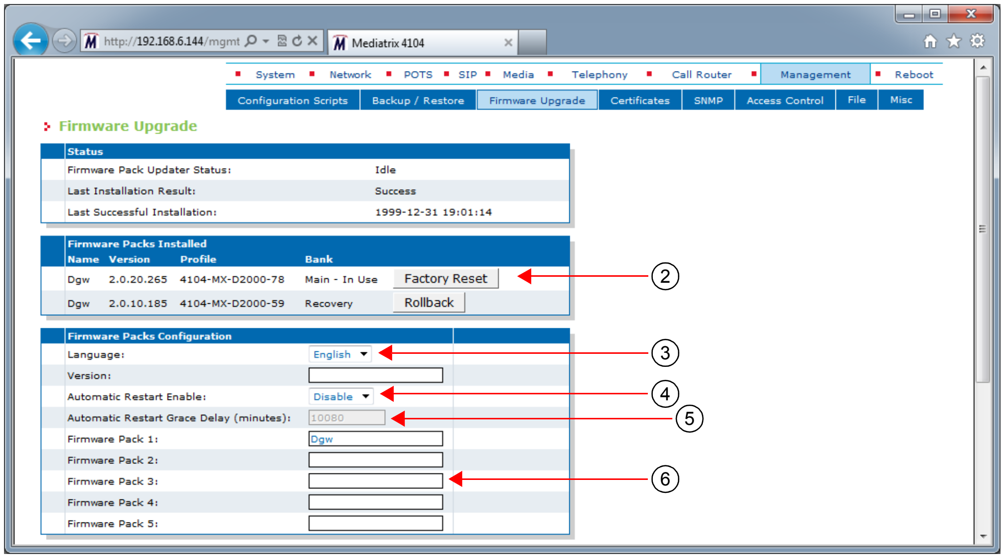
Firmware Packs Configuration

This section allows you to define the firmware pack version and name(s) to properly download them.

▶ To set the firmware pack parameters:

1. In the web interface, click the *Management* link, then the *Firmware Download* sub-link.

Figure 197: Management – Firmware Download Web Page



2. In the *Firmware Packs Installed* section of the *Firmware Upgrade* page, click one of the available buttons if required:

Table 306: Available Buttons

Button	Description
Factory Reset	You can apply a factory reset to the current unit by clicking the **Factory Reset** button. See “Factory Reset” on page 16 for more details.
Rollback	You can revert back to the previously installed MFP found in the recovery bank at any time by clicking the **Rollback** button. If the recovery bank contains a MFP that can be used, it is displayed in the *Bank* column of the *Firmware Packs Installed* section. When a rollback is performed, the configuration of the MFP in the recovery bank applies. The current configuration is lost. The **Rollback** button is displayed only if the current bank's application and the recovery bank's application both support the rollback mechanism and have been both installed from an application supporting the rollback. Otherwise, the **Rollback** button is not displayed. **Note:** This feature does not apply to the Aastra TA7102i model.

3. In the *Firmware Packs Configuration* section of the *Firmware Upgrade* page, enter the version of the firmware pack to install in the *Version* field.

Currently, you cannot install two firmware packs with different versions.

4. Set the *Automatic Restart Enable* drop-down menu with whether or not to automatically restart the system when needed for completing a firmware update operation.

You can also set a grace delay in the next step.

5. If automatic restart is enabled, set the *Automatic Restart Grace Delay* field with the grace delay, in minutes, that the unit waits for all telephony calls to be terminated before the automatic restart can occur.

The maximum value is set to 10080 minutes (7 days).

During that delay, it is impossible to make new calls but calls in progress are not terminated. When all calls are completed, then the unit restarts.

You can also set a services restart grace period as described in "Graceful Restart of Services" on page 56.

6. Enter the name of up to five firmware packs to install in the *Firmware Pack* fields.

   You can install several firmware packs at the same time. In that case, enter the firmware pack names in different rows of the table.

   When extracting the content of the ZIP file, available firmware packs are listed as directories under the *xxx/FirmwarePacks* directory.

> **Note:** The *Language* drop-down menu currently supports only English.

7. Proceed to "Transfer Configuration" on page 427.

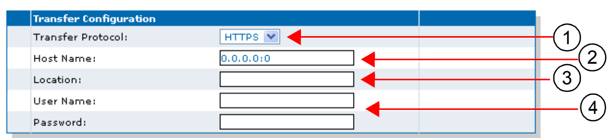
Transfer Configuration

The following describes how to configure the transfer parameters required to perform a firmware update.

► **To setup the firmware download path:**

1. In the *Transfer Configuration* section of the *Firmware Upgrade* page, select a transfer protocol to transfer a firmware pack in the *Transfer Protocol* drop-down menu.

Figure 198: Transfer Configuration Section



You have the following choices:

- HTTP: HyperText Transfer Protocol.
- HTTPS: HyperText Transfer Protocol over Transport Layer Security.
- TFTP: Trivial File Transfer Protocol.
- FTP: File Transfer Protocol. Note that the Aastra unit FTP client does not support the EPSV command.

HTTP and HTTPS support basic or digest authentication mode as described in RFC 2617. HTTPS requires a valid certificate.

If you have selected HTTP or HTTPS, please note that your server may activate some caching mechanism for the firmware pack download.

2. Set the static update files server IP address or domain name and port number to use when downloading a firmware pack in the *Host Name* field.

   This is the current address and port number of the PC that hosts the firmware packs. Use the special port value 0 to indicate the protocol default. For instance, the TFTP default port is 69, the HTTP default port is 80, and the HTTPS default port is 443.

   The default value is **0.0.0.0:0**.

   This parameter is not required if you have selected the **File** transfer protocol.

3. Set the firmware download path in the *Location* field.

   This is the location of the folder that contains the modules to download into the Aastra unit. In other words, this is where the zip file containing the firmware pack has been extracted. This path is relative to the root of the external media and excludes.

   Let's consider the following example:

   - The directory that contains the files required for download is called:

- This directory is under **C:/Root/Download**.

Table 307: Path Configurations Example

Root Path	Corresponding Path Name
c:/root/download	N/A
c:/	root/download
c:/root	download

The following are some tips to help your download process:

- Use the “/” character when defining the path to indicate sub-directories. For instance, *root/download*.
- If you are using the TFTP protocol, note that some TFTP servers on Windows do not recognize the “/” character and produce an error. In this case, use the “\” character.
- Use basic directory names, without spaces or special characters such as “~”, “@”, etc., which may cause problems.
- Cut and paste the path and/or name of the directory that contains the extracted files into the firmware download path of the Aastra unit (you may have to convert “\” into “/”) to eliminate typographical errors.

Note that you can define the **C:/Root/Download** part as you want. The file names may also differ from the example shown above.

4. If your server requires authentication when downloading a firmware pack, set the following:

- The user name in the *User Name* field.
- The password in the *Password* field.

Caution: The *User Name* and *Password* fields are not accessible if you have the User or Observer access right. See “Users” on page 591 for more details.

5. Proceed to “Firmware Pack Update Procedure” on page 429.

Certificate Validation

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

When downloading a MFP from an HTTPS server, you can define the level of security to use when validating the server's certificate.

Table 308: Certificate Validation Parameters

Parameter	Description
NoValidation	Allow a connection to the server without validating its certificate. The only condition is to receive a certificate from the server. This option provides partial security and should be selected with care.
HostName	Allow a connection to the server by validating its certificate is trusted and valid. The validations performed on the certificate include the expiration date and that the Subject Alternate Name (SAN) or Common Name (CN) matches the FQDN or IP address of the server.

▶ **To set the certificate validation parameter:**

1. In the *fpuMIB*, set the certificate validation behaviour in the `MfpTransferCertificateValidation` variable.

You can also use the following line in the CLI or a configuration script:

```
fpu.MfpTransferCertificateValidation="Value"
```

where *Value* may be as follows:

Table 309: Certificate Validation Values

Value	Meaning
100	NoValidation
200	HostName

Firmware Pack Update Procedure

The following describes how to update the firmware pack of the Aastra unit.

Extracting the Firmware Pack Zip File

The firmware pack zip file contains the firmware information required for the update. Extract the contents of the zip file on the PC designated as the update files server without modifying the defined folder name. This creates a directory that contains the files required for the Aastra unit to properly update its firmware.

You must extract the zip file under the root path as defined in the update files server or the firmware pack update will not proceed.

Launching a Firmware Pack Update

The following describes how to launch a firmware pack update.

▶ **To launch the firmware pack update:**

1. If not already done, set the firmware packs parameters as defined in "Firmware Packs Configuration" on page 425.

2. If not already done, unzip the firmware pack file as described in "Extracting the Firmware Pack Zip File" on page 429.

3. If not already done, set the transfer configuration parameters as described in "Transfer Configuration" on page 427.

4. Do one of the following:

- To save your settings without performing a firmware update, click *Submit*.
- To save your settings and perform a firmware update now, click *Submit & Install Now*.

  The firmware pack update may take several minutes, depending on your Internet connection, network conditions and servers conditions.

Caution: Aastra recommends to close and re-open your Web browser after a reboot that installs a firmware update. This is because your browser may activate a caching mechanism for some files. This mechanism caches some of the files to improve performance. This may cause problems when the cached files change in the Aastra unit after a firmware update and the web pages are no longer compatible with the cached files.

Firmware Pack Downgrade

It is possible to downgrade a Aastra unit from the current version to an older version. The procedure is the same as with a firmware upgrade.

Firmware Pack Update Status

When the Aastra unit initiates a firmware pack update, the LEDs indicate the status of the process.

Table 310: LED States in Firmware Pack Update

Event	LED State
Firmware pack downloading and writing	All LEDs are cycling from left to right, individually blinking 1 Hz, 33% duty. **Warning**: Do not turn the Aastra unit off while in this state.
Firmware pack download failed	All LEDs are blinking at 3 Hz, 50% duty. One LED out of two has a 180 degree phase. This pattern lasts for 8 seconds.

You can also view the firmware pack update status in the Status section of the *Firmware Upgrade* page.

Note: When the firmware pack update fails, the Aastra unit tries to download the firmware three times. In some cases, the unit may also restart.

Spanning Tree Protocol (STP)

Many network switches use the Spanning Tree Protocol (STP) to manage Ethernet ports activity. When a firmware pack update occurs, the Ethernet connector of the Aastra unit may switch off. This shutdown may trigger these network switches to shutdown the matching Ethernet port for at least one minute. This shutdown on the switch side can prevent firmware pack update.

To prevent this, the Aastra unit supports the STP. However, this management has a potential time cost. It may appear from time to time that firmware pack updates take more time. This is normal.

When using the unit, Aastra recommends to disable the Spanning Tree Protocol on the network to which the unit is connected.

CHAPTER

43

Certificates Management

This chapter describes how to transfer and manage certificates into the Aastra unit.

Standards Supported	• RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Introduction

The Aastra unit uses digital certificates, which are a collection of data used to verify the identity of the holder or sender of the certificate.

The certificates contain the following information:

- certificate name
- issuer and issued to names
- Validity period (the certificate is not valid before or after this period)
- Usage of the certificate (Identifies in which role or context a certificate can be used by the host it authenticates).
    - TlsClient: The certificate identifies a TLS client. A host authenticated by this kind of certificate can act as a client in a SIP over TLS connection when mutual authentication is required by the server.
    - TlsServer: The certificate identifies a TLS server. A host authenticated by this kind of certificate can serve files or web pages using the HTTPS protocol or can act as a server in a SIP over TLS connection.
- whether or not the certificate is owned by a CA (Certification Authority)

The Aastra unit uses two types of certificates:

Table 311: Certificates Types

Type	Description
Host	Certificates used to certify the unit (e.g.: a web server with HTTPS requires a host certificate).
Others	Any other certificate including trusted CA certificates used to certify peers (e.g.: a SIP server with TLS).

The transferred certificate must be in Privacy Enhanced Mail (PEM) (host or others) or Distinguished Encoding Rules (DER) (others) format. When transferring a host certificate, the certificate must be appended to the private key to form one PEM file. The private key must not be encrypted.

You can transfer a certificate by using the HTTP or HTTPS protocol, but Aastra recommends to use HTTPS.

To access the unit via HTTPS, your browser must support RFC 2246 (TLS 1.0). The latest version of Microsoft Internet Explorer supports HTTPS browsing.

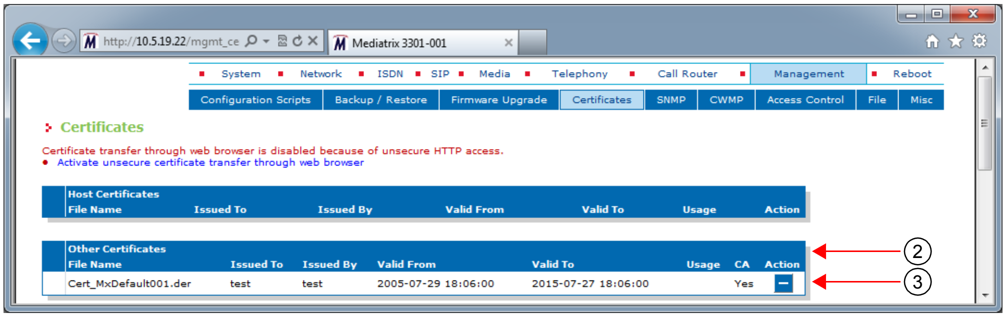
Managing Certificates

You can view certificates information and you can delete certificates.

▶ **To view and manage certificates:**

1. In the web interface, click the *Management* link, then the *Certificates* sub-link.

Figure 199: Management – Certificates Information Web Page



The *Host Certificates* section contains the certificates used to certify the unit. The *Others Certificates* section contains any other certificate used to certify peers.

2. If applicable, delete a certificate in the *Host Certificates* or *Others Certificates* sections by clicking the button of the certificate you want to delete.

3. If applicable, delete a certificate in the *Other Certificates* section by clicking the button of the certificate you want to delete.

4. Click *Submit* if you do not need to set other parameters.

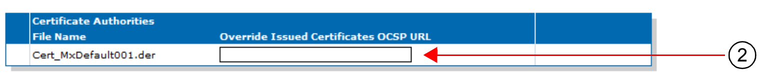
Certificate Authorities

This section contains information specific to certificate authority (CA) files.

▶ **To view and manage certificate authorities information:**

1. In the *Certificate Authorities* section of the *Certificates* page, define a specific OCSP URL to use for certificate revocation status of certificates issued by this certificate authority (CA) in the corresponding *Override OCSP URL* field.

Figure 200: Certificate Authorities Section



The URL should follow one of these formats:

```
http://hostname[:port]
http://hostname/path/filename.xxx
```

Note: The default empty value means that the OCSP URL present in the certificate to verify will be used for checking its revocation status.

2. Click *Submit* if you do not need to set other parameters.

Certificate Upload through the Web Browser

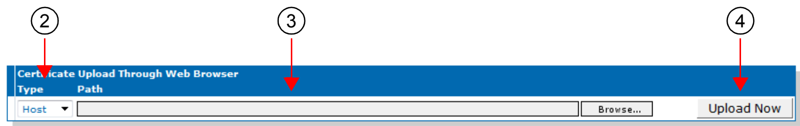
The following steps explain how to transfer (add) a certificate from the web interface.

▶ To upload a certificate:

1. If you are currently using an unsecure HTTP access, the *Certificate Upload Through Web Browser* section is disabled. This is to avoid transferring a certificate in clear text. To enable the section, access the secure site by clicking the *Activate unsecure certificate transfer through web browser* link at the top of the window.
2. In the *Certificate Upload Through Web Browser* section of the *Certificates* page, select the type of the certificate in the *Type* drop-down menu.

   Before transferring the certificate, you must indicate whether this is a Host or Others certificate.

   Figure 201: Certificate Upload Through Web Browser Section

3. Use the *Browse* button to select the certificate to transfer.

   The maximum certificate name is 50 characters.
4. Initiate the certificate upload by clicking the **Upload Now** button.

   The Aastra unit immediately transfers the certificate. Once the certificate is transferred, you must restart the *SipEp* and *Web* services in the *System* > *Services* page ("Chapter 4 - Services" on page 53) before using the newly transferred certificate. Click the link in the message that is displayed to access the *Services* web page.

Transferring a Certificate via Configuration Script

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

You can use a special command to transfer a certificate by configuration script or CLI. This command has the following parameters: URL of the certificate to download, its Type (Host/ Others), the username and password. See "Appendix B - Scripting Language" on page 627 for more details on the Aastra proprietary scripting language

▶ To transfer a certificate via configuration script:

1. Use the following line in the CLI or a configuration script:
   ```
   Cert.DownloadCertificate FileUrl=Value UserName=Value Password=Value Type=Value
   ```

where the different values may be as follows:

Table 312: Certificate Transfer Values

Value	Description
`FileUrl`	URL to a Certificate file that is loaded upon executing the execution of Download command. The transfer protocols supported are: • HTTP • HTTPS • TFTP • FTP Examples of valid URLS: • http://www.myserver.com/Cert_MxDefault001.der • tftp://myserver.com:69/myfolder/Cert_MxDefault001.der When the port is not included in the URL, the default port for the chosen protocol is used. This field may contain some macros that are substituted by the actual value at the moment of fetching the configuration script. The supported macros are: • *%mac%* - the MAC address of the unit. • *%product%* - the Product name of the unit.
`UserName`	When authentication is required by the remote file server, this variable is used as the username.
`Password`	When authentication is required by the remote file server, this variable is used as the password.
`Type`	Type of certificate to transfer. • Host: Certificate used to certify the host system. • Other: Remote systems certificates and issuers certificates.

For instance, a valid command would be:

```
Cert.DownloadCertificate FileUrl=http://www.myserver.com/Cert_MxDefault001.der
UserName=MyName Password=MyPassword Type=Host
```

Host Certificate Associations

The *Host Certificate Associations* section allows you to define which services can use the host certificates.

▶ **To set host certificate associations:**

1. In the *Host Certificate Associations* section of the *Certificates* page, check the services that can use a given host certificate.

Figure 202: Host Certificate Associations Section

Table 313: Host Certificate Associations Parameters

Parameter	Description
SIP	Specifies if this certificate can be used for SIP security.
Web	Specifies if this certificate can be used for Web security.

Table 313: Host Certificate Associations Parameters (Continued)

Parameter	Description
EAP	Specifies if this certificate can be used for EAP security.

2. Click *Submit* if you do not need to set other parameters.

CHAPTER

44

SNMP Configuration

This chapter describes how to set the SNMP parameters of the Aastra unit.

Standards Supported	• RFC 1157: Simple Network Management Protocol (SNMP) • RFC 1910: User-based Security Model for SNMPv2 • RFC 2104: HMAC: Keyed-Hashing for Message Authentication • RFC 2576: Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework • RFC 2741: Agent Extensibility (AgentX) Protocol Version 1 • RFC 3411: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks • RFC 3412: Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) • RFC 3413: Simple Network Management Protocol (SNMP) Applications • RFC 3414: User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) • RFC 3415: View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)[a] • RFC 3416: Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) • RFC 3417: Transport Mappings for the Simple Network Management Protocol (SNMP) • RFC 3826: The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model

a. The Aastra unit complies to RFC 3415 but does not support the related MIBs.

Introduction

All parameters available in the Aastra unit web interface may also be configured via SNMP. The Aastra unit SNMP feature offers the following options:

- Password-protected access
- Remote management
- Simultaneous management

The Aastra unit SNMP feature allows you to configure all the MIB services by using a SNMP browser to contact the MIBs of the Aastra unit. It is assumed that you have basic knowledge of TCP/IP network administration.

Note: The Aastra unit's SNMP settings do not support IPv6. See "IPv4 vs. IPv6 Availability" on page 85 for more details.

You can use the MIB browser built in the Aastra' Unit Manager Network.

You can also use any third-party SNMP browser or network management application running the SNMP protocol to monitor and configure the Aastra unit. However, the information may not be presented in the same manner depending on the SNMP browser used.

Locate the proper parameter to modify and change (SET) its value.

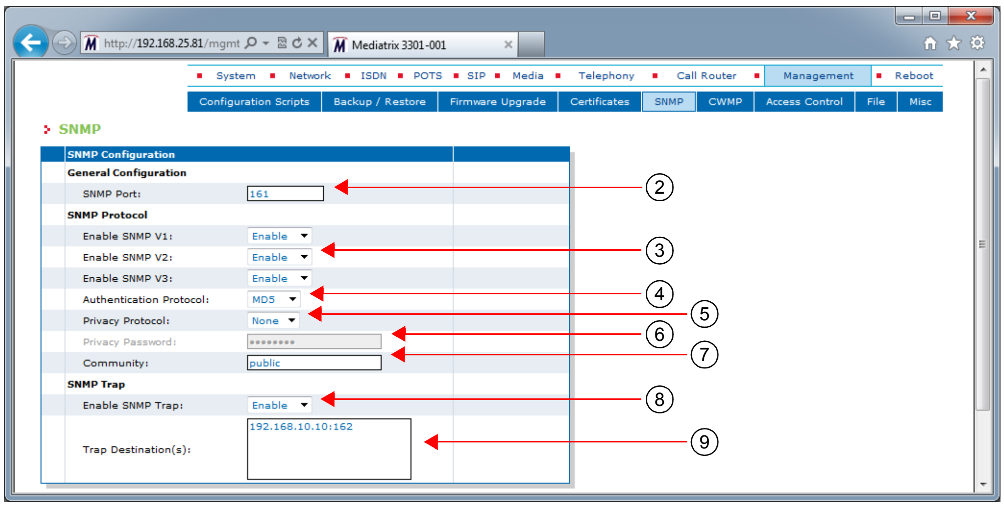
SNMP Configuration Section

The SNMP Configuration section allows you to configure the SNMPv3 privacy information that allows securing the Aastra unit, as well as defining where the Aastra unit must send traps.

▶ **To set SNMP parameters:**

1. In the web interface, click the *Management* link, then the *Snmp* sub-link.

Figure 203: Management – Snmp Web Page



2. Set the *SNMP Listening Port* field with the port number on which the SNMP service listens for incoming SNMP requests.

The default value is **161**.

3. Specify with which SNMP version a user can connect to the system by setting one of the following drop-down menus to **enable**:

Table 314: SNMP Versions

SNMP Version	Drop-down menu to set to Enable
SNMPv1	Enable SNMP V1
SNMPv2	Enable SNMP V2
SNMPv3	Enable SNMP V3

By default, SNMPv3 is enabled.

Caution: It is possible to disable all three versions of SNMP on the Aastra unit. If you do so, you will no longer be able to access the unit in SNMP. To recover from this situation, you must perform a factory reset procedure.

Note: Please note that a “public” user might be granted (unsecure) access by using SNMPv1 or SNMPv2, while an “admin” user should rather be granted a SNMPv3 access. Furthermore, access for users in SNMPv3 will require authentication and could be done with or without privacy according to the unit’s configuration. This means that the unit does not grant an SNMPv3 access without authentication and privacy.

4. If SNMPv3 is enabled, set the *Authentication Protocol* drop-down menu with the authentication protocol to use with SNMPv3.

Table 315: SNMP Authentication Protocol

Protocol	Description
MD5	MD5 encoding is used. This is the default value.
SHA1	SHA1 encoding is used.

Caution: The *Authentication Protocol* field is not accessible if you have the User or Observer access right. See "Users" on page 591 for more details.

SNMPv3 will grant access to all users who are configured in the unit and have a password with 8 characters or more (in the AAA service as described in "Chapter 49 - Access Control Configuration" on page 591).

5. If SNMPv3 is enabled, set the privacy protocol to use with SNMPv3 in the *Privacy Protocol* drop-down menu.

Table 316: SNMP Privacy Protocol

Protocol	Description
None	No encryption is used. The *Privacy Password* parameter is ignored. This is the default value.
DES	DES encryption is used.

Caution: The *Privacy Protocol* field is not accessible if you have the User or Observer access right. See "Users" on page 591 for more details.

6. If you are using the DES privacy, set the password to use in the *Privacy Password* field.

Caution: The *Privacy Password* field is not accessible if you have the User or Observer access right. See "Users" on page 591 for more details.

7. Set the *Community* field with the string to use for the community field of SNMPv1 and SNMPv2 read-write commands and traps.

   This field must not be empty.

   The use of a community name provides context for agents receiving requests and initiating traps. An SNMP agent won't respond to a request from a management system outside its configured community.

   The community name field may influence the AAA user name that will be used by the Aastra for non-authenticated SNMP access (SNMPv1 and SNMPv2). See "Additional SNMP Parameters" on page 441 for more information.

8. Specify that traps can be sent by setting the *Enable SNMP Traps* drop-down menu to **enable**.

   There are five conditions that the Aastra unit checks before sending a trap:

   - The traps are enabled.
   - The destination address is valid.
   - The NetSnmp Agent is ready.
   - The destination address is reachable according to the routing table.
   - The appropriate physical link is up.

If all of those conditions are true, then the Aastra unit sends the traps. If any of those conditions is false, the Aastra unit waits (1 second) and retries until it succeeds. Even if the traps are delayed, they will be sent with the appropriate timestamp when all the conditions are met.

Furthermore, the SNMP version(s) currently enabled (see Step 2 for more details) define which type of trap may be sent.

Table 317: Trap Type Sent vs SNMP Version Enabled

SNMP Version Enabled			Trap Sent	
SNMPv1	**SNMPv2**	**SNMPv3**	**Trap V1**	**Trap V2c**
	Enabled			✓
		Enabled		✓
	Enabled	Enabled		✓
Enabled			✓	
Enabled	Enabled		✓	✓
Enabled		Enabled	✓	✓
Enabled	Enabled	Enabled	✓	✓

Note: You can also enable the traps via the CLI. See "Chapter 2 - Command Line Interface (CLI)" on page 19 for details on how to work with the CLI.

The Aastra unit handles five different types of trap:

Table 318: Trap Types

Trap	Description
coldStart	A coldStart(0) trap means that the sending protocol entity is reinitializing itself so that the agent's configuration or the protocol entity implementation may be altered. This trap is sent prior to a reboot that follows a firmware update, a backup restoration or a default settings application. Note that if the unit is shut down unexpectedly (power failure, power switch), this trap is not emitted. When the unit reboots because of a firmware upgrade, no coldStart traps are sent before this reboot. In that specific case, a coldStart trap is sent after the reboot if the installation scripts succeeded.
warmStart	A warmStart(1) trap means that the sending protocol entity is reinitializing itself so that neither the agent configuration nor the protocol entity implementation is altered. This trap is sent prior to all other reboots. Note that if the unit is shut down unexpectedly (power failure, power switch), this trap is not emitted. When the unit reboots because of a firmware upgrade, no warmStart traps are sent before this reboot. In that specific case, a warmStart trap is sent after the reboot if the installation scripts failed.
linkDown	A linkDown(2) trap means that the SNMPv2 entity acting in an agent role has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state. This other state is indicated by the included value of ifOperStatus. The Trap-PDU of type linkDown includes ifIndex, ifAdminStatus, ifOperStatus (as of RFC 2233) of the interface that generated the trap.

Table 318: Trap Types (Continued)

Trap	Description
linkUp	A linkUp(3) trap means that the SNMPv2 entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus. The Trap-PDU of type linkUp includes ifIndex, ifAdminStatus, ifOperStatus (as of RFC 2233) of the interface that generated the trap.
authenticationFailure	An authenticationFailure(4) trap means that the sending protocol entity is the addressee of a protocol message that is not properly authenticated. This trap is sent when an authentication failure occurs from the Web, CLI or SNMP interface.

9. If the traps are enabled, set the *Trap Destination (s)* field with the addresses/FQDNs and ports where to send traps.

   You can specify up to 5 destinations by using a comma between them (comma is not authorized within a FQDN). The port numbers are optional. Note that the traps are sent simultaneously to all destinations.

   Example:

   `trapdest.com:2345, 123.45.67.89`

   The default value is **192.168.10.10:162**.

10. Click *Submit* if you do not need to set other parameters.

Additional SNMP Parameters

This section describes configuration that is available only in the MIB parameters of the Aastra unit. You can configure these parameters as follows:

- by using a MIB browser
- by using the CLI
- by creating a configuration script containing the configuration variables

A user name can be added to be used by the SNMP v1/v2 to access the configuration.

For non-authenticated access (SNMPv1 and SNMPv2), the Aastra will use the AAA user name from the *SnmpUser* variable if it is not empty. If empty, the community name is used as the AAA user name.

To add an SNMP user name:

1. In the *snmpMIB*, set the *SnmpUser* variable to a valid AAA user name.

   You can also use the following line in the CLI or a configuration script:

   snmp.`SnmpUser`="Value"

   where *Value* is a valid AAA user name.

Caution: If the provided SNMP user name does not exist in the *AAA.UsersStatus* table or if the SNMP user name is empty and the community name does not exist in the *AAA.UsersStatus* table, the SNMP access will fail.

Partial Reset

When a partial reset is triggered, the following parameters are affected:

- Listening Port: Default value **161**.
- Enable SNMPv1: Default value **disable**.
- Enable SNMPv2: Default value **disable**.

- Enable SNMPv3: Default value **enable**.

See “Partial Reset” on page 15 for more details.

SNMP Statistics

The following are the statistics the Aastra unit keeps.

Table 319: SNMP Statistics

MIB Variable	Statistics Description
`statsGetRequest`	Number of GET requests handled by the service.
`statsGetNextRequest`	Number of GET-NEXT requests handled by the service.
`statsSetRequest`	Number of SET requests handled by the service.

CHAPTER
45
Access Control Configuration

This chapter describes how to set the Access Control parameters of the Aastra unit.

Standards Supported	• RFC 2617: HTTP Authentication: Basic and Digest Access Authentication • RFC 2865: Remote Authentication Dial In User Service (RADIUS) • RFC 2866: RADIUS Accounting

Caution: The *Access Control* page is not accessible if you have the User or Observer access right. See "Users" on page 443 for more details.

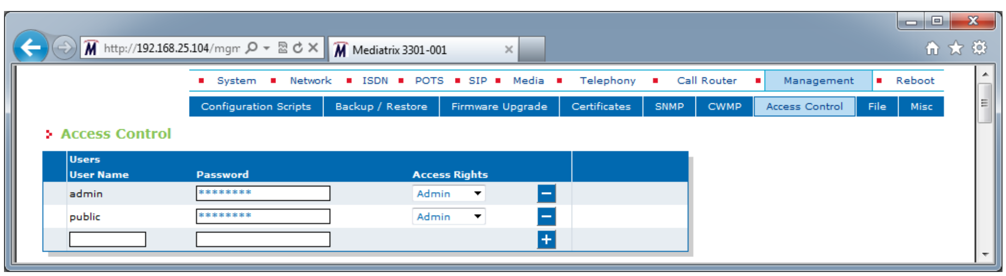
Users

The *Users* section allows you to manage the users that can access the web interface. You can add a maximum of 10 users.

To manage users:

1. In the web interface, click the *Management* link, then the *Access Control* sub-link.

Figure 204: Management – Access Control Web Page



2. If you want to add a new user, enter its name in the blank *User Name* field in the bottom left of the window, enter the corresponding password in the blank *Password* field, then click the + button.

   The name is case-sensitive.

3. If you want to delete an existing user, click the corresponding − button.

   If you delete all users in the table, the profile's default user(s) will be used upon unit restart.

Note: A system restart is required to completely remove the user. The current activities of this user are not terminated on removal.

4. If you want to change the password of an existing user, type it in the corresponding *Password* field.

   The password is case sensitive. All characters are allowed.

5. Define the access rights template applying to a user in the corresponding *Access Rights* drop-down menu.

You have the following choices:

Table 320: Access Rights

Access Right	Description
Admin	User is allowed to read and modify all variables of the unit.
User	User is allowed to read and modify all variables except passwords and secrets.
Observer	User is only allowed to read variables that are not passwords or secrets.

See “Access Rights Description” on page 447 for mode details on the various operations allowed with each access right.

6. Click *Submit* if you do not need to set other parameters.

Partial Reset

When a partial reset is triggered, the password and access rights reset back to the default value (see “Partial Reset” on page 15 for more details).

Services Access Control Type

The *Services Access Control Type* section allows you to define the type of authentication and accounting to use for the CLI, SNMP, and Web services.

Authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted.

Accounting measures the resources a user consumes during access. This can include the amount of system time or the amount of data a user has sent and/or received during a session.

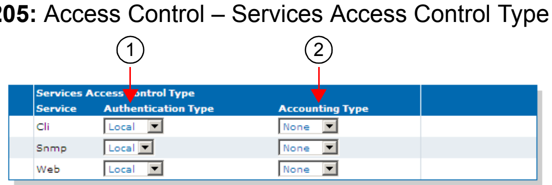
▶ **To set the Services Access Control type:**

1. In the *Services Access Control Type* section of the *Access Control* page, set the authentication type a service uses for incoming authentication requests in the corresponding *Authentication Type* column.

Table 321: Authentication Types

Type	Description
Local	Incoming authentication attempts are validated against the user names and passwords stored in the Local Users table (see “Users” on page 443 for more details).
Radius	Incoming authentication attempts are validated against the first responding Radius server configured in the *Radius Servers* section (“Radius Servers” on page 445). When no server is configured or the servers are unreachable, an authentication attempt of type Local is performed against the user names and passwords stored in the Local Users table (see “Users” on page 443 for more details). **Note:** This type is not available for the SNMP interface.

Figure 205: Access Control – Services Access Control Type Section



2. Set the accounting type a service uses in the corresponding *Accounting Type* column.

   Accounting starts once users are successfully authenticated and stops when their session is over.

Table 322: Accounting Types

Type	Description
None	Accounting is disabled.
Radius	Accounting is done by the first responding Radius server configured in the *Radius Servers* section ("Radius Servers" on page 445).

3. Click *Submit* if you do not need to set other parameters.

Partial Reset

When a partial reset is triggered, the Radius authentication is disabled (see "Partial Reset" on page 15 for more details).

Radius Servers

The *Radius Servers* section allows you to define up to three Radius servers. It also allows you to define authentication server and accounting server information, for the CLI, SNMP, and Web services.

Note: The Aastra unit's Radius server settings do not support IPv6. See "IPv4 vs. IPv6" on page 85 for more details.

Radius Authentication occurs when the *Authentication Type* column of the *Services Access Control Type* section ("Services Access Control Type" on page 444) is set to **Radius** for the service from which the authentication request is coming. You can configure up to three Radius servers for each service listed in the *Select a Service* drop-down menu. The first authentication attempt is sent to the Radius server with the highest priority, which is set in the *Priority* column (1 being the highest priority). When authentication fails or the request reaches the timeout set in the *Server Request Timeout* field, the next server with the highest priority is used. When all servers have failed to reply or no servers are configured for the service asking for authentication, authentication is attempted against local user names and passwords as a fallback strategy. Radius authentication is available for the CLI and Web services.

Radius Accounting is enabled by setting the *Accounting Type* column of the *Services Access Control Type* section ("Services Access Control Type" on page 444) to **Radius** for one or more services. When such a configuration is set, accounting requests made through those services are forwarded to a Radius server configured in the *Radius Servers* section. You can configure up to three Radius servers for each service listed in the *Select a Service* drop-down menu. The first accounting request is sent to the Radius server with the highest priority, which is set in the *Priority* column (1 being the highest priority). When the accounting request fails or the request reaches the timeout set in the *Server Request Timeout* field, the next server with the highest priority is used. The CLI, Web, and SNMP services can use the accounting functionality.

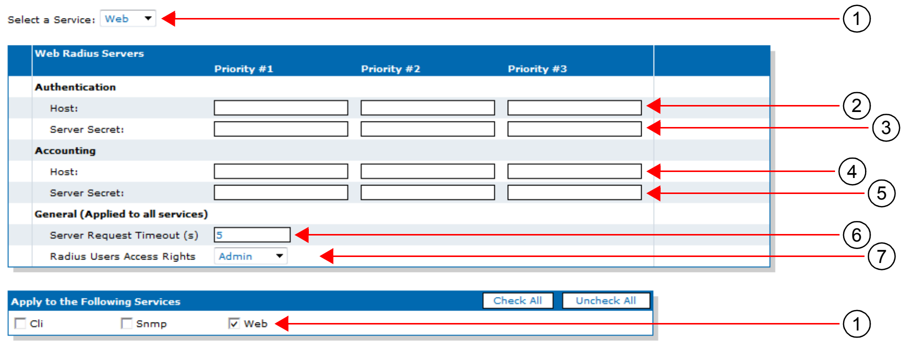
▶ **To set the Radius servers information:**

1. Select to which service you want to apply the changes in the *Select a Service* drop-down menu above the *Radius Servers* section.

   You can copy the configuration of the selected service to one or more services of the Aastra unit in the *Apply to the Following Services* section at the bottom of the page. You can select specific services by checking them, as well as use the *Check All* or *Uncheck All* buttons.

2. In the *Authentication* part of the *Radius Servers* section, set the host name and port of a Radius server used for authentication requests in the corresponding *Host* field.

Figure 206: Access Control – Radius Servers Section



You can configure up to three Radius servers with a different priority.

Note: This parameter is not available for the SNMP service.

3. Set the secret key shared between the Radius server and the unit in the corresponding *Server Secret* field.

The Authentication Secret key must be the same as the secret key stored on the corresponding Radius authentication server.

Note: This parameter is not available for the SNMP service.

4. In the *Accounting* part, set the host name and port of a Radius server used for accounting requests in the corresponding *Host* field.

You can configure up to three Radius servers with a different priority.

5. Set the secret key shared between the Radius server and the unit in the corresponding *Server Secret* field.

The Accounting Secret key must be the same as the secret key stored on the corresponding Radius accounting server.

6. Set the *Server Request Timeout* field with the maximum time, in milliseconds, the unit waits for a reply from a Radius server.

This parameter applies to all services. Upon reaching the timeout, the request is sent to the next configured server.

7. Define the access rights template applying to a user in the corresponding *Radius Users Access Rights* drop-down menu.

This parameter applies to all services. You have the following choices:

Table 323: Radius Users Access Rights

Access Right	Description
Admin	User is allowed to read and modify all variables of the unit.
User	User is allowed to read and modify all variables except passwords and secrets.
Observer	User is only allowed to read variables that are not passwords or secrets.

See “Access Rights Description” on page 447 for mode details on the various operations allowed with each access right.

8. Click *Submit* if you do not need to set other parameters.

Access Rights Description

You have three templates of rights from which you can select the permissions given to each user allowed in a unit (see "Users" on page 443 and "Radius Servers" on page 445).

The following table describes the various operations allowed with each access right.

Table 324: Access Rights Description

Access Right	Observer	User	Admin
Read configuration	**Yes**	**Yes**	**Yes**
Modify Configuration	No	**Yes**[a]	**Yes**
Read/Write Passwords	No	No	**Yes**
Change Access Rights	No	No	**Yes**
Execute Configuration Script	No	**Yes**[a]	**Yes**
Export Configuration	No	**Yes**[a]	**Yes**
Backup/Restore configuration	No	No	**Yes**
Firmware updates	No	No	**Yes**

a. Passwords cannot be changed and will not be exported to a configuration script.

CHAPTER 46

File Manager

This chapter describes how to use the unit's File Manager.

File Manager

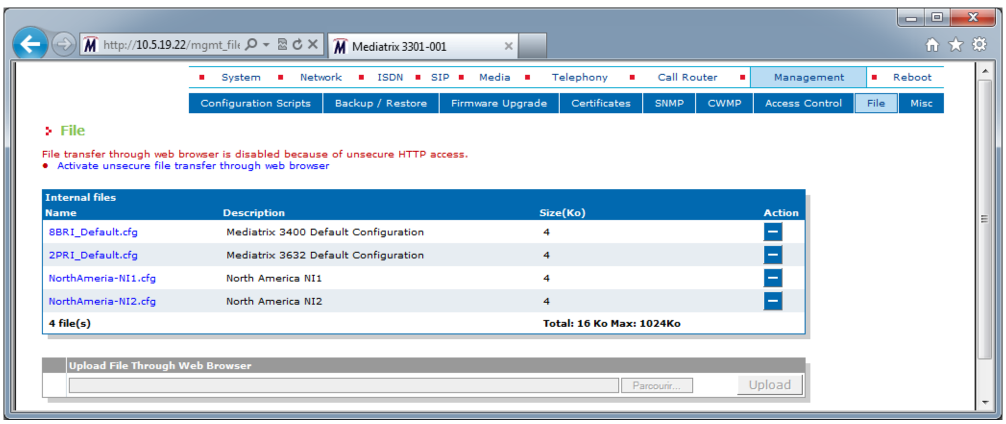
The *File* page allows you to view and delete the files you have created with the File transfer protocol, for instance, a configuration backup..

> **Note:** The files under the File service are not included in the backup process. In the same way, the restore process will not remove any file under the File service.

To use the File manager:

1. In the web interface, click the *Management* link, then the *File* sub-link.

Figure 207: Management – File Web Page



If you want to delete an existing file, click the corresponding button.

You can directly download a file via your web browser by clicking it. You will then be able to see its contents.

2. To add a file to the unit's File System, type the path and name of the file to add in the field of the *Upload File Through Web Browser* section, or select an existing one on the PC with the **Browse** button.

   If you are currently using an unsecure HTTP access, the *Upload File Through Web Browser* section is disabled. This is to avoid transferring a file in clear text. To enable the section, access the secure site by clicking the *Activate unsecure file transfer through web browser* link at the top of the window.

3. Click **Submit**.

Partial Reset

When a partial reset is triggered, the user-defined presets are deleted.

CHAPTER

47

Miscellaneous

This chapter describes how to set various parameters used to manage the Aastra unit.

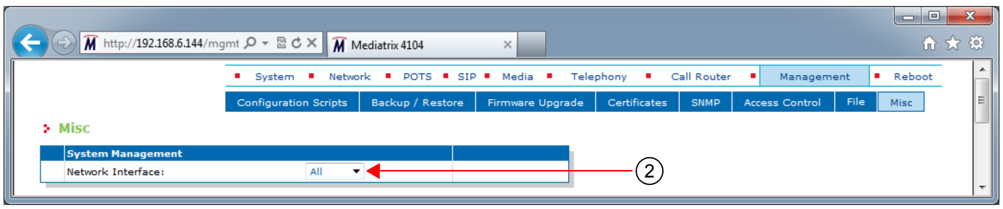
Management Interface Configuration

The *Miscellaneous* page allows you to specify which one of the existing network interfaces is used to manage the Aastra unit.

▶ **To set the system management interface:**

1. In the web interface, click the *Management* link, then the *Misc* sub-link.

Figure 208: Management – Misc Web Page



2. Select which one of the existing network interfaces is used to manage the device in the *Network Interface* drop-down menu.

   The management services (typically Web and/or SNMP) can be reached through this network interface.

   Before the system management services can be used, they need to be bound (or linked) to a physical port of your Aastra unit.

   The special value "All" means to bind all network interfaces.

3. Click *Submit* if you do not need to set other parameters.

Partial Reset

When a partial reset is triggered, the Management Interface reverts back to its default value.

Appendices

Page Left Intentionally Blank

APPENDIX

A

Country-Specific Parameters

The following parameters differ depending on the country in which you are.

Definitions

The following are some useful definitions.

Table 325: Definitions

Term	Description
Dial Tone	Indicates the endpoint is ready to receive dialing.
Busy Tone	Indicates the endpoint or equipment is in use, engaged or occupied.
Ringback Tone	Indicates the called line is ringing out.
Special Information Tone	Identifies network-provided announcements.
Stutter Dial Tone	Notifies the user that they have a voice mail message when the phone does not or cannot have a message-waiting light.
Confirmation Tone	Confirms a command performed by the user (such as activate a service).
Receiver Off Hook (ROH) Tone	Indicates that the telephone is not hung up correctly.
Message Waiting Indicator Tone	Indicates there is a message waiting somewhere for the owner of the phone
Network Congestion Tone	Indicates that all switching paths are busy, all toll trunks are busy, or there are equipment blockages.
Intercept Tone	Indicates that you have dialed incorrectly or that the feature you've requested is not available on your terminal.
Preemption Tone	In military telephone systems, a distinctive tone that is used to indicate to connected users, i.e., subscribers, that their call has been preempted by a call of higher precedence.
Reorder Tone	Indicates that all switching paths are busy, all toll trunks are busy, there are equipment blockages, the caller dialled an unassigned code, or the digits dialled got messed up along the way.
FED Tone	Indicates the far end tone detection.

Conventions

The following conventions apply to this Appendix.

Frequencies

- Symbol “*” means modulated. For instance: 425 Hz * 25 means 425 Hz modulated at 25 Hz.
- Symbol “+” means added. For instance: 425 Hz + 330 Hz means that both 425 Hz and 330 Hz

sines are played at the same time.

- When a tone is composed of more than one frequency, if not otherwise specified, the given electrical level applies to each frequency taken separately.

Impedance

Impedance is the apparent resistance, in an electric circuit, to the flow of an alternating current, analogous to the actual electrical resistance to a direct current, being the ratio of electromotive force to the current.

When representing an impedance, the following applies:

- Symbol "//" means parallel.
- Symbol "+" means serial.

Furthermore, there are two types of impedances:

- Input Impedance
- Terminal Balance Return Loss (TBRL) Impedance

Input Impedance

Impedance of the Aastra at the Tip and Ring wires.

Terminal Balance Return Loss (TBRL) Impedance

Balance return loss attributable to transmission loss between two points. It is used to characterize an impedance balancing property of the 2-wire analog equipment port.

Each country has its own definition of the TBRL value. For instance, in North America, TIA/EIA 464 (and TIA/EIA 912) define two TBRL values:

- 600 Ω for "on-premise" or short loop ports.
- 350 Ω + (1000 Ω || 21 nF) for "off-premise" or long loop ports.

A wire length above 2.5 km is considered long loop according to TIA/EIA 912 section 6.4 (7)(b)).

In Europe, ETSI 300 439 also mentions a TBRL value. However, most European countries have different requirements regarding the TBRL Impedance. This is also true for other countries around the world. Each one of them has different requirements.

Line Attenuation

Values are given in dBr (deciBel relative):

- A "+" for input means that the digital side is attenuated by x decibels relative to the analog side.
- A "+" for output means that the analog side is amplified by x decibels relative to the digital side.
- A "-" for input means that the digital side is amplified by x decibels relative to the analog side.
- A "-" for output means that the analog side is attenuated by x decibels relative to the digital side.

On-Off Sequences

Values in bold are "on" cycles, where tones are audible. Values in normal style are "off" cycles, where tones are not audible. When not otherwise specified, sequences repeat forever. A "x" symbol means that the sequences between parenthesis is repeated x times. The next cycle(s) repeat forever, unless otherwise specified. Values are in seconds.

For instance:

3*(**0.1** - 0.1) then **0.6** - 1.0 - **0.2** - 0.2

means that the 0.1s on and 0.1s off sequence is repeated 3 times, afterwards the 0.6s on, 1.0s off, 0.2s on and 0.2s off sequence repeats forever.

Australia

The following parameters apply if you have selected Australia as location.

Australia 1

The following parameters apply if you have selected Australia 1 as location.

Table 326: Australia 1 Parameters

Parameter	Value	**On –** Off - *CID* **Sequence (s)**	Elect. Levels
Busy Tone	425 Hz	**0.38** – 0.38	-18 dBm
Call Waiting Tone	425 Hz	**0.2** - 0.2, **0.2** - *4.4*, **0.2** - 0.2, **0.2** - 4.4	-23 dBm
Dial Tone	425 Hz 400 Hz 450 Hz	**CONTINUOUS** **CONTINUOUS** **CONTINUOUS**	-18 dBm -24 dBm -24 dBm
Message Waiting Indicator Tone	425 Hz 400 Hz 450 Hz	**(0.1 - 0.04)x72, CONTINUOUS** (0.1 - 0.04)x72, CONTINUOUS (0.1 - 0.04)x72, CONTINUOUS	-18 dBm -24 dBm -24 dBm
Network Congestion Tone	425 Hz 425 Hz	**0.38** - 0.38, 0.38 - 0.38 0.38 - 0.38, **0.38** - 0.38	-13 dBm -23 dBm
Receiver Off Hook (ROH) Tone	2350 Hz	**CONTINUOUS**	-5 dBm
Reorder Tone	425 Hz	**2.5** - 0.5	-18 dBm
Ringback Tone	425 Hz 400 Hz 450 Hz	**0.4** - 0.2, **0.4** - 2.0 **0.4** - 0.2, **0.4** - 2.0 **0.4** - 0.2, **0.4** - 2.0	-18 dBm -24 dBm -24 dBm
Special Information Tone	425 Hz	**2.5** - 0.5	-18 dBm
Stutter Dial Tone	425 Hz 400 Hz 450 Hz	**CONTINUOUS** **CONTINUOUS** **CONTINUOUS**	-18 dBm -24 dBm -24 dBm
Ring	AC: 53 VRMS, 25 Hz DC: -10 Vdc	**0.4** - 0.2, **0.4** - 2.0	
Loop Current	30 ma		
Input Impedance (FXS)	600 Ω		
Input Impedance (FXO)	600 Ω		
Tbrl-Impedance	600 Ω		
FED Tone	425 Hz	**8.0**	
Default Caller ID (FXS)	BELLCORE		
FXS Line Attenuation (Input)			+0 dBr
FXS Line Attenuation (Output)			-6 dBr
FXO Line Attenuation (Input)			+6 dBr
FXO Line Attenuation (Output)			+0 dBr
Delay Before Answering	2 seconds		
Delay Before Dialing (No Dial Tone Detection)	4 seconds		

Australia 2

The following parameters apply if you have selected Australia 2 as location.

Table 327: Australia 2 Parameters

Parameter	Value	**On –** Off - *CID* **Sequence (s)**	Elect. Levels
Busy Tone	425 Hz	**0.38** – 0.38	-18 dBm
Call Waiting Tone	425 Hz	**0.2** - 0.2, **0.2** - *4.4*, **0.2** - 0.2, **0.2** - 4.4	-23 dBm
Dial Tone	425 Hz 400 Hz 450 Hz	**CONTINUOUS** **CONTINUOUS** **CONTINUOUS**	-18 dBm -24 dBm -24 dBm
Message Waiting Indicator Tone	425 Hz 400 Hz 450 Hz	**(0.1 - 0.04)x72, CONTINUOUS** (0.1 - 0.04)x72, CONTINUOUS (0.1 - 0.04)x72, CONTINUOUS	-18 dBm -24 dBm -24 dBm
Network Congestion Tone	425 Hz 425 Hz	**0.38** - 0.38, 0.38 - 0.38 0.38 - 0.38, **0.38** - 0.38	-13 dBm -23 dBm
Receiver Off Hook (ROH) Tone	2350 Hz	**CONTINUOUS**	-5 dBm
Reorder Tone	425 Hz	**2.5** - 0.5	-18 dBm
Ringback Tone	425 Hz 400 Hz 450 Hz	**0.4** - 0.2, **0.4** - 2.0 **0.4** - 0.2, **0.4** - 2.0 **0.4** - 0.2, **0.4** - 2.0	-18 dBm -24 dBm -24 dBm
Special Information Tone	425 Hz	**2.5** - 0.5	-18 dBm
Stutter Dial Tone	425 Hz 400 Hz 450 Hz	**CONTINUOUS** **CONTINUOUS** **CONTINUOUS**	-18 dBm -24 dBm -24 dBm
Ring	AC: 53 VRMS, 25 Hz DC: -10 Vdc	**0.4** - 0.2, **0.4** - 2.0	
Loop Current	30 ma		
Input Impedance (FXS)	220 Ω + 820 Ω // 120 nF		
Input Impedance (FXO)	220 Ω + 820 Ω // 115 nF		
Tbrl-Impedance	220 Ω + 820 Ω // 120 nF		
FED Tone	425 Hz	**8.0**	
Default Caller ID (FXS)	BELLCORE		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-9 dBr
FXO Line Attenuation (Input)			+6 dBr
FXO Line Attenuation (Output)			+0 dBr
Delay Before Answering	2 seconds		
Delay Before Dialing (No Dial Tone Detection)	4 seconds		

Austria

The following parameters apply if you have selected Austria1 as location.

Table 328: Austria1 Parameters

Parameter	Value	**On –** Off - *CID* **Sequence (s)**	Elect. Levels
Busy Tone	450 Hz	**0.3** – 0.3	-20 dBm
Call Waiting Tone	440 Hz	2.0 – **0.3**, *10.0* – **0.3**, 10.0	-17 dBm
Confirmation Tone	450 Hz	(**0.1** – 0.1) x 3 End	-20 dBm
Dial Tone	450 Hz	**CONTINUOUS**	-20 dBm
Message Waiting Indicator Tone	450 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-20 dBm
Network Congestion Tone	450 Hz	**0.3** – 0.3	-20 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	**0.1** – 0.1	-19 dBm
Reorder Tone	950 Hz 1400 Hz 1800 Hz	**0.33** - 0.33 - 0.33 - 1.0 0.33 - **0.33** - 0.33 - 1.0 0.33 - 0.33 - **0.33** - 1.0	-20 dBm -20 dBm -20 dBm
Ringback Tone	450 Hz	**1.0** – 5.0	-20 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** - 0.33 - 0.33 - 1.0 0.33 - **0.33** - 0.33 - 1.0 0.33 - 0.33 - **0.33** - 1.0	-20 dBm -20 dBm -20 dBm
Stutter Dial Tone	450 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-20 dBm
Ring (FXS)	AC: 45 VRMS, 50 Hz DC: -15 Vdc	**1.0** – 5.0	
Loop Current	30 ma		
Flash Hook Detection Range	Min: 170 ms Max: 900 ms		
Input Impedance (FXS)	220 Ω + 820 Ω // 115 nF		
Input Impedance (FXO)	270 Ω + 750 Ω // 150 nF		
Tbrl-Impedance	600 Ω		
FED Tone	450 Hz	**8.0**	
Default Caller ID (FXS)	BELLCORE		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-10 dBr
FXO Line Attenuation (Input)			+6 dBr
FXO Line Attenuation (Output)			-1 dBr
Delay Before Answering	0 seconds		
Delay Before Dialing (No Dial Tone Detection)	4 seconds		

Brazil

The following parameters apply if you have selected Brazil as location.

Table 329: Brazil Parameters

Parameter	Value	**On –** Off - *CID* **Sequence (s)**	Elect. Levels
Busy Tone	425 Hz	**0.25** – 0.25	-10 dBm
Call Waiting Tone	440 Hz	2.0 – **0.3**, *10.0* – **0.3**, 10.0	-17 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3 End	-15 dBm
Dial Tone	425 Hz	**CONTINUOUS**	-15 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-15 dBm
Network Congestion Tone	425 Hz	**0.2** – 0.2	-10 dBm
Receiver Off Hook (ROH) Tone	425 Hz	**0.25** – 0.25	-10 dBm
Reorder Tone	425 Hz	**0.75** – 0.25, **0.25** – 0.25	-10 dBm
Ringback Tone	425 Hz	**1.0** – 4.0	-15 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** - 0.03 - 0.33 - 0.03 - 0.33 - 1.0 0.33 - 0.03 - **0.33** - 0.03 - 0.33 - 1.0 0.33 - 0.03 - 0.33 - 0.03 - **0.33** - 1.0	-15 dBm -15 dBm -15 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-15 dBm
Ring (FXS)	AC: 45 VRMS, 25 Hz DC: -15 Vdc	**1.0** – 4.0	
Loop Current	30 ma		
Flash Hook Detection Range	Min: 170 ms Max: 900 ms		
Input Impedance (FXS)	900 Ω		
Input Impedance (FXO)	900 Ω		
Tbrl-Impedance	800 Ω // 50 nF		
FED Tone	425 Hz	**8.0**	
Default Caller ID (FXS)	TELEBRAS_DTMF		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr
FXO Line Attenuation (Input)			6 dBr
FXO Line Attenuation (Output)			0 dBr
Delay Before Answering	0 seconds		
Delay Before Dialing (No Dial Tone Detection)	0 seconds		

China

The following parameters apply if you have selected China as location.

Table 330: China Parameters

Parameter	Value	**On –** Off - *CID* **Sequence (s)**	Elect. Levels
Busy Tone	450 Hz	**0.35** – 0.35	-10 dBm
Call Waiting Tone	450 Hz	**0.4** – *4.0*, **0.4** – 4.0	-20 dBm
Confirmation Tone	450 Hz	(**0.1** – 0.1) x 3, End	-10 dBm
Dial Tone	450 Hz	**CONTINUOUS**	-10 dBm
Intercept Tone	450 Hz	**0.2** – 0.2, **0.2** – 0.6	-20 dBm
Message Waiting Indicator Tone	450 Hz	**0.4** – 0.04	-10 dBm
Network Congestion Tone	450 Hz	**0.7** – 0.7	-10 dBm
Preemption Tone	450 Hz	**0.2** – 0.2, **0.2** – 0.6	-20 dBm
Receiver Off Hook (ROH) Tone	950 Hz 950 Hz 950 Hz 950 Hz	**5.0** – 5.0 – 5.0 – 5.0 5.0 – **5.0** – 5.0 – 5.0 5.0 – 5.0 – **5.0** – 5.0 5.0 – 5.0 – 5.0 – **5.0**	-25 dBm -16 dBm -8 dBm -6 dBm
Reorder Tone	450 Hz	**0.1** – 0.1, **0.1** – 0.1, **0.1** – 0.1, **0.4** – 0.4	-10 dBm
Ringback Tone	450 Hz	**1.0** – 4.0	-10 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** - 0.33 - 0.33 - 1.0 0.33 - **0.33** - 0.33 - 1.0 0.33 - 0.33 - **0.33** - 1.0	-10 dBm -10 dBm -10 dBm
Stutter Dial Tone	450 Hz	**0.4** – 0.04	-10 dBm
Ring	AC: 45 VRMS, 25 Hz DC: -15 Vdc	**1.0** – 4.0	
Loop Current	30 ma		
Flash Hook Detection Range	Min: 170 ms Max: 900 ms		
Input Impedance (FXS)	600 Ω		
Input Impedance (FXO)	600 Ω		
Tbrl-Impedance	600 Ω		
FED Tone	450 Hz	**8.0**	
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-9 dBr
FXO Line Attenuation (Input)			0 dBr
FXO Line Attenuation (Output)			0 dBr
Delay Before Answering	0 seconds		
Delay Before Dialing (No Dial Tone Detection)	0 seconds		

Czech Republic

The following parameters apply if you have selected Czech Republic1 as location.

Table 331: Czech Republic1 Parameters

Parameter	Value	**On –** Off - *CID* **Sequence (s)**	Elect. Levels
Busy Tone	425 Hz	**0.33** – 0.33	-12 dBm
Call Waiting Tone	425 Hz	2.0 – **0.33**, *10.0* – **0.33**, 10.0	-11 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3, End	-12 dBm
Dial Tone	425 Hz	**0.33** – 0.33, **0.66** – 0.66	-12 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10, **0.33** – 0.33, **0.66** – 0.66	-12 dBm
Network Congestion Tone	425 Hz	**0.17** – 0.17	-12 dBm
Receiver Off Hook (ROH) Tone	425 Hz	**0.17** – 0.17	-12 dBm
Ringback Tone	425 Hz	**1.0** – 4.0	-12 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** - 0.33 - 0.33 - 1.0 0.33 - **0.33** - 0.33 - 1.0 0.33 - 0.33 - **0.33** - 1.0	-12 dBm -12 dBm -12 dBm
Stutter Dial Tone	425 Hz	(**0.17** – 0.17) x 3, **0.66** – 0.66	-12 dBm
Ring (FXS)	AC: 45 VRMS, 25 Hz DC: -15 Vdc	**1.0** – 4.0	
Loop Current	30 ma		
Flash Hook Detection Range	Min: 170 ms Max: 900 ms		
Input Impedance (FXS)	600 Ω		
Input Impedance (FXO)	270 Ω + 750 Ω // 150 nF		
Tbrl Impedance	220 Ω + 820 Ω // 115 nF		
FED Tone	425 Hz	**0.165** – 0.165	
Default Caller ID (FXS)	V23		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr
FXO Line Attenuation (Input)			+6 dBr
FXO Line Attenuation (Output)			-1 dBr
Delay Before Answering	0 seconds		
Delay Before Dialing (No Dial Tone Detection)	4 seconds		

France

The following parameters apply if you have selected France1 as location.

Table 332: France1 Parameters

Parameter	Value	**On –** Off - *CID* **Sequence (s)**	Elect. Levels
Busy Tone	440 Hz	**0.5** – 0.5	-20 dBm
Call Waiting Tone	440 Hz	2.0 – **0.3**, *10.0* – **0.3**, 10.0	-17 dBm
Confirmation Tone	440 Hz	(**0.1** – 0.1) x 3, End	-17 dBm
Dial Tone	440 Hz	**CONTINUOUS**	-17 dBm
Message Waiting Indicator Tone	440 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-17 dBm
Network Congestion Tone	440 Hz	**0.25** – 0.25	-20 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	**0.1** – 0.1	-19 dBm
Ringback Tone	440 Hz	**1.5** – 3.5	-20 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.3** - 0.03 - 0.3 - 0.03 - 0.3 - 1.0 0.3 - 0.03 - **0.3** - 0.03 - 0.3 - 1.0 0.3 - 0.03 - 0.3 - 0.03 - **0.3** - 1.0	-20 dBm -20 dBm -20 dBm
Stutter Dial Tone	440 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-17 dBm
Ring (FXS)	AC: 45 VRMS, 50 Hz DC: -15 Vdc	**1.5** – 3.5	
Loop Current	30 ma		
Flash Hook Detection Range	Min: 170 ms Max: 900 ms		
Input Impedance (FXS)	215 Ω + 1000 Ω // 137 nF		
Input Impedance (FXO)	270 Ω + 750 Ω // 150 nF		
Tbrl-Impedance	600 Ω		
FED Tone	440 Hz	**8.0**	
Default Caller ID (FXS)	BELLCORE		
FXS Line Attenuation (Input)			+1.9 dBr
FXS Line Attenuation (Output)			-8.9 dBr
FXO Line Attenuation (Input)			+6 dBr
FXO Line Attenuation (Output)			-1 dBr
Delay Before Answering	0 seconds		
Delay Before Dialing (No Dial Tone Detection)	4 seconds		

Germany

The following parameters apply if you have selected Germany as location.

Germany 1

The following parameters apply if you have selected Germany 1 as location.

Table 333: Germany 1 Parameters[a]

Parameter	Value	On – Off - *CID* Sequence (s)	Elect. Levels
Busy Tone	425 Hz	**0.48** – 0.48	-16 dBm
Call Waiting Tone	440 Hz	**0.3** – End	-17 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3, End	-16 dBm
Dial Tone	425 Hz	**CONTINUOUS**	-16 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-16 dBm
Network Congestion Tone	425 Hz	**0.24** – 0.24	-16 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	**0.1** – 0.1	-19 dBm
Ringback Tone	425 Hz	**1.0** – 4.0	-16 dBm
Special Information Tone	900 Hz 1400 Hz 1800 Hz	**0.33** - 0.33 - 0.33 - 1.0 0.33 - **0.33** - 0.33 - 1.0 0.33 - 0.33 - **0.33** - 1.0	-16 dBm -16 dBm -16 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-16 dBm
Ring (FXS)	AC: 45 VRMS, 25 Hz DC: -15 Vdc	**1.0** – 4.0	
Loop Current	30 ma		
Flash Hook Detection Range	Min: 170 ms Max: 900 ms		
Input Impedance (FXS)	220 Ω + 820 Ω // 115 nF		
Input Impedance (FXO)	270 Ω + 750 Ω // 150 nF		
Tbrl-Impedance	220 Ω + 820 Ω // 115 nF		
FED Tone	425 Hz	**8.0**	
Default Caller ID (FXS)	BELLCORE		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-10 dBr
FXO Line Attenuation (Input)			+6 dBr
FXO Line Attenuation (Output)			-1 dBr
Delay Before Answering	0 seconds		
Delay Before Dialing (No Dial Tone Detection)	4 seconds		

a. The Germany 2 choice in the MIB is exactly the same as Germany 1.

Germany 2

The following parameters apply if you have selected Germany 2 as location.

Table 334: Germany 2 Parameters

Parameter	Value	**On –** Off - *CID* **Sequence (s)**	Elect. Levels
Busy Tone	425 Hz	**0.48** – 0.48	-13 dBm
Call Waiting Tone	440 Hz	2.0 – **0.3**, *10.0* – **0.3**, 10.0	-17 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3, End	-13 dBm
Dial Tone	425 Hz	**CONTINUOUS**	-13 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-13 dBm
Network Congestion Tone	425 Hz	**0.24** – 0.24	-13 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	**0.1** – 0.1	-16 dBm
Ringback Tone	425 Hz	**1.0** – 4.0	-13 dBm
Special Information Tone	900 Hz 1400 Hz 1800 Hz	**0.33** - 0.33 - 0.33 - 1.0 0.33 - **0.33** - 0.33 - 1.0 0.33 - 0.33 - **0.33** - 1.0	-13 dBm -13 dBm -13 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-13 dBm
Ring (FXS)	AC: 57 VRMS, 25 Hz DC: -5 Vdc	**1.0** – 4.0	
Loop Current	30 ma		
Flash Hook Detection Range	Min: 170 ms Max: 900 ms		
Input Impedance (FXS)	220 Ω + 820 Ω // 115 nF		
Input Impedance (FXO)	270 Ω + 750 Ω // 150 nF		
Tbrl-Impedance	220 Ω + 820 Ω // 115 nF		
FED Tone	425 Hz	**8.0**	
Default Caller ID (FXS)	BELLCORE		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr
FXO Line Attenuation (Input)			+6 dBr
FXO Line Attenuation (Output)			-1 dBr
Delay Before Answering	0 seconds		
Delay Before Dialing (No Dial Tone Detection)	4 seconds		

Israel2

The following parameters apply if you have selected Israel2 as location.

Table 335: Israel2 Parameters

Parameter	Value	**On –** Off - *CID* **Sequence (s)**	Elect. Levels
Busy Tone	400 Hz	**0.5** – 0.5	-14 dBm
Call Waiting Tone	400 Hz	**0.5** – *10.0*, **0.5** – 10.0	-16 dBm
Confirmation Tone	400 Hz	**0.17** – 0.34, **0.14** – 0.14, End	-14 dBm
Dial Tone	400 Hz	**CONTINUOUS**	-14 dBm
Hold Tone	400 Hz	**0.05** – 2.0, End	-16 dBm
Message Waiting Indicator Tone	400 Hz	(**0.16** – 0.16) x 10, **CONTINUOUS**	-14 dBm
Network Congestion Tone	400 Hz	**0.25** – 0.25	-14 dBm
Receiver Off Hook (ROH) Tone	1440+2060+2452+2600 Hz	**0.12** – 0.1	-14 dBm
Reorder Tone	1000 Hz 1400 Hz 1800 Hz	**0.33** - 0.33 - 0.33 - 1.0 0.33 - **0.33** - 0.33 - 1.0 0.33 - 0.33 - **0.33** - 1.0	-14 dBm -14 dBm -14 dBm
Ringback Tone	400 Hz	**1.0** – 3.0	-14 dBm
Special Information Tone	450 + 150 Hz	**0.5** – End	-14 dBm
Stutter Dial Tone	400 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-15 dBm
Ring	AC: 45 VRMS, 25 Hz DC: -15 Vdc	**1.0** – 3.0	
Loop Current	30 ma		
Flash Hook Detection Range	Min: 170 ms Max: 900 ms		
Input Impedance (FXS)	600 Ω		
Input Impedance (FXO)	600 Ω		
Tbrl-impedance	600 Ω		
FED Tone	400 Hz	**8.0**	
Default Caller ID (FXS)	BELLCORE		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-9 dBr
FXO Line Attenuation (Input)			0 dBr
FXO Line Attenuation (Output)			0 dBr
Delay Before Answering	0 seconds		
Delay Before Dialing (No Dial Tone Detection)	0 seconds		

Italy

The following parameters apply if you have selected Italy1 as location.

Table 336: Italy1 Parameters

Parameter	Value	On – Off - *CID* Sequence (s)	Elect. Levels
Busy Tone	425 Hz	**0.5** – 0.5	-13 dBm
Call Waiting Tone	440 Hz	2.0 – **0.3**, *10.0* – **0.3**, 10.0	-17 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3, End	-13 dBm
Dial Tone	425 Hz	**0.2** – 0.2, **0.6** – 1.0	-13 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10, **0.2** – 0.2, **0.6** – 1.0	-13 dBm
Network Congestion Tone	425 Hz	**0.2** – 0.2	-13 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	**0.1** – 0.1	-19 dBm
Ringback Tone	425 Hz	**1.0** – 4.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** - 0.33 - 0.33 - 1.0 0.33 - **0.33** - 0.33 - 1.0 0.33 - 0.33 - **0.33** - 1.0	-20 dBm -20 dBm -20 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **0.2** – 0.2, **0.6** – 1.0	-13 dBm
Ring (FXS)	AC: 45 VRMS, 25 Hz DC: -15 Vdc	**1.0** – 4.0	
Loop Current	30 ma		
Flash Hook Detection Range	Min: 170 ms Max: 900 ms		
Input Impedance (FXS)	180 Ω + 630 Ω // 60 nF		
Input Impedance (FXO)	270 Ω + 750 Ω // 150 nF		
Tbrl-impedance	750 Ω // 18 nF		
FED Tone	425 Hz	**0.2** – 0.2, **0.6** – 1.0	
Default Caller ID (FXS)	BELLCORE		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr
FXO Line Attenuation (Input)			+6 dBr
FXO Line Attenuation (Output)			-1 dBr
Delay Before Answering	0 seconds		
Delay Before Dialing (No Dial Tone Detection)	4 seconds		

Japan

The following parameters apply if you have selected Japan 2 as location.

Table 337: Japan 2 Parameters

Parameter	Value	On – Off - *CID* Sequence (s)	Elect. Levels
Busy Tone	400 Hz	**0.5** – 0.5	-13 dBm
Call Waiting Tone	400 Hz	2.0 - **0.3**, *10.0* - **0.3**, 10.0	-17 dBm
Confirmation Tone	400 Hz	(**0.1** – 0.1) x 3, End	-13 dBm
Dial Tone	400 Hz	**CONTINUOUS**	-19 dBm
Message Waiting Indicator Tone	400 Hz	(**0.1** - 0.1)x10, **CONTINUOUS**	-13 dBm
Network Congestion Tone	400 Hz	**0.5** – 0.5	-13 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	**0.1** – 0.1	-19 dBm
Ringback Tone	400 Hz 420 Hz 380 Hz	**1.0** – 2.0 **1.0** – 2.0 **1.0** – 2.0	-16 dBm -22 dBm -22 dBm
Special Information Tone	400 Hz	**0.1** – 0.1	-13 dBm
Stutter Dial Tone	400 Hz	(**0.1** - 0.1)x3, **CONTINUOUS**	-13 dBm
Ring	AC: 45 VRMS, 20 Hz DC: -15 Vdc	**1.0** – 2.0	
Loop Current	30 ma		
Input Impedance (FXS)	600 Ω + 1000 nF		
Input Impedance (FXO)	600 Ω		
Tbrl-Impedance	600 Ω + 1000 nF		
FED Tone	400 Hz	**8.0**	
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			+0 dBr
FXS Line Attenuation (Output)			-9 dBr
FXO Line Attenuation (Input)			+0 dBr
FXO Line Attenuation (Output)			+0 dBr
Delay Before Answering	2 seconds		
Delay Before Dialing (No Dial Tone Detection)	3 seconds		

Mexico

The following parameters apply if you have selected Mexico as location.

Table 338: Mexico Parameters

Parameter	Value	**On –** Off - *CID* **Sequence (s)**	Elect. Levels
Busy Tone	425 Hz	**0.25** – 0.25	-18 dBm
Call Waiting Tone	440 Hz	2.0 – **0.3**, *10.0* – **0.3**, 10.0	-17 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3, End	-14 dBm
Dial Tone	425 Hz	**CONTINUOUS**	-14 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10 **CONTINUOUS**	-14 dBm
Network Congestion Tone	425 Hz	**0.25** – 0.25	-18 dBm
Preemption Tone	425 Hz	**0.5** – 0.17, **0.17** – 0.17	-18 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	**0.1** – 0.1	-19 dBm
Ringback Tone	425 Hz	**1.0** – 4.0	-16 dBm
Special Information Tone	900 Hz 1400 Hz 1800 Hz	**1.0** - 1.0 - 1.0 - 1.0 1.0 - **1.0** - 1.0 - 1.0 1.0 - 1.0 - **1.0** - 1.0	-14 dBm -14 dBm -14 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-14 dBm
Ring	AC: 45 VRMS, 25 Hz DC: -15 Vdc	**1.0** – 4.0	
Loop Current	30 ma		
Flash Hook Detection Range	Min: 170 ms Max: 900 ms		
Input Impedance (FXS)	600 Ω		
Input Impedance (FXO)	600 Ω		
Tbrl-impedance	600 Ω		
FED Tone	425 Hz	**8.0**	
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-3 dBr
FXO Line Attenuation (Input)			0 dBr
FXO Line Attenuation (Output)			0 dBr
Delay Before Answering	0 second		
Delay Before Dialing (No Dial Tone Detection)	0 second		

North America

The following parameters apply if you have selected North America as location.

North America 1

The following parameters apply if you have selected North America 1 as location.

Table 339: North America 1 Parameters

Parameter	Value	**On –** Off - *CID* **Sequence (s)**	Elect. Levels
Busy Tone	480+620 Hz	**0.5** – 0.5	-21 dBm
Call Waiting Tone	440 Hz	2.0 – **0.3**, *10.0* – **0.3**, 10.0	-17 dBm
Confirmation Tone	350+440 Hz	(**0.1** – 0.1) x 3, End	-17 dBm
Dial Tone	350+440 Hz	**CONTINUOUS**	-17 dBm
Intercept Tone	440+620 Hz	**0.5** – 0.5	-14 dBm
Message Waiting Indicator Tone	350+440 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-17 dBm
Network Congestion Tone	480+620 Hz	**0.25** – 0.25	-21 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	**0.1** – 0.1	-19 dBm
Reorder Tone	480+620 Hz	**0.3** – 0.2	-21 dBm
Ringback Tone	440+480 Hz	**2.0** – 4.0	-19 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** - 0.33 - 0.33 - 1.0 0.33 - **0.33** - 0.33 - 1.0 0.33 - 0.33 - **0.33** - 1.0	-14 dBm
Stutter Dial Tone	350+440 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-17 dBm
Ring (FXS)	AC: 45 VRMS, 20 Hz DC: -15 Vdc	**2.0** – 4.0	
Loop Current	30 ma		
Flash Hook Detection Range	Min: 300 ms Max: 1100 ms		
Input Impedance (FXS)	600 Ω		
Input Impedance (FXO)	600 Ω		
Tbrl-Impedance[a] (FXS)	600 Ω		
FED Tone	440 Hz	**8.0**	
Default Caller ID (FXS)	BELLCORE		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-3 dBr
FXO Line Attenuation (Input)			0 dBr
FXO Line Attenuation (Output)			0 dBr
Delay Before Answering	0 seconds		
Delay Before Dialing (No Dial Tone Detection)	0.7 seconds		

a. TBRL-Impedance for “on-premise” or short loop ports.

Spain

The following parameters apply if you have selected Spain1 as location.

Table 340: Spain1 Parameters

Parameter	Value	**On –** Off - *CID* **Sequence (s)**	Elect. Levels
Busy Tone	425 Hz	**0.2** – 0.2	-13 dBm
Call Waiting Tone	440 Hz	2.0 – **0.3**, *10.0* – **0.3**, 10.0	-17 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3, End	-10 dBm
Dial Tone	425 Hz	**CONTINUOUS**	-10 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-10 dBm
Network Congestion Tone	425 Hz	**0.2** – 0.2, **0.2** – 0.2, **0.2** – 0.6	-13 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	**0.1** – 0.1	-19 dBm
Reorder Tone	425 Hz	**0.2** – 0.2, **0.2** – 0.6	-13 dBm
Ringback Tone	425 Hz	**1.5** – 3.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** - 0.33 - 0.33 - 1.0 0.33 - **0.33** - 0.33 - 1.0 0.33 - 0.33 - **0.33** - 1.0	-20 dBm -20 dBm -20 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-10 dBm
Ring (FXS)	AC: 45 VRMS, 25 Hz DC: -15 Vdc	**1.5** – 3.0	
Loop Current	30 ma		
Flash Hook Detection Range	Min: 170 ms Max: 900 ms		
Input Impedance (FXS)	220 Ω + 820 Ω // 120 nF		
Input Impedance (FXO)	270 Ω + 750 Ω // 150 nF		
Tbrl-Impedance	220 Ω + 820 Ω // 120 nF		
FED Tone	425 Hz	**8.0**	
Default Caller ID (FXS)	BELLCORE		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-7 dBr
FXO Line Attenuation (Input)			+6 dBr
FXO Line Attenuation (Output)			-1 dBr
Delay Before Answering	0 seconds		
Delay Before Dialing (No Dial Tone Detection)	4 seconds		

Switzerland

The following parameters apply if you have selected Switzerland as location.

Table 341: Switzerland Parameters

Parameter	Value	On – Off - *CID* Sequence (s)	Elect. Levels
Busy Tone	425 Hz	**0.5** – 0.5	-13 dBm
Call Waiting Tone	440 Hz	2.0 – **0.3**, *10.0* – **0.3**, 10.0	-17 dBm
Confirmation Tone	425 Hz	(**0.1** – 0.1) x 3, End	-8 dBm
Dial Tone	425 Hz	**CONTINUOUS**	-8 dBm
Message Waiting Indicator Tone	425 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-8 dBm
Network Congestion Tone	425 Hz	**0.2** – 0.2	-13 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	**0.1** – 0.1	-19 dBm
Ringback Tone	425 Hz	**1.0** – 4.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** - 0.33 - 0.33 - 1.0 0.33 - **0.33** - 0.33 - 1.0 0.33 - 0.33 - **0.33** - 1.0	-13 dBm -13 dBm -13 dBm
Stutter Dial Tone	425 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-8 dBm
Ring (FXS)	AC: 45 VRMS, 25 Hz DC: -15 Vdc	**1.0** – 4.0	
Loop Current	30 ma		
Flash Hook Detection Range	Min: 170 ms Max: 900 ms		
Input Impedance (FXS)	220 Ω + 820 Ω // 115 nF		
Input Impedance (FXO)	270 Ω + 750 Ω // 150 nF		
Tbrl-impedance	220 Ω + 820 Ω // 115 nF		
FED Tone	425 Hz	**8.0**	
Default Caller ID (FXS)	BELLCORE		
FXS Line Attenuation (Input)			0 dBr
FXS Line Attenuation (Output)			-6.5 dBr
FXO Line Attenuation (Input)			+6 dBr
FXO Line Attenuation (Output)			-1 dBr
Delay Before Answering	0 seconds		
Delay Before Dialing (No Dial Tone Detection)	4 seconds		

United Arab Emirates

The following parameters apply if you have selected United Arab Emirates as location.

United Arab Emirates 2

The following parameters apply if you have selected the United Arab Emirates 2 as location.

Table 342: United Arab Emirates 2 Parameters

Parameter	Value	**On –** Off - *CID* **Sequence (s)**	Elect. Levels
Busy Tone	400 Hz	**0.38** – 0.38	-13 dBm
Call Waiting Tone	425 Hz	(**0.2** – *12.0*, **0.2** –12.0)x2 End	-13 dBm
Confirmation Tone	400 Hz	(**0.1** – 0.1) x 3 End	-13 dBm
Dial Tone	350+450 Hz	**CONTINUOUS**	-13 dBm
Message Waiting Indicator Tone	350+440 Hz	(**0.1** – 0.1) x 10 **CONTINUOUS**	-13 dBm
Network Congestion Tone	400 Hz	**0.4** – 0.35, **0.23** – 0.53	-13 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	(**0.1** – 0.1)	-19 dBm
Reorder Tone	400 Hz	**CONTINUOUS**	-13 dBm
Ringback Tone	425 Hz	**0.4** – 0.2, **0.4** – 2.0	-13 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** – 0.33, 0.33 – 1.0 0.33 – **0.33**, 0.33 – 1.0 0.33 – 0.33, **0.33** – 1.0	-13 dBm -13 dBm -13 dBm
Stutter Dial Tone	350+450 Hz	(**0.4** – 0.04-) x 5 **CONTINUOUS**	-13 dBm
Ring	AC: 45 VRMS, 25 Hz DC: -15 Vdc	**0.4** – 0.2, **0.4** – 2.0	
Loop Current	30 ma		
Flash Hook Detection Range	Min: 170 ms Max: 900 ms		
Input Impedance (FXS)	600 Ω		
Input Impedance (FXO)	600 Ω		
Tbrl-impedance	600 Ω		
FED Tone	440 Hz	**8.0**	
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-3 dBr
FXO Line Attenuation (Input)			+0 dBr
FXO Line Attenuation (Output)			+0 dBr
Delay Before Answering	0 seconds		
Delay Before Dialing (No Dial Tone Detection)	0 seconds		

United Arab Emirates 3

The following parameters apply if you have selected the United Arab Emirates 3 as location.

Table 343: United Arab Emirates 3 Parameters

Parameter	Value	**On –** Off - *CID* **Sequence (s)**	Elect. Levels
Busy Tone	400 Hz	**0.38** – 0.38	-19 dBm

Table 343: United Arab Emirates 3 Parameters (Continued)

Parameter	Value	**On –** Off - *CID* **Sequence (s)**	Elect. Levels
Call Waiting Tone	440 Hz	2.0 – **0.3**, *10.0* –**0.3**, 10.0	-17 dBm
Confirmation Tone	350+440 Hz	(**0.1** – 0.1) x 3 End	-22 dBm
Dial Tone	350+440 Hz	**CONTINUOUS**	-22 dBm
Message Waiting Indicator Tone	350+440 Hz	(**0.1** – 0.1) x 10 **CONTINUOUS**	-22 dBm
Network Congestion Tone	400 Hz	**0.4** – 0.35, **0.23** – 0.53	-19 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	(**0.1** – 0.1)	-19 dBm
Reorder Tone	400 Hz	**CONTINUOUS**	-19 dBm
Ringback Tone	400+450 Hz	**0.4** – 2.0, **0.4** – 0.2	-22 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** – 0.33, 0.33 – 1.0 0.33 – **0.33**, 0.33 – 1.0 0.33 – 0.33, **0.33** – 1.0	-19 dBm -19 dBm -19 dBm
Stutter Dial Tone	350+440 Hz	(**0.1** – 0.1-) x 3 **CONTINUOUS**	-22 dBm
Ring	AC: 45 VRMS, 25 Hz DC: -15 Vdc	**0.4** – 2.0, **0.4** – 0.2	
Loop Current	30 ma		
Flash Hook Detection Range	Min: 170 ms Max: 900 ms		
Input Impedance (FXS)	600 Ω		
Input Impedance (FXO)	600 Ω		
Tbrl-impedance	600 Ω		
FED Tone	440 Hz	**8.0**	
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-3 dBr
FXO Line Attenuation (Input)			+0 dBr
FXO Line Attenuation (Output)			+0 dBr
Delay Before Answering	0 seconds		
Delay Before Dialing (No Dial Tone Detection)	0 seconds		

United Arab Emirates 4

The following parameters apply if you have selected the United Arab Emirates 4 as location.

Table 344: United Arab Emirates 4 Parameters

Parameter	Value	**On –** Off - *CID* **Sequence (s)**	Elect. Levels
Busy Tone	400 Hz	**0.38** – 0.38	-19 dBm
Call Waiting Tone	440 Hz	2.0 – **0.3**, *10.0* –**0.3**, 10.0	-17 dBm
Confirmation Tone	350+440 Hz	(**0.1** – 0.1) x 3 End	-22 dBm
Dial Tone	350+440 Hz	**CONTINUOUS**	-13 dBm
Message Waiting Indicator Tone	350+440 Hz	(**0.1** – 0.1) x 10 **CONTINUOUS**	-22 dBm
Network Congestion Tone	400 Hz	**0.4** – 0.35, **0.23** – 0.53	-19 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	(**0.1** – 0.1)	-19 dBm
Reorder Tone	400 Hz	**CONTINUOUS**	-19 dBm
Ringback Tone	400+450 Hz	**0.4** – 2.0, **0.4** – 0.2	-22 dBm

Table 344: United Arab Emirates 4 Parameters (Continued)

Parameter	Value	**On –** Off - *CID* **Sequence (s)**	Elect. Levels
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** – 0.33, 0.33 – 1.0 0.33 – **0.33**, 0.33 – 1.0 0.33 – 0.33, **0.33** – 1.0	-19 dBm -19 dBm -19 dBm
Stutter Dial Tone	350+440 Hz	(**0.1** – 0.1-) x 3 **CONTINUOUS**	-22 dBm
Ring	AC: 45 VRMS, 25 Hz DC: -15 Vdc	**0.4** – 2.0, **0.4** – 0.2	
Loop Current	30 ma		
Flash Hook Detection Range	Min: 170 ms Max: 900 ms		
Input Impedance (FXS)	600 Ω		
Input Impedance (FXO)	600 Ω		
Tbrl-impedance	600 Ω		
FED Tone	440 Hz	**8.0**	
Default Caller ID	BELLCORE		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-3 dBr
FXO Line Attenuation (Input)			+0 dBr
FXO Line Attenuation (Output)			+0 dBr
Delay Before Answering	0 seconds		
Delay Before Dialing (No Dial Tone Detection)	0 seconds		

UK

The following parameters apply if you have selected the United Kingdom as location.

Table 345: UK Parameters

Parameter	Value	**On –** Off - *CID* **Sequence (s)**	Elect. Levels
Busy Tone	400 Hz	**0.38** – 0.38	-19 dBm
Call Waiting Tone	440 Hz	2.0 – **0.3**, *10.0* – **0.3**, 10.0	-17 dBm
Confirmation Tone	350+440 Hz	(**0.1** – 0.1) x 3, End	-22 dBm
Dial Tone	350+440 Hz	**CONTINUOUS**	-22 dBm
Message Waiting Indicator Tone	350+440 Hz	(**0.1** – 0.1) x 10, **CONTINUOUS**	-22 dBm
Network Congestion Tone	400 Hz	**0.4** – 0.35, **0.23** – 0.53	-19 dBm
Receiver Off Hook (ROH) Tone	1400+2060+2450+2600 Hz	**0.1** – 0.1	-19 dBm
Reorder Tone	400 Hz	**CONTINUOUS**	-19 dBm
Ringback Tone	400+450 Hz	**0.4** – 0.2, **0.4** – 2.0	-22 dBm
Special Information Tone	950 Hz 1400 Hz 1800 Hz	**0.33** – 0.33, 0.33 – 1.0 0.33 – **0.33**, 0.33 – 1.0 0.33 – 0.33, **0.33** – 1.0	-19 dBm -19 dBm -19 dBm
Stutter Dial Tone	350+440 Hz	(**0.1** – 0.1) x 3, **CONTINUOUS**	-22 dBm
Ring (FXS)	AC: 45 VRMS, 25 Hz DC: -15 Vdc	**0.4** – 0.2, **0.4** – 2.0	
Loop Current	30 ma		
Flash Hook Detection Range	Min: 170 ms Max: 900 ms		
Input Impedance (FXS)	300 Ω + 1000 Ω // 220 nF		
Input Impedance (FXO)	320 Ω + 1050 Ω // 230 nF		
Tbrl-impedance	370 Ω + 620 Ω // 310 nF		
FED Tone	440 Hz	**8.0**	
Default Caller ID (FXS)	V23		
FXS Line Attenuation (Input)			-3 dBr
FXS Line Attenuation (Output)			-9 dBr
FXO Line Attenuation (Input)			+6 dBr
FXO Line Attenuation (Output)			-1 dBr
Delay Before Answering	0 seconds		
Delay Before Dialing (No Dial Tone Detection)	4 seconds		

APPENDIX

B Scripting Language

This appendix describes the Aastra proprietary scripting language. It also lists a few configuration samples that can be pasted or typed into the CLI (see “Chapter 2 - Command Line Interface (CLI)” on page 11 for more details) or downloaded into the Aastra via the Configuration Script feature (see“Chapter 40 - Creating a Configuration Script” on page 414.

You can substitute the values listed in these examples with your own values. When enums are involved, refer to the MIB structure with a MIB browser to determine the actual value you need to insert. You can also refer to the *Configuration Reference Guide*, which lists all the parameters, tables, and commands available in the Aastra.

This appendix covers the following topics:

- General Scripting Language Syntax
- Assigning scalar values
- Assigning table cell values
- Executing commands
- Variable Values (Enums)
- Call Router Specific Information
- Examples

General Scripting Language Syntax

The Aastra proprietary scripting language can be used to assign values to configuration variables and execute configuration commands. The scripting language may be used when creating configuration scripts and when working with the Command Line Interface (“Chapter 2 - Command Line Interface (CLI)” on page 11).

Using the scripting language requires a bit of knowledge about the Aastra’s configuration variables tree structure.

The scripting language uses the following general syntax:

```
[keyword] [Context_Name [separator expression [operator constant]]] [#comment]
```

All specific syntaxes in this Appendix are derived from this general syntax.

Note that the brackets ([and]) are used to mark optional arguments. They are not part of the syntax.

Table 346: Scripting Language Syntax

Token Types	Description
`keyword`	A token that defines the type of operation to execute on `expression` or the type of data to retrieve from `expression`. Currently, only the ***set*** keyword is supported, which assigns value of `constant` to `expression`.
`Context_Name`	Defines to which service the following `expression` belongs. For instance, the Configuration Manager `context` is *Conf*, the Firmware Pack Updater `context` is *Fpu*, and the Host Configuration `context` is *Hoc*.
`separator`	Delimiter defined as “.” (dot).

Table 346: Scripting Language Syntax (Continued)

Token Types	Description
`expression`	String that describes a configuration object. It can resolve to either: • a scalar variable • a cell • a column • a row • a table When a service, a scalar, a command or a table variable has the same name as a keyword, you should use the "get" and "set " keywords to access this variable.
`operator`	Only the assignment operator (=) is defined.
`constant`	A textual string or a number to assign to `expression`.
`comment`	Anything following the comment marker (#) up to the end of the line is ignored.

Supported Characters

When using the scripting language, the following ASCII codes are supported:

```
10  LF, line feed               62  >, greater than           94  ^, caret
13  CR, carriage return         63  ?, question mark          95  _, underscore
32  space                       64  @, commercial at          96  `, back quote
33  !, exclamation mark         65  A                         97  a
34  ", double quote             66  B                         98  b
35  #, hash                     67  C                         99  c
36  $, dollar                   68  D                         100 d
37  %, percent                  69  E                         101 e
38  &, ampersand                70  F                         102 f
39  ', quote                    71  G                         103 g
40  (, open parenthesis         72  H                         104 h
41  ), close parenthesis        73  I                         105 i
42  *, asterisk                 74  J                         106 j
43  +, plus                     75  K                         107 k
44  ,, comma                    76  L                         108 l
45  -, minus                    77  M                         109 m
46  ., full stop                78  N                         110 n
47  /, oblique stroke           79  O                         111 o
48  0, zero                     80  P                         112 p
49  1                           81  Q                         113 q
50  2                           82  R                         114 r
51  3                           83  S                         115 s
52  4                           84  T                         116 t
53  5                           85  U                         117 u
54  6                           86  V                         118 v
55  7                           87  W                         119 w
56  8                           88  X                         120 x
57  9                           89  Y                         121 y
58  :, colon                    90  Z                         122 z
59  ;, semicolon                91  [, open square bracket    123 {, open curly bracket
60  <, less than                92  \, backslash              124 |, vertical bar
61  =, equals                   93  ], close square bracket   125 }, close curly bracket
                                                              126 ~, tilde
```

All other ASCII codes are invalid.

Note that you must escape the XML reserved characters when inserting them in a configuration script:

- < : <
- > : >
- % : %

- & : &

Assigning Scalar Values

The following is a sample script command assigning a value to a scalar configuration variable:

```
Service_Name.Scalar_Name=value
```

Table 347: Scalar Syntax

Command	Description
`Service_Name`	Defines which service should process the expression. For instance, the Configuration Manager `context` is *Conf*, the Firmware Pack Updater `context` is *Fpu*, and the Host Configuration `context` is *Hoc*.
`Scalar_Name`	Name of the specific variable to which assign a value.
`value`	A textual string or a number to assign to the argument.

A valid script line would be:

```
Cli.InactivityTimeOut=25
```

Assigning Table Cell Values

When you want to get the value of a specific table cell or set the value of a specific table cell, you must follow a particular syntax:

```
[get]Service_Name.Table_Name[Index=key].Column_Name
[set]Service_Name.Table_Name[Index=key].Column_Name=<value>
```

Table 348: Table Cell Syntax

Command	Description
`Service_Name`	Defines which service should process the expression. For instance, the Configuration Manager `context` is *Conf*, the Firmware Pack Updater `context` is *Fpu*, and the Host Configuration `context` is *Hoc*.
`Table_Name`	Name of the table that contains the cell.
`index=key`	List of index values identifying the row on which the cell is located. The list of indexes is in the name=value form, separated by spaces and enclosed within brackets. The index is always the first column of a table.
`Column_Name`	Name of the column that contains the cell.
`value`	A textual string or a number to assign to the argument.

Let's take for instance the *NetworkInterfacesStatus* table:

InterfaceName	InterfaceStatus	LinkName	IpAddr
Interface1	100[a]		10.1.1.1
Interface2	400[b]		10.1.1.2
Interface3	400	[c][d]	10.1.1.3

a. This enum means "disabled"

b. This enum means "ok"
c.
d.

If you want to get the IP address value of Interface 3, you would have to enter the following command:

```
get Bni.NetworkInterfacesStatus[InterfaceName=Interface3].IpAddr
```

Executing Commands

Configuration commands are used to make the Aastra perform actions such as restarting the unit, restarting a service, refreshing its SIP registration, etc.

There are two types of commands you can execute:

- Normal Commands
- Row Commands

Normal Commands

The normal command feature has the following syntax:

```
Service_Name.Command_Name arg1=value1 –b arg2=[value2 value3 value4]
```

Table 349: Normal Command Syntax

Command	Description
`Service_Name`	Defines which service should process the command. For instance, the Configuration Manager `context` is *Conf*, the Firmware Pack Updater `context` is *Fpu*, and the Host Configuration `context` is *Hoc*.
`Command_Name`	The command to execute.
`arg`*n*	Name of the argument for which you want to assign a value. Three types of arguments are allowed: • flags (beginning with '-', without anything else, for instance, "-b" in the command syntax above). Flags are optional. • scalar arguments (with mandatory '=' and following value). They are mandatory unless they have a default value, in which case they are optional. • vector arguments (with mandatory '=' and following a list of values enclosed within brackets and separated by spaces). They are mandatory unless they have a default value, in which case they are optional. The number and types of arguments depend on the specific command you are using.
`value`*n*	A textual string or a number to assign to the argument.

For instance, a valid command would be:

```
Conf.BackupImage FileName=backup_test_1 Location=/testfiles/Conf/v1/ManualTests/
TransferProtocol=400 TransferUsername=testuser TransferPassword=test
TransferSrvHostname="test1.Aastra.com"
```

Another valid command (without arguments) would be:

```
SipEp.RegistrationRefresh
```

Double Quotes

You must use double quotes when the text parameter contains special characters such as dot or "#". For instance, entering the following command results in a bad command:

```
Conf.BackupImage FileName=test.cfg Location=config TransferProtocol=400
TransferUsername=Usr1 TransferPassword=Pwd1 TransferSrvHostname=192.168.6.3
```

You must enclose each text parameter that contains special characters such as dot or "#" with double quotes. In the above example, you must enclose FileName=test.cfg and TransferSrvHostname=192.168.6.3 in double quotes:

```
Conf.BackupImage FileName="test.cfg" Location=config TransferProtocol=400
TransferUsername=Usr1 TransferPassword=Pwd1 TransferSrvHostname="192.168.6.3"
```

Row Commands

Row commands appear as table cells and allow you to perform an action on a specific row of the relevant table.

Row commands are available in several services of the Aastra. For instance, the Call Router service uses the `Up`, `Down`, `Insert`, and `Delete` commands in its various tables.

The row command feature has the following syntax:

```
Context_Name.Table_Name[index1=value1 index2=value2].Row_Command=execute_value
```

Table 350: Row Command Syntax

Command	Description
`Context_Name`	Defines which service should process the command. For instance, the Configuration Manager `context` is *Conf*, the Firmware Pack Updater `context` is *Fpu*, and the Host Configuration `context` is *Hoc*.
`Table_Name`	Table where the row command is located.
`indexn=valuen`	List of index values identifying the row on which to execute the command. The list of indexes is in the name=value form, separated by spaces and enclosed within brackets. The index is always the first column of a table. See "Assigning Table Cell Values" on page 479 for more details.
`Row_Command`	The row command to execute.
`execute_value`	Numerical value of the enum.

For instance, the following executes the service Dhcp's StaticLeases Delete row command on one of the table's rows. The *StaticLeases* table only has one index column: the *MacAddress* column. The *Delete* row command is an enum that has two possible values: *noOp (0)* and *delete (10)*. The command is executed by assigning the execute value (10) to the Delete cell.

```
Dhcp.StaticLeases[MacAddress="0090F8001234"].Delete=10
```

DeleteAllRows Command

The *DeleteAllRows* command is a table command that you can use to delete all rows of a specific table to start anew. You can use it as follows:

```
Service_Name.Table_Name.DeleteAllRows
```

A valid command would be:

```
CRout.MappingExpression.DeleteAllRows
```

Variable Values (Enums)

The scripting language represents enums with their numeric value, and not their textual value. For instance, the TFTP transfer protocol values available are as follows:

- 100
- 200

- 300
- 400
- 500

This does not mean much. By looking into the MIB structure of the Aastra with a MIB browser or requesting help on the variable in the CLI, you will be able to determine that the values really mean the following:

- 100: HTTP
- 200: HTTPS
- 300: TFTP
- 400: FTP
- 500: FILE

Call Router Specific Information

When working with call router parameters, you must be aware of the following:

- You must prefix the name of a route with “route-”, for instance: **route-***isdn_sip*.
- You must prefix the name of a SIP interface with “sip-”, for instance: **sip-***default*.
- You must prefix the name of an ISDN interface with “isdn-”, for instance: **isdn-***default*.
- You must prefix the name of a hunt with “hunt-”, for instance: **hunt-***hunt1*.

Examples

This section gives a few configuration samples that can be used both in the CLI or as part of a configuration script.

Management Functions

The following sections describe how to perform some useful management functions such as a configuration backup/restore and changing the default user password.

Configuration Backup / Restore

Each of the two following commands must be created in one line.

```
Conf.BackupImage FileName="image.text" Location="resultfolder" TransferProtocol=300
TransferUsername=""  TransferPassword=""  TransferSrvHostname=“192.168.3.4"

Conf.RestoreImage FileName="image.text" Location="resultfolder" TransferProtocol=300
TransferUsername=""  TransferPassword=""  TransferSrvHostname=“192.168.3.4"
```

Configuration of a User Password

If you are using the CLI, the new password will be used the next time you connect to the Aastra.

```
Aaa.Users[UserName=public].Password=TestPwd
```

Debugging

The following sections allow you to enable two useful debugging tools of the Aastra: syslog messages and PCM traces.

Enabling Syslog

This example assumes that you run a syslog server at address 192.168.3.4.

```
Nlm.SyslogRemoteHost="192.168.3.4"
Cli.MinSeverity=300
Bni.MinSeverity=400
Hoc.MinSeverity=500
```

Configuring PCM Capture

The PCM traces are two different RTP streams made specifically to record all analog signals that are either sent or received on the analog side of the Aastra. Only the configured port, port #1 and/or #2 are sending the PCM traces for a maximum of four simultaneous RTP streams.

The RTP streams are sent to a configurable IP address, normally an IP address on your network where it can be recorded with a packet sniffer (such as Wireshark). Moreover, they are independent from the regular RTP streams of the VoIP call.

All streams are sent instantly at startup with an average ptime of 15 ms. This means that until the PCM traces are disabled, even an idle unit will continuously send up to 66.6 packets/s X 4 streams = 267 packets/s using approximately 174 bytes each, for a total of 46 Kbytes of upstream bandwidth.

```
Mipt.PcmCaptureEnable=1
Mipt.PcmCaptureEndpoint="Bri1-1"
Mipt.PcmCaptureIpAddr="192.168.3.3"
Mipt.restart
```

APPENDIX
C

Maximum Transmission Unit (MTU)

This appendix describes the MTU (Maximum Transmission Unit) requirements of the Aastra.

What is MTU?

The *Maximum Transmission Unit* (MTU) is a parameter that determines the largest packet than can be transmitted by an IP interface (without it needing to be broken down into smaller units). Each interface used by TCP/IP may have a different MTU value specified.

The MTU should be larger than or equal to the largest packet you wish to transmit unfragmented. Note that this only prevents fragmentation locally. Some other link in the path may have a smaller MTU: the packet will be fragmented at that point, although some routers may refuse packets larger than their MTU.

Aastra's MTU

The Aastra's MTU is 1500 bytes, which is the Ethernet typical value.

Possible Hardware Problem

The implementation of the IEEE Standard 802.1q in the Aastra may have a minor problem because of hardware limitations.

802.1q increases the Ethernet frame header by 4 bytes, adding a Virtual LAN ID and a user_priority. This is useful to limit broadcasts that cross bridges, and it may also prioritize frames in the queuing algorithm of switches. However, it also increases the maximum possible size of Ethernet frames from 1518 to 1522 bytes, and this might not be handled adequately by every hardware.

A workaround is available for PCs running Windows to avoid sending 1522 bytes packets (note that this happens only in special and rare cases). The workaround is to reduce the MTU of the interface (the one that sends packets with 802.1q framing) by 4 bytes.

1. Use the registry editor (regedt32) and go to the key:

   Windows 2000 and later:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\<ethernet adapter>`

   Windows NT4 and 98:

   `\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<ethernet adapter>\Parameters\Tcpip`

   where <Ethernet adapter> can be found by using the command "ipconfig /all".

2. Add (or modify) a value named MTU of type REG_DWORD. Set it to 1496 (instead of 1500), in decimal. Restart the computer to have those changes in effect.

   In Windows 2000 and later this value is under the following key:

   - Key: *Tcpip\Parameters\Interfaces\ID* for Adapter2

- Value Type: REG_DWORD Number
- Valid Range: 68 - the MTU of the underlying network
- Default: 0xFFFFFFFF
- Description: This parameter overrides the default MTU for a network interface. The MTU is the maximum packet size in bytes that the transport will transmit over the underlying network. The size includes the transport header. Note that an IP datagram may span multiple packets. Values larger than the default for the underlying network will result in the transport using the network default MTU. Values smaller than 68 will result in the transport using an MTU of 68.

3. To validate that the changes are correct, try to ping the Aastra with large packets once restarted:
`ping -l 2000`

This will cause IP fragmentation, the first fragment being as large as the interface allows it. With the MTU reduced, you should now receive an answer. For more informations, see:

http://support.microsoft.com/default.aspx?scid=kb;en-us;120642.

APPENDIX

D

Web Interface – SNMP Variables Mapping

All parameters available in the Aastra web interface may also be configured via SNMP. The Aastra SNMP feature offers the following options:

- Password-protected access
- Remote management
- Simultaneous management

This Appendix lists the mapping between the web interface fields and the corresponding SNMP variables of the Aastra.

System Page

Information Sub-Page

Current Status Section

Field Name	SNMP Variable	Description
System Description	unitInfoProductName	Product name of the unit.
Firmware	mfpInstalledInfoMfpVersion	Version of the Firmware Pack installed.
Profile	mfpInstalledInfoMfpProfileName	Name of the profile.
MAC Address	unitInfoMacAddress	MAC address of the unit.
Serial Number	unitInfoSerialNumber	Serial number of the unit.
System Uptime	sysUpTime	Time since the last restart.
System Time	currentTimeSystem	Current date and time system configured in the unit.

Services Sub-Page

System Service

Field Name	SNMP Variable	Description
System Service	servicesInfoName	Current service name.
Status	servicesInfoExecState	Shows the execution state of the service.

User Service

Field Name	SNMP Variable	Description
User Service	servicesInfoName	Current service name.
Status	servicesInfoExecState	Shows the execution state of the service.
Startup Type	servicesInfoStartupType	Selects the service startup type.
Action	serviceCommandsRestart	Restarts, starts or stops the service.

Field Name	SNMP Variable	Description
Comment	servicesInfoComment	Comments on the service's current state.
	Start (command)	Starts the service.
	Stop (command)	Stops the service.
	Restart (command)	Restarts the service.

Restart Required Services

Field Name	SNMP Variable	Description
Graceful Delay (min)	graceDelay	The delay (in minutes) allowed for telephony calls to be all completed.
Cancel	CancelRestartRequiredServices (command)	Cancels the restart during the grace delay period.
	RestartRequiredServices (command)	Restarts all required services

Hardware Sub-Page

Unit Configuration Section

Field Name	SNMP Variable	Description
Unit Configuration	portsConfiguration	Configures how each port provides a link interface.
Clock Reference	physicalLinkClockMode	A port can either generate the clocking for the line or accept the clock from the line.

BRI Cards Configuration Section

Field Name	SNMP Variable	Description
Slot	physicalLinkInterfaceName	Identifies the interface.
Clock Reference	physicalLinkClockMode	A port can either generate the clocking for the line or accept the clock from the line.

PRI Cards Configuration Section

Field Name	SNMP Variable	Description
Slot	physicalLinkInterfaceName	Identifies the interface.
Clock Reference	physicalLinkClockMode	Indicates the preferred synchronisation source to use for the internal clock of this digital card.
Line Type	physicalLinkLineCoding	Defines the transmission encoding of bits.

Endpoints Sub-Page

Unit States Section

Field Name	SNMP Variable	Description
Administrative	unitAdminState	Indicates the current maintenance state of a unit.
Operational	unitOpState	The operational state of the unit reflects the unit's internal state.

Field Name	SNMP Variable	Description
Usage	unitUsageState	The usage state of the unit indicates its running state.
Action	unitUnlock unitLock unitForceLock	Allows to use a unit. Gracefully disallows to use a unit. Forcefully disallows to use a unit.

Endpoint States Section

Field Name	SNMP Variable	Description
Endpoint	endpointEpId	String that identifies an endpoint in other tables.
Administrative	endpointAdminState	Administrative state of an endpoint.
Operational	endpointOpState	Operational state of an endpoint.
Usage	endpointUsageState	Ru7ning state of an endpoint.
Initial Administrative	endpointInitialAdminStateConfig	Initial administrative state of an endpoint.
Action	endpointUnlock endpointLock endpointForceLock	Allows using the endpoint. Gracefully disallows using the endpoint. Forcefully disallows using the endpoint.

Administration Section

Field Name	SNMP Variable	Description
Disable Unit When No Gateways Are In State Ready	unitDisabledWhenNoGatewayReadyEnable	Indicates if the unit operational state is automatically set to disable when all signaling gateways are not ready.
Shutdown Endpoint When Operational State is 'Disable' And Its Usage State Is 'idle-unusable'	endpointAutomaticShutdownEnable	Indicates if an endpoint is physically shutdown when in the 'idle-unusable' usage state.

Syslog Sub-Page

Field Name	SNMP Variable	Description
Remote Host	syslogRemoteHost	Host name and port number of the device that archives log entries.
Authentication, Authorization and Accounting (AAA)	minSeverity (aaaMIB)	Minimal Severity of Notification
Basic Network Interface (BNI)	minSeverity (bniMIB)	Minimal Severity of Notification
Call Routing (CROUT)	minSeverity (cRoutMIB)	Minimal Severity of Notification
Certificate Manager (CERT)	minSeverity (certMIB)	Minimal Severity of Notification
Command Line Interface (CLI)	minSeverity (cliMIB)	Minimal Severity of Notification
Configuration Manager (CONF)	minSeverity (confMIB)	Minimal Severity of Notification
Device Control Manager (DCM)	minSeverity (dcmMIB)	Minimal Severity of Notification
DHCP (DHCP)	minSeverity (dhcpMIB)	Minimal Severity of Notification
Endpoint Administration (EpAdm)	minSeverity (epAdmMIB)	Minimal Severity of Notification

Field Name	SNMP Variable	Description
Endpoint Services (EpServ)	minSeverity (epServMIB)	Minimal Severity of Notification
Ethernet manager (Eth)	minSeverity (ethMIB)	Minimal Severity of Notification
Firmware Pack Updater (FPU)	minSeverity (fpuMIB)	Minimal Severity of Notification
Host Configuration (HOC)	minSeverity (hocMIB)	Minimal Severity of Notification
Integrated Services Digital Network (ISDN)	minSeverity (isdnMIB)	Minimal Severity of Notification
Local Quality Of Service (LQOS)	minSeverity (lQosMIB)	Minimal Severity of Notification
Media IP Transport (MIPT)	minSeverity (miptMIB)	Minimal Severity of Notification
Notifications and Logging Manager (NLM)	minSeverity (nlmMIB)	Minimal Severity of Notification
Plain Old Telephony System Lines service (POTS)	minSeverity (potsMIB)	Minimal Severity of Notification
Process Control Manager (PCM)	minSeverity (pcmMIB)	Minimal Severity of Notification
Service Controller Manager (SCM)	minSeverity (scmMIB)	Minimal Severity of Notification
SIP ALG (SipAlg)	minSeverity (sipAlgMIB)	Minimal Severity of Notification
SIP Endpoint (SipEp)	minSeverity (sipEpMIB)	Minimal Severity of Notification
Diagnostic Traces	diagnosticTracesEnable	Enables traces allowing the Technical Assistance Centre to further assist in resolving some issues.
Filter	diagnosticTracesFilter	Filter applied to diagnostic traces.

Events Sub-Page

Field Name	SNMP Variable	Description
Activation	eventsActivation	Current activation state for this system event.
Criteria	eventsCriteria	Expression an event must match in order to apply the specified action.
Service	N/A	N/A
Notification	N/A	N/A
Action	eventsAction	Action to apply to the system event if the criteria matches.
Config Status	eventsConfigStatus	Configuration status of the row.
	InsertEvent (command)	Inserts a row to the EventsTable
	eventsDelete	Deletes this row.

Local Log Sub-Page

Local Log Status Section

Field Name	SNMP Variable	Description
Maximum Number of Entries	LocalLogMaxNbEntries	Maximum number of entries that the local log can contain. When adding a new entry while the local log is full, the oldest entry is erased to make room for the new one.

Field Name	SNMP Variable	Description
Number of Error Entries	LocalLogNbErrorEntries	Current number of error entries in the local log.
Number of Critical Entries	LocalLogNbCriticalEntries	Current number of critical entries in the local log.

Local Log Entries Section

Field Name	SNMP Variable	Description
Local Time	LocalTime	Local date and time at which the log entry was inserted. Format is YYYY-MM-DD HH:MM:SS.
Severity	Severity	Severity of the log entry.
Service Name	ServiceTextkey	Textual identifier of the service that issued the log entry.
Service Key	ServiceNumkey	Numerical identifier of the service that issued the log entry.
Message Key	NotificationId	Numerical identifier of the notification message.
Message Content	Message	The readable content of the log message.

Network Page

Status Sub-Page

Interfaces Status Section

Field Name	SNMP Variable	Description
Interface	networkInterfaceStatusInterfaceName	Network interface name.
Link	networkInterfaceStatusLinkName	Name of the link interface associated with the network interface.
IP Address	networkInterfacesStatusIpAddr	Current address and network mask of the network interface.
Default Router	networkInterfacesDefaultRouter	Current default gateway of the network interface.
Connection Uptime	networkInterfacesConnectionUptime	The time, in seconds, for which this IP interface has been connected.
Status	uplinkInterfaceStatus	Operational status of the *Uplink* network interface.
VLAN Override	netorknterfacesStatusVlanOverrideEnable	Indicates if the VLAN ID of the current network interface has been overridden by the values received from the LLDP protocol.

LLDP Status Section

Field Name	SNMP Variable	Description
Type	remoteMediaPolicyStateAppType	The type of application.
Vlan ID	remoteMediaPolicyStateVlanId	VLAN ID.
User Priority (802.1Q)	remoteMediaPolicyStatePriority	802.1Q User Priority.
DiffServ (DSCP)	remoteMediaPolicyStateDscp	DSCP (DiffServ).
Policy Flag	remoteMediaPolicyStatePolicyFlag	Indicates if an Endpoint Device wants to explicitly advertise that the network policy for a specific application type is required but is currently unknown.
Tagged Flag	remoteMediaPolicyStateTaggedFlag	The Tagged flag.

Host Status Section

Field Name	SNMP Variable	Description
General Configuration		
Automatic Configuration Interface	subnetsAutomaticConfigurationInterface	The network interface that provides the automatic configuration (E.g.: DNS servers, NTP server, etc.) to this subnet.
Host Name Configuration		
Host Name	domainNamesInfoSubnetName	Name of the subnet.
Domain Name	domainNamesInfoDomainName	Indicates the subnet's current domain name.
Default Gateway Configuration		
IPv4 Default Gateway	defaultRoutersInfoDefaultRouter	Indicates the subnet's current default gateway.
IPv6 Default Gateway	defaultRoutersInfoDefaultRouter	Indicates the subnet's current default gateway.
DNS Configuration		
Primary DNS	dnsServersInfoIpAddress1	Indicates the subnets' first DNS server.
Secondary DNS	dnsServersInfoIpAddress2	Indicates the subnets' secondary DNS server.
Third DNS	dnsServersInfoIpAddress3	Indicates the subnets' third DNS server.
Fourth DNS	dnsServersInfoIpAddress4	Indicates the subnets' fourth DNS server.
SNTP Configuration		
Primary SNTP Host	sntpServersInfoHostName1	Indicates the subnets' first NTP server.
Secondary SNTP Host	sntpServersInfoHostName2	Indicates the subnets' second NTP server.
Third SNTP Host	sntpServersInfoHostName3	Indicates the subnets' third NTP server.
Fourth SNTP Host	sntpServersInfoHostName4	Indicates the subnets' fourth NTP server.

Advanced IP Routes Section

Field Name	SNMP Variable	Description
#	advancedIpRoutesStatusIPriority	Unique identifier of the row in the table.
Source Address	advancedIpRoutesStatusSourceAddress	Source address[/mask] criteria used to match the rule.
Source Link	advancedIpRoutesStatusSourceLink	Source link criteria used to match the rule.
Forward To Network	advancedIpRoutesStatusForwardToNetwork	Network on which the packet is forwarded.
State	advancedIpRoutesStatusStatus	Status of the rule.

IPv4 Routes Section

Field Name	SNMP Variable	Description
Link	ipRoutesStatus	Link (interface) ID.
Destination	ipRoutesStatus	Destination IP address or network address.
Gateway	ipRoutesStatus	Specifies the gateway IP address.
Protocol	ipRoutesStatus	Identifies the entity that installed the route.

Firewall Section

Field Name	SNMP Variable	Description
#	networkRulesStatusPriority	Unique identifier of the row in the table.
Source Address	networkRulesStatusSourceAddress	Source address[/mask] criteria an incoming packet must have to match this rule.

Field Name	SNMP Variable	Description
Source Port	networkRulesStatusSourcePort	Source port[-port] criteria an incoming packet must have to match this rule.
Destination Address	networkRulesStatusDestinationAddress	Destination address[/mask] criteria an incoming packet must have to match this rule.
Destination Port	networkRulesStatusDestinationPort	Destination port[-port] criteria an incoming packet must have to match this rule.
Protocol	networkRulesStatusProtocol	Protocol criteria an incoming packet must have to match this rule.
Connection State	networkRulesStatusConnectionState	Connection state associated with the incoming packet.
Action	networkRulesStatusAction	Action taken when this rule matches a packet.

Network Address Translation Section

Field Name	SNMP Variable	Description
#	sNatRulesStatusPriority dNatRulesStatusPriority	Unique identifier of the row in the table.
Source Address	sNatRulesStatusSourceAddress dNatRulesStatusSourceAddress	Source address[/mask] criteria an incoming packet must have to match this rule.
Source Port	sNatRulesStatusSourcePort dNatRulesStatusSourcePort	Source port[-port] criteria an incoming packet must have to match this rule.
Destination Address	sNatRulesStatusDestinationAddress dNatRulesStatusDestinationAddress	Destination address[/mask] criteria an incoming packet must have to match this rule.
Destination Port	sNatRulesStatusDestinationPort dNatRulesStatusDestinationPort	Destination port[-port] criteria an incoming packet must have to match this rule.
Protocol	sNatRulesStatusProtocol dNatRulesStatusProtocol	Protocol criteria an incoming packet must have to match this rule.
New Address	sNatRulesStatusNewAddress dNatRulesStatusNewAddress	New address[:port] applied to the source of the packet.

Host Sub-Page

General Configuration Section

Field Name	SNMP Variable	Description
Automatic Configuration Interface	automaticConfigurationInterface	The network interface that provides the automatic configuration used by the unit (e.g.: Default gateway, DNS servers, NTP server, etc.).
Automatic IPv4 config source network:	automaticConfigurationInterface	The network interface that provides the automatic configuration used by the unit (e.g.: Default gateway, DNS servers, NTP server, etc.).
Automatic IPv6 config source network	ipv6AutomaticConfigurationInterface	The network interface that provides the IPv6 automatic configuration (Default Router, domain name, DNS servers and NTP server) used by the unit.

Host Name Configuration Section

Field Name	SNMP Variable	Description
Domain Name Configuration Source	domainNameConfigSource	Configuration source for the domain name.
Domain Name	staticDomainName	Static domain name.
Host Name	hostName	System’s host name.

Default Gateway Configuration Section

Field Name	SNMP Variable	Description
IPv4		
Configuration Source	defaultRouterConfigSource	Configuration source for the default gateway.
Default Gateway	staticDefaultRouter	Static default gateway address.
IPv6		
Configuration Source	defaultRouterConfigSource	Configuration source for the default gateway.
Default Gateway	staticDefaultRouter	Static default gateway address.

DNS Configuration Section

Field Name	SNMP Variable	Description
Configuration Source	dnsServersConfigSource	Configuration source for the DNS servers.
Primary DNS	staticDnsServersIpAddress1	Indicates the subnets' first DNS server.
Secondary DNS	staticDnsServersIpAddress2	Indicates the subnets' secondary DNS server.
Third DNS	staticDnsServersIpAddress3	Indicates the subnets' third DNS server.
Fourth DNS	staticDnsServersIpAddress4	Indicates the subnets' fourth DNS server.

SNTP Configuration Section

Field Name	SNMP Variable	Description
Configuration Source	sntpConfigSource	Configuration source for the SNTP parameters.
Primary SNTP	staticSntpServersHostName1	Indicates the subnets' first NTP server.
Secondary SNTP	staticSntpServersHostName2	Indicates the subnets' second NTP server.
Third SNTP	staticSntpServersHostName3	Indicates the subnets' third NTP server.
Fourth SNTP	staticSntpServersHostName4	Indicates the subnets' fourth NTP server.
Synchronization Period	sntpSynchronizationPeriod	Time interval between system time synchronization cycles.
Synchronization Period On Error	sntpSynchronizationPeriodOnError	Time interval between retries after an unsuccessful request to the SNTP server.

Time Configuration Section

Field Name	SNMP Variable	Description
Static Time Zone	staticTimeZone	Specifies the time zone in which the system is located.

Interfaces Sub-Page

Interface Configuration Section

Field Name	SNMP Variable	Description
Interface	networkInterfacesInterfaceName	Network interface name.
Link	networkInterfacesLinkName	Name of the link interface associated with the network interface.
Type	networkInterfacesConnectionType	Connection type of the network interface.
Static IP Address	networkInterfacesStaticIpAddr	IPv4 address and network mask of the network interface.

Field Name	SNMP Variable	Description
Static Default Router	networkInterfacesStaticDefaultRouter	IPv4 address of the default gateway for the network interface when the ConnectionType is set to ipStatic.
Activation	networkInterfacesActivation	Attempts to activate the network interface.
+	AddNetwork (command)	Adds a new network interface.
−	networkInterfacesDelete	Deletes the network interface and removes it from the system.

PPPoE Configuration Section

Field Name	SNMP Variable	Description
Service Name	pppServiceName	Name of the service requested to the access concentrator when establishing the next PPPoE connection.
Protocol	pppAuthenticationProtocol	Authentication protocol to use for authenticating the system to the PPP peer.
User Name	pppIdentity	Name that identifies the system to the PPP peer during the authentication process.
Password	pppSecret	Secret that identifies the system to the PPP peer during the authentication process.

LLDP Configuration Section

Field Name	SNMP Variable	Description
Network Interface	NetworkInterface	The network interface name on which LLDP should be enabled.
Chassis ID	ChassisId	The address type to populate the chassis ID.
Override Network Policy	OverrideNetworkPolicyEnable	Enables the LLDP-MED protocol override of the VLAN ID, User Priority and DiffServ values.

Ethernet Link Configuration Section

Field Name	SNMP Variable	Description
Link	linksName	The name of the Ethernet link.
MTU	linksMtu	Configures the MTU (Maximum Transmission Unit) of a specific Ethernet link.
802.1x Authentication	linksIeee8021XAuthentication	Configures the IEEE 802.1x authentication protocol activation on the Ethernet link interface.
EAP Username	eapUserName	Username used to authenticate each Ethernet link interfaces during the IEEE 802.1x EAP-TLS authentication process.
Certificate Validation	eapCertificationValidation	Level of validation used by the device to authenticate the IEEE 802.1x EAP-TLS peer's certificate. This variable controls also the criteria used to select the host certificate sent during the authentitication handshake

VLAN Sub-Page

Field Name	SNMP Variable	Description
Link	vlanLinkName	Name of the Ethernet link over which the VLAN interface is built.
Id	vlanId	VLAN ID used by the VLAN interface.
Default User Priority	vlanDefaultUserPriority	Default User Priority value the interface uses when tagging packets.

Field Name	SNMP Variable	Description
	AddVlan (command)	Adds a new virtual LAN.
	vlanDelete	Deletes the VLAN interface and removes it from the system.

Local Firewall Sub-Page

Field Name	SNMP Variable	Description
Config Modified	configModifiedStatus	Shows whether the configuration of the local firewall was modified without being applied.

Local Firewall Configuration Section

Field Name	SNMP Variable	Description
Default Policy	defaultPolicy	Action taken when a packet doesn't match any rules.

Local Firewall Rules Section

Field Name	SNMP Variable	Description
#	localRulesPriority	Unique identifier of the row in the table.
Activation	localRulesActivation	Current state for this rule.
Source Address	localRulesSourceAddress	Source address of the incoming packet.
Source Port	localRulesSourcePort	Source port of the incoming packet.
Destination Address	localRulesDestinationAddress	Destination address of the incoming packet.
Destination Port	localRulesDestinationPort	Destination port of the incoming packet.
Protocol	localRulesProtocol	Protocol of the incoming packet.
Action	localRulesAction	Action that will be taken in the matching packets.
	localRulesInsert	Inserts a new row before this row.
	localRulesDelete	Deletes this row.
	localRulesDown	Moves the current row downside.
	localRulesUp	Moves the current row upside.

IP Routing Sub-Page

Field Name	SNMP Variable	Description
Config Modified	configModifiedStatus	Shows whether or not the Network Address Translation configuration has been modified without being applied.
Rollback	Rollback (command)	Rolls back the current configuration to the running configuration as showed in the status.

IP Routing Configuration Section

Field Name	SNMP Variable	Description
IPv4 Forwarding	ipv4ForwardingEnable	Enables/disables IPv4 forwarding.

Advanced IP Routes Section

Field Name	SNMP Variable	Description
#	advancedIpRoutesPriority	Unique identifier of the row in the table.
Activation	advancedIpRoutesActivation	Activates this route.
Source Address	advancedIpRoutesSourceAddress	Specifies the source IP address criteria an incoming packet must have to match this rule.
Source Link	advancedIpRoutesSourceLink	Specifies the source link criteria an incoming packet must have to match this rule.
Forward to Network	advancedIpRoutesForwardToNetwork	Network on which to route the packet.
	advancedIpRoutesInsert	Inserts a new row before this row.
	advancedIpRoutesDelete	Deletes this row.
	advancedIpRoutesDown	Moves the current row downside.
	advancedIpRoutesUp	Moves the current row upside.

Static IP Routes Section

Field Name	SNMP Variable	Description
Index	staticIpRoutesIndex	Unique identifier of the row in the table.
Destination	staticIpRoutesDestination	Specifies the destination IP address criteria that an outgoing packet must have to match this route.
Link	staticIpRoutesLink	Output link (interface) name.
Gateway	staticIpRoutesGateway	Specifies the IP address of the gateway used by the route.
	insertStaticIpRoute (command)	Inserts a new row at the end of the StaticIpRoutes table.
	staticIpRoutesDelete	Deletes this row.

Network Firewall Sub-Page

Field Name	SNMP Variable	Description
Config Modified	configModifiedStatus	Shows whether the configuration of the network firewall was modified without being applied.
Rollback	Rollback (command)	Rolls back the current configuration to the running configuration as showed in the status.

Network Firewall Configuration Section

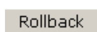
Field Name	SNMP Variable	Description
Default Policy	defaultPolicy	Action taken when a packet does not match any rules.

Network Firewall Rules Section

Field Name	SNMP Variable	Description
#	networkRulesPriority	Unique identifier of the row in the table.
Activation	networkRulesActivation	Activates this rule.
Source Address	networkRulesSourceAddress	Source address of the incoming packet.
Source Port	networkRulesSourcePort	Source port of the incoming packet.

Field Name	SNMP Variable	Description
Destination Address	networkRulesDestinationAddress	Destination address of the incoming packet.
Destination Port	networkRulesDestinationPort	Destination port of the incoming packet.
Protocol	networkRulesProtocol	Protocol of the incoming packet.
Connection State	networkRulesConnectionState	Connection state associated with the incoming packet.
Action	networkRulesAction	Action that will be taken in the matching packets.
	networkRulesInsert	Inserts a new row before this row.
	networkRulesDelete	Deletes this row.
	networkRulesDown	Moves the current row downside.
	networkRulesUp	Moves the current row upside.

NAT Sub-Page

Field Name	SNMP Variable	Description
Config Modified	configModifiedStatus	Shows whether or not the Network Address Translation configuration has been modified without being applied.
	Rollback (command)	Rolls back the current configuration to the running configuration as showed in the status.

Source Network Address Translation Rules Section

Field Name	SNMP Variable	Description
#	sNatRulesPriority	Unique identifier of the row in the table.
Activation	sNatRulesActivation	Activates this rule.
Source Address	sNatRulesSourceAddress	Source address of the incoming packet.
Source Port	sNatRulesSourcePort	Source port of the incoming packet.
Destination Address	sNatRulesDestinationAddress	Destination address of the incoming packet.
Destination Port	sNatRulesDestinationPort	Destination port of the incoming packet.
Protocol	sNatRulesProtocol	Protocol of the incoming packet.
New Address	sNatRulesNewAddress	New address applied to the destination of the packet.
	sNatRulesInsert	Inserts a new row before this row.
	sNatRulesDelete	Deletes this row.
	sNatRulesDown	Moves the current row downside.
	sNatRulesUp	Moves the current row upside.

Destination Network Address Translation Rules Section

Field Name	SNMP Variable	Description
#	dNatRulesPriority	Unique identifier of the row in the table.
Activation	dNatRulesActivation	Activates this rule.
Source Address	dNatRulesSourceAddress	Source address of the incoming packet.
Source Port	dNatRulesSourcePort	Source port of the incoming packet.
Destination Address	dNatRulesDestinationAddress	Destination address of the incoming packet.

Field Name	SNMP Variable	Description
Destination Port	dNatRulesDestinationPort	Destination port of the incoming packet.
Protocol	dNatRulesProtocol	Protocol of the incoming packet.
New Address	dNatRulesNewAddress	New address applyed to the destination of the packet.
+	dNatRulesInsert	Inserts a new row before this row.
−	dNatRulesDelete	Deletes this row.
v	dNatRulesDown	Moves the current row downside.
^	dNatRulesUp	Moves the current row upside.

DHCP Server Sub-Page

DHCP Server Status Section

Field Name	SNMP Variable	Description
Subnet Status	subnetsConfigStatus	Subnet configuration status.
Lease Time (Option 51)		
Lease Time	leaseTimesInfoDefault	Indicates the subnet's current default lease time in seconds.
Default Gateway (Option 3)		
Default Gateway	defaultRoutersInfoDefaultRouter	Indicates the subnet's current default gateway.
DNS (Option 6)		
Primary DNS	dnsServersInfoDns1	Indicates the subnets' first DNS server.
Secondary DNS:	dnsServersInfoDns2	Indicates the subnets' secondary DNS server.
Third DNS	dnsServersInfoDns3	Indicates the subnets' third DNS server.
Fourth DNS	dnsServersInfoDns4	Indicates the subnets' fourth DNS server.
NTP (Option 42)		
Primary SNTP Host	ntpServersInfoNtp1	Indicates the subnets' first NTP server.
Secondary SNTP Host	ntpServersInfoNtp2	Indicates the subnets' second NTP server.
Third SNTP Host	ntpServersInfoNtp3	Indicates the subnets' third NTP server.
Fourth SNTP Host	ntpServersInfoNtp4	Indicates the subnets' fourth NTP server.

DHCP Server Leases Section

Field Name	SNMP Variable	Description
MAC Address	assignedLeasesInfoMacAddress	MAC address of the host.
IP Address	assignedLeasesInfoIpAddress	IP Address of the host.
Subnet Name	assignedLeasesInfoSubnetName	Indicates on which subnet the host is located.
Time Left	assignedLeasesInfoLeaseTimeLeft	Indicates the lease time left in seconds.

DHCP Server Configuration Section

Field Name	SNMP Variable	Description
DHCP Server Enable	subnetsEnableSubnet	Enables the subnet configuration.
Start IP Address	subnetsStartAddress	Start address of the subnet range.

Field Name	SNMP Variable	Description
End IP Address	subnetsEndAddress	End address of the subnet range.
Automatic Configuration Interface	subnetsAutomaticConfigurationInterface	Interface that will provide the automatic configuration to this subnet.
Lease Time (Option 51)		
Subnet Specific	specificLeaseTimesEnableConfig	Defines the lease time configuration to use for a specific subnet.
Lease Time	defaultLeaseTime specificLeaseTimesLeaseTime	Specifies the lease time (in seconds) default setting for all subnets. Specifies the subnet's specific lease time in seconds.
Domain Name (Option 15)		
Enable Option	specificDomainNamesEnableOption	Enables the domain name option.
Subnet Specific	specificDomainNamesEnableConfig	Defines the domain name configuration to use for this specific subnet.
Configuration Source	defaultDomainNameConfigSource specificDomainNamesConfigSource	Default configuration source of all subnets. Subnet's domain name specific configuration source.
Domain Name	defaultStaticDomainName specificDomainNamesStaticName	Default static domain name for all subnets. Static Domain Name Configuration.
Default Gateway (Option 3)		
Enable Option	specificDefaultRoutersEnableOption	Enables the default gateway option.
Configuration Source	specificDefaultRoutersConfigSource	The subnet's specific router configuration source.
Default Gateway	specificDefaultRoutersStaticRouter	Specifies the subnet's default gateway.
DNS (Option 6)		
Enable Option	specificDnsServersEnableOption	Enables the DNS servers option.
Subnet Specific	specificDnsServersEnableConfig	Defines the DNS servers configuration to use for a specific subnet.
Configuration Source	defaultDnsServersConfigSource specificDnsServersConfigSource	Default configuration source for the DNS servers of all subnets. DNS servers specific configuration source for the subnet.
Primary DNS	specificDnsServersStaticDns1	IP address of the first DNS server of the subnet.
Secondary DNS:	specificDnsServersStaticDns2	IP address of the second DNS server of the subnet.
Third DNS	specificDnsServersStaticDns3	IP address of the third DNS server of the subnet
Fourth DNS	specificDnsServersStaticDns4	IP address of the fourth DNS server of the subnet.
NTP (Option 42)		
Enable Option	specificNtpServersEnableOption	Enables the NTP servers option.
Subnet Specific	specificNtpServersEnableConfig	Defines the NTP servers configuration to use for a specific subnet.
Configuration Source	defaultNtpServersConfigSource specificNtpServersConfigSource	Default configuration source for the NTP servers of all subnets. NTP servers specific configuration source for the subnet.
Primary NTP	specificNtpServersStaticNtp1	IP address of the first NTP server of the subnet.
Secondary NTP	specificNtpServersStaticNtp2	IP address of the second NTP server of the subnet.
Third NTP	specificNtpServersStaticNtp3	IP address of the third NTP server of the subnet.
Fourth NTP	specificNtpServersStaticNtp4	IP address of the fourth NTP server of the subnet.
NBNS (Option 44)		
Enable Option	specificNbnsServersEnableOption	Enable NBNS servers option.
Subnet Specific	specificNbnsServersEnableConfig	Defines the NBNS servers configuration to use for a specific subnet.
Primary NBNS	specificNbnsServersStaticNbns1	IP address of the first NBNS server of the subnet.
Secondary NBNS	specificNbnsServersStaticNbns2	IP address of the second NBNS server of the subnet.

Field Name	SNMP Variable	Description
Third NBNS	specificNbnsServersStaticNbns3	IP address of the third NBNS server of the subnet.
Fourth NBNS	specificNbnsServersStaticNbns4	IP address of the fourth NBNS server of the subnet.

QoS Sub-Page

Differentiated Service Field Configuration Section

Field Name	SNMP Variable	Description
Default DiffServ (IPv4)	defaultDiffServ	Default Differentiated Services value used by the unit for all generated packets.
Default Traffic Class (IPv6)	defaultTrafficClass	Default Traffic Class value used by the unit for all generated IPv6 packets.

Ethernet 802.1Q Tagging Configuration Section

Field Name	SNMP Variable	Description
Enable	ethernet8021QTaggingEnablePriorityTagging	Enables or disables user priority tagging on the interface.
Default User Priority	ethernet8021QTaggingDefaultUserPriority	Default User Priority value the interface uses when tagging packets.

Service Class Configuration Section

Field Name	SNMP Variable	Description
DiffServ (IPv4)	serviceClassesDiffServ	Differentiated Services value for a specific service class.
Traffic Class (IPv6)	serviceClassesTrafficClass	Default Traffic Class value used in IPv6 packets.
User Priority	servicesClassesUserPriority	User priority for a specific service class.

Network Traffic Control Configuration Section

Field Name	SNMP Variable	Description
Physical Link	linkBandwidthControlLinkName	Name of the Ethernet link over which the bandwidth limitation is applied.
Egress Limit	linkBandwidthControlEgressLimit	Indicates the bandwidth limitation for the selected link interface.

POTS Page

Status Sub-Page

Line Status Section

Field Name	SNMP Variable	Description
ID	lineId	String that identifies a line in other tables.
Type	lineTypeStatus	The status POTS type of the line.
State	lineState	The current call control state for this channel.

Config Sub-Page

General Configuration Section

Field Name	SNMP Variable	Description
Caller ID Customization	CallerIdCustomization	Allows selecting the detection/generation method of caller ID.
Caller ID Transmission	CallerIdTransmission	Allows selecting the transmission type of the caller ID.
Vocal Unit Information	VocalUnitInformation	Determines whether or not the unit's IP or MAC address or firmware version number can be acquired using the *#*0, *#*1, and *#*8 digit maps respectively.

FXS Config Sub-Page

FXS Configuration Section

Field Name	SNMP Variable	Description
Line Supervision Mode	fxsLineSupervisionMode	Determines how the power drop and line polarity are used to signal the state of a line.
Disconnect Delay	fxsDisconnectDelay	Determines whether or not call clearing occurs as soon as the called user is the first to hang up a received call.
Auto Cancel Timeout	fxsDefaultAutoCancelTimeout	Time, in seconds, the endpoint rings before the call is automatically cancelled.
Inband Ringback	fxsInbandRingback	Determines whether or not the FXS endpoint needs to generate a ringback for incoming ringing call.
Shutdown Behavior	fxsShutdownBehavior	Determines the FXS endpoint behavior when it becomes shut down.
Power Drop on Disconnect Duration	fxsPowerDropOnDisconnectDuration	Determines the power drop duration that is made at the end of a call when the call is disconnected by the remote party.
Service Activation	FxsServiceActivation	Selects the method used by the user to activate supplementary services like call hold, second call, call waiting, call transfer and conference call.

FXS Country Configuration Section

Field Name	SNMP Variable	Description
Override Country Customization	fxsCountryCustomizationOverride	Allows overriding FXS-related default country settings.
Country Override Loop Current	fxsCountryCustomizationLoopCurrent	Loop current generated by the FXS port in ma.
Country Override Flash Hook Detection Range	fxsCountryCustomizationFlashHookDetectionRange	The range in which the hook switch must remain pressed to perform a flash hook.

FXS Bypass Section

Field Name	SNMP Variable	Description
Endpoint	fxsBypassId	String that identifies a line in other tables.
Activation	fxsBypassActivation	Specifies when the bypass needs to be activated.
Activation DTMF Map	fxsBypassActivationDtmfMap	Specifies the DTMFs to signal to enable the bypass.
Deactivation Timeout	fxsBypassDeactivationTimeout	Specifies the delay to wait before deactivating the bypass after an on hook if the bypass is activated on demand.

SIP Page

Gateways Sub-Page

SIP Gateway Status Section

Field Name	SNMP Variable	Description
Name	gatewayStatusName	Name of the SIP gateway.
Network Interface	gatewayStatusNetworkInterface	Network on which the gateway listens for incoming SIP traffic.
Port	gatewayStatusPort	Port on which the gateway listens for incoming unsecure SIP traffic.
Secure Port	gatewayStatusSecurePort	Port on which the gateway listens for incoming secure SIP traffic.
State	gatewayStatusState	Current state of the gateway.

SIP Gateway Configuration Section

Field Name	SNMP Variable	Description
Name	gatewayName	Name of the SIP gateway. It identifies the gateway in other tables.
Network Interface	gatewayNetworkInterface	Network on which the gateway listens for incoming SIP traffic.
Port	gatewayPort	Port on which the gateway listens for incoming unsecure SIP traffic.
Secure Port	gatewayStatusSecurePort	Port on which the gateway listens for incoming secure SIP traffic.
	InsertGateway (command)	Adds a row.
	gatewayDelete	Deletes this row.

Servers Sub-Page

Field Name	SNMP Variable	Description
Submit & Refresh Registration	RegistrationRefresh (command)	Command to refresh the registrations.

TLS Persistent Connections Status Section

Field Name	SNMP Variable	Description
Gateway	tlsPersistentConnectionStatusGateway	The SIP gateway used to register.
Local Port	tlsPersistentConnectionStatusLocalPort	Local port used by the TLS persistent connection.
Configured Remote Host	tlsPersistentConnectionStatusRemoteHost	The remote host used to establish the TLS persistent connection.
Remote IP Address	tlsPersistentConnectionStatusRemoteAddress	The resolved IP address of the remote host used to establish the TLS persistent connection.
State	tlsPersistentConnectionStatusState	The current state of the TLS persistent connection.

SIP Default Servers Section

Field Name	SNMP Variable	Description
Registrar Host	defaultStaticRegistrarServerHost	SIP registrar server FQDN and port.
Proxy Host	defaultStaticProxyHomeDomainHost	SIP proxy server FQDN and port.
Outbound Proxy Host	defaultStaticProxyOutboundHost	SIP outbound proxy server FQDN and port.
Messaging Server Host	defaultStaticMessagingHost	Messaging server FQDN and port.

SIP Gateway Specific Registrar Servers Section

Field Name	SNMP Variable	Description
Gateway Name	gwSpecificRegistrationGatewayName	String that identifies a SIP gateway in other tables.
Gateway Specific	gwSpecificRegistrationEnableConfig	Defines the configuration to use for a specific SIP gateway.
Registrar Host	gwSpecificRegistrationServerHost	SIP registrar server FQDN and port for a specific SIP gateway.

SIP Gateway Specific Proxy Servers Section

Field Name	SNMP Variable	Description
Gateway Name	gwSpecificProxyGatewayName	String that identifies a SIP gateway in other tables.
Gateway Specific	gwSpecificProxyEnableConfig	Defines the configuration to use for a specific SIP gateway.
Proxy Host	gwSpecificProxyHomeDomainHost	SIP proxy server FQDN and port for a specific SIP gateway.
Outbound Proxy Host	gwSpecificProxyOutboundHost	SIP outbound proxy server FQDN and port for a specific SIP gateway.

Keep Alive Section

Field Name	SNMP Variable	Description
Keep Alive Method	sipKeepAliveMethod	Method used to perform the SIP keep alive.
Keep Alive Interval	sipKeepAliveInterval	Defines the interval, in seconds, at which SIP OPTIONS are sent to verify the server status.
Keep Alive Destination	sipKeepAliveDestination	Determines the behaviour of the device when performing the keep alive action.

SIP Gateway Specific Keep Alive Targets Section

Field Name	SNMP Variable	Description
Gateway Name	gwKeepAliveAlternateDestinationGatewayName	String that identifies a SIP gateway in other tables.
Alternate Target	gwKeepAliveAlternateDestinationAlternateDestination	Alternate destination target server FQDN and port for a specific SIP gateway.

Registrations Sub-Page

Endpoints Registration Status Section

Field Name	SNMP Variable	Description
Endpoint	registrationStatusEndpoint	The endpoint related to this registration.
User Name	registrationStatusUsername	The username currently used by the registration.

Field Name	SNMP Variable	Description
Gateway Name	registrationStatusGateway	The SIP gateway used to register.
Registrar	registrationStatusRegistrar	The host of the registrar currently used by the registration.
Status	registrationStatusState	The current state of the registration.

Endpoints Messaging Subscription Status Section

Field Name	SNMP Variable	Description
Endpoint	mwiStatusEndpoint	The endpoint related to this subscription.
User Name	mwiStatusUsername	The username currently used by the subscription.
Gateway Name	mwiStatusGatewayName	The SIP gateway used for this subscription.
Messaging Host	mwiStatusMessagingHost	Messaging server FQDN and port used to subscribe the event state.
MWI Status	mwiStatusSubscriptionState	The current state of the subscription.

Unit Registration Status Section

Field Name	SNMP Variable	Description
User Name	registrationStatusUsername	The username currently used by the registration.
Gateway Name	registrationStatusGateway	The SIP gateway used to register.
Registrar	registrationStatusRegistrar	The host of the registrar currently used by the registration.
Status	registrationStatusState	The current state of the registration.

Endpoints Registration Section

Field Name	SNMP Variable	Description
Endpoint	userAgentEpId	String that identifies an endpoint in other tables.
User Name	userAgentUserName	String that uniquely identifies this endpoint in the domain.
Friendly Name	userAgentFriendlyName	Friendly name for SIP User Agent.
Register	userAgentRegister	Indicate whether the endpoint needs to register to the registrar.
Gateway Name	userAgentGatewayName	Selects on which SIP gateway the user configuration is applied.
Submit & Refresh Registration	RegistrationRefresh (command)	Command to refresh the registrations.

Unit Registration Section

Field Name	SNMP Variable	Description
Index	registrationUsersIndex	Unique identifier of the row.
User Name	registrationUsersUsername	String that uniquely identifies this user in the domain.
Gateway Name	registrationUsersGatewayName	Selects on which SIP gateway the user configuration is applied.
	registrationInsertUser (command)	Adds a row.
	registrationUsersDelete	Delete this row.
Submit & Refresh Registration	RegistrationRefresh (command)	Command to refresh the registrations.

Registration Configuration Section

Field Name	SNMP Variable	Description
Default Registration Refresh Time	defaultRegistrationRefreshTime	Defines the time, relative to the end of the registration, at which a registered unit will begin updating its registration.
Proposed Expiration Value In Registration	defaultRegistrationProposedExpirationValue	Configures the suggested expiration delay of a contact in the SIP REGISTER.
Default Expiration Value In Registration	defaultRegistrationExpirationValue	Configures the default registration expiration.

Authentication Sub-Page

Field Name	SNMP Variable	Description
Index	authenticationIndex	Authentication index for this row.
Apply to	authenticationApplyTo	Entity to which apply authentication.
Endpoint	authenticationEpId	Endpoint Identification.
Gateway	authenticationGatewayName	String that identifies a SIP gateway in other tables.
Validate Realm	authenticationValidateRealm	Defines whether or not the current credentials are valid for any realm.
Realm	authenticationRealm	Authentication Realm.
User Name	authenticationUserName	String that uniquely identifies this entity in the realm.
Password	authenticationPassword	User password.
Submit & Refresh Registration	RegistrationRefresh (command)	Command to refresh the registrations.
	authenticationInsert	Inserts a new row before this row.
	authenticationDelete	Deletes this row.
	authenticationDown	Moves the current row downside.
	authenticationUp	Moves the current row upside.

Transport Sub-Page

General Configuration Section

Field Name	SNMP Variable	Description
Add SIP Transport in Registration	transportConfigRegistrationEnable	Indicates whether or not the SIP Gateway must include its supported transports in its registrations.
Add SIP Transport in Contact Header	transportConfigContactEnable	Indicates whether or not the SIP Gateway must include its supported transport in all SIP messages that have the contact header, except for the REGISTER message.
Persistent TLS Base Port	transportTlsPersistentBasePort	Base port used to establish TLS persistent connections with SIP servers when the TLS transport is enabled.
Persistent TLS Retry Interval	transportTlsPersistentRetryInterval	Time interval before retrying the establishment of a TLS persistent connection.
TLS Trusted Certificate Level	transportTlsCertificateTrustLevel	Defines how a peer certificate is considered trusted for a TLS connection.
TCP Connect Timeout	interopTcpConnectTimeout	Defines the maximum time, in seconds, the unit should try to establish a TCP or TLS connection to SIP hosts.

Protocol Configuration Section

Field Name	SNMP Variable	Description
UDP	transportConfigUdpEnable	Enables or disables the UDP transport.
UDP QValue	transportConfigUdpQValue	Indicates the priority of the UDP transport.
TCP	transportConfigTcpEnable	Enables or disables the TCP transport.
TCP QValue	transportConfigTcpQValue	Indicates the priority of the TCP transport.
TLS	transportConfigTlsEnable	Enables or disables the TLS transport.
TLS QValue	transportConfigTlsQValue	Indicates the priority of the TLS transport.

Interop Sub-Page

Behavior on T.38 INVITE Not Accepted Section

Field Name	SNMP Variable	Description
SIP Error Code	behaviorOnT38InviteNotAcceptedSipErrorCode	SIP code in the error response to an INVITE for T.38 fax.
Behavior	behaviorOnT38InviteNotAcceptedBehavior	Behavior of the device when receiving a SIP error response to an INVITE for T.38 fax.

SIP Interop Section

Field Name	SNMP Variable	Description
Secure Header	interopSiemensTransportHeaderEnable	Add the 'x-Siemens-Call-Type' header to the SIP packets.
Default Username Value	interopDefaultUsernameValue	Username to use when the username is empty or undefined.
OPTIONS Method Support	interopSipOptionsMethodSupport	Determines the behaviour of the device when answering a SIP OPTIONS request.
Ignore OPTONS on no usable endpoints	InteropIgnoreSipOptionsOnNoUsableEndpoints	Determines whether or not the SIP OPTIONS requests should be ignored when all endpoints are unusable.
Behavior On Machine Detection	InteropBehaviorOnMachineDetection	Specifies the SIP device behavior when a machine is detected during a call.
Registration Contact Matching	InteropRegistrationContactMatching	Specifies the matching behaviour for the contact header received in positive responses to REGISTER requests sent by the unit.
Transmission Timeout	interopTransmissionTimeout	Changes the time to wait for a response or an ACK before considering a transaction timed out.

SDP Interop Section

Field Name	SNMP Variable	Description
Offer Answer Model		
Answer Codec Negotiation	answerCodecNegotiation	Defines the codec negotiation rule when generating a SDP answer.
Enforce Offer Answer Model	interopEnforceOfferAnswerModel	Determines whether or not the unit requires strict adherence to RFC 3264 from the peer when negotiating capabilities for the establishment of a media session.
Allow Less Media in Response	interopAllowLessMediaInResponse	Selects whether or not the unit enables the mapping between the "+" prefix of the username and the "type of number" property.
Allow Media Reactivation in Answer	interopAllowMediaReactivationInAnswer	Determines the unit behaviour when receiving a SDP answer activating a media that had been previously deactivated in the offer.
Multiple Active Media		

Field Name	SNMP Variable	Description
Allow Audio and Image Negotiation	interopAllowAudioAndImageNegotiation	Determines the unit behaviour when offering media or answering to a media offer with audio and image negotiation.
Allow Multiple Active Media in Answer	interopAllowMultipleActiveMediaInAnswer	Determines the behaviour of the device when answering a request offering more than one active media.
Other		
On Hold SDP Stream Direction in Answer	interopOnHoldSdpStreamDirection	Define how to set the direction attribute and the connection address in the SDP when answering a hold offer with the direction attribute “sendonly”.
Codec Vs Bearer Capabilities Mapping Preferred Codec Choice	interopCodecVsBearerCapabilitiesMappingPreferredCodecChoice	Configures the behavior of the CodecVsBearerCapabilitiesMapping table by modifying the selection of the preferred codec in the incoming SDP.

TLS Interop Section

Field Name	SNMP Variable	Description
Certificate Validation	InteropTlsCertificateValidation	Specifies which level of security is used to validate the peer certificate.

Misc Interop Section

Field Name	SNMP Variable	Description
Map Plus to TON International	interopMapPlusToTonInternational	Defines the behaviour of the unit when receiving less media announcements in the response than in the offer.
Ignore Plus in Username	interopIgnorePlusInUsername	Determines whether or not the plus character (+) is ignored when attempting to match a challenge username with usernames in the Authentication table.
Escape Pound (#) in SIP URI Username	interopEscapePoundInSipUriUsername	Determines whether or not the pound character (#) must be escaped in the username part of a SIP URI.
Escape Format	interopEscapeFormat	Configures the escaped characters to lower or uppercase hexadecimal format in SIP headers.

Misc Sub-Page

Penalty Box Section

Field Name	SNMP Variable	Description
Penalty Box Activation	penaltyBoxEnable	Indicates whether the unit uses the penalty box feature.
Penalty Box Time	penaltyBoxTime	Amount of time that a host spends in the penalty box.

SIP to Cause Error Mapping Section

Field Name	SNMP Variable	Description
SIP Code	errorMappingSipToCauseSipCode	SIP code to map to a cause.
Cause	errorMappingSipToCauseCause	Cause to map to the SIP code.
+	ErrorMappingInsertSipToCause (command)	Inserts a new row before this row.
−	erromappingSipToCauseDelete	Deletes this row.

Configure New SIP To Cause Error Mapping Panel

Field Name	SNMP Variable	Description
SIP Code	errorMappingSipToCauseSipCode	SIP code to map to a cause.
Cause	errorMappingSipToCauseCause	Cause to map to the SIP code.

Cause to SIP Error Mapping

Field Name	SNMP Variable	Description
Cause	errorMappingCauseToSipCause	Cause to map to the SIP code.
SIP Code	errorMappingCauseToSipSipCode	SIP code to map to a cause.
+	ErrorMappingInsertCauseToSip (command)	Inserts a new row before this row.
−	erromappingCauseToSipDelete	Deletes this row.

Cause To SIP Error Mapping Panel

Field Name	SNMP Variable	Description
Cause	errorMappingCauseToSipCause	Cause to map to the SIP code.
SIP Code	errorMappingCauseToSipSipCode	SIP code to map to a cause.

Additional Headers Section

Field Name	SNMP Variable	Description
Reason Header Support	ReasonHeaderSupport	Indicates whether or not the unit uses the SIP reason header.
Referred-By Support	ReferredByHeader	Indicates how the Referred-By header is used when participating in a transfer.

PRACK Section

Field Name	SNMP Variable	Description
UAS PRACK Support	uasPrackSupport	Determines the support of RFC 3262 (PRACK) when acting as as user agent server.
UAC PRACK Support	uacPrackSupport	Determines the support of RFC 3262 (PRACK) when acting as as user agent client.

Session Refresh Section

Field Name	SNMP Variable	Description
Session Refresh Timer Enable	defaultSessionTimerEnable	Enables/Disables the session expiration services.
Minimum Expiration Delay (s)	defaultSessionTimerMinimumExpirationDelay	Minimum value for the periodical session refreshes.
Maximum Expiration Delay (s):	defaultSessionTimerMaximumExpirationDelay	Suggested maximum time for the periodical session refreshes.
Session Refresh Request Method	sessionRefreshRequestMethod	Selects the method used for sending Session Refresh Requests.

SIP Gateway Configuration Section

Field Name	SNMP Variable	Description
Gateway Name	gatewayName	Name of the SIP gateway. It identifies the gateway in other tables.
SIP Domain Override	gatewayDomain	Controls whether or not to override the SIP domain used.

SIP Transfer Section

Field Name	SNMP Variable	Description
Blind Transfer Method	BlindTransferMethod	Selects the SIP method to use in a blind transfer scenario.

Diversion Section

Field Name	SNMP Variable	Description
Method	diversionConfigMethod	Selects the SIP method used to receive/send call diversion information in an INVITE.

Event Handling Section

Field Name	SNMP Variable	Description
Gateway Name	gwEventHandlingGatewayName	String that identifies a SIP gateway in other tables.
Reboot	gwEventHandlingReboot	Specifies whether a remote reboot via a SIP NOTIFY message event is supported or not for a specific SIP gateway.
CheckSync	gwEventHandlingCheckSync	Specifies whether a transfer script via a SIP NOTIFY message event is supported or not for a specific SIP gateway.

Messaging Subscription Section

Field Name	SNMP Variable	Description
Username in Request-URI	defaultUsernameInRequestUriEnable gwSpecificMwiUsernameInRequestUriEnable	Indicates whether or not the unit adds the username in the request URI of MWI SUBSCRIBE requests.

Advice Of Charge (AOC) Section

Field Name	SNMP Variable	Description
Gateway Name	GatewayName	String that identifies a SIP gateway in other tables.
AOC-D Support	AocDSupport	Specifies whether AOC (D)uring a call is supported for a specific SIP gateway.
AOC-E Support	AocESupport	Specifies whether AOC at the (E)nd of a call is supported for a specific SIP gateway.

Media Page

CODECS Sub-Page

Field Name	SNMP Variable	Description
Select Endpoint	endpointEpId	String that identifies an endpoint in other tables.

CODEC Section

Field Name	SNMP Variable	Description
Endpoint Specific	epSpecificCodecG711AlawEnableConfig epSpecificCodecG711MulawEnableConfig	Configuration to use for a specific endpoint.
	epSpecificCodecG723EnableConfig	
	epSpecificCodecG726r16kbpsEnableConfig epSpecificCodecG726r24kbpsEnableConfig epSpecificCodecG726r32kbpsEnableConfig epSpecificCodecG726r40kbpsEnableConfig	
	epSpecificCodecG729EnableConfig	
	epSpecificCodecT38EnableConfig	
	epSpecificCodecClearModeEnableConfig	
	epSpecificCodecClearChannelEnableConfig	
	epSpecificCodecXCCDEnableConfig	
Voice	defaultCodecG711AlawVoiceEnable epSpecificCodecG711AlawVoiceEnable	Indicates whether the codec can be selected for voice transmission.
	defaultCodecG711MulawVoiceEnable epSpecificCodecG711MulawVoiceEnable	
	defaultCodecG723VoiceEnable epSpecificCodecG723VoiceEnable	
	defaultCodecG726r16kbpsVoiceEnable epSpecificCodecG726r16kbpsVoiceEnable	
	defaultCodecG726r24kbpsVoiceEnable epSpecificCodecG726r24kbpsVoiceEnable	
	defaultCodecG726r32kbpsVoiceEnable epSpecificCodecG726r32kbpsVoiceEnable	
	defaultCodecG726r40kbpsVoiceEnable epSpecificCodecG726r40kbpsVoiceEnable	
	defaultCodecG729VoiceEnable epSpecificCodecG729VoiceEnable	
	defaultCodecClearModeVoiceEnable epSpecificCodecClearModeVoiceEnable	
	defaultCodecClearChannelVoiceEnable epSpecificCodecClearChannelVoiceEnable	
	defaultCodecXCCDVoiceEnable epSpecificCodecXCCDVoiceEnable	

Field Name	SNMP Variable	Description
Data	defaultCodecG711AlawDataEnable epSpecificCodecG711AlawDataEnable	Indicates whether the codec can be selected for data transmission.
	defaultCodecG711MulawDataEnable epSpecificCodecG711MulawDataEnable	
	defaultCodecG726r32kbpsDataEnable epSpecificCodecG726r32kbpsDataEnable	
	defaultCodecG726r40kbpsDataEnable epSpecificCodecG726r40kbpsDataEnable	
	defaultCodecT38DataEnable epSpecificCodecT38DataEnable	
	defaultCodecClearModeDataEnable epSpecificCodecClearModeDataEnable	
	defaultCodecClearChannelDataEnable epSpecificCodecClearChannelDataEnable	
	defaultCodecXCCDDataEnable epSpecificCodecXCCDDataEnable	

CODEC vs. Bearer Capabilities Mapping Section

Field Name	SNMP Variable	Description
Index	defaultCodecVsBearerCapabilitiesMappingIndex	Index of the current Codec vs. Bearer match.
Enable	defaultCodecVsBearerCapabilitiesMappingEnableMap	Defines if the outgoing codecs priority or selection should reflect the incoming ITC and vice versa.
CODEC	defaultCodecVsBearerCapabilitiesMappingCodec	The codec to be prioritized or selected in an outgoing INVITE when the incoming SETUP's ITC matches defaultCodecVsBearerCapabilitiesMappingInformationTransferCap.
Mapping Type	defaultCodecVsBearerCapabilitiesMappingMappingType	The ITC value to be set in the outgoing SETUP when the incoming INVITE's priority codec matches defaultCodecVsBearerCapabilitiesMappingCodec.
ITC	defaultCodecVsBearerCapabilitiesMappingInformationTransferCap	Mapping Type

Generic Voice Activity Detection (VAD)

Field Name	SNMP Variable	Description
Endpoint Specific	epSpecificCodecEnableConfig	Configuration to use for a specific endpoint.
Enable (G.711 and G.726)	defaultCodecGenericVoiceActivityDetection epSpecificCodecGenericVoiceActivityDetection	Generic VAD configuration.

G.711 a-law Section

Field Name	SNMP Variable	Description
Use Endpoint Specific	epSpecificCodecG711AlawEnableConfig	Configuration to use for a specific endpoint.
Voice Transmission	defaultCodecG711AlawVoiceEnable epSpecificCodecG711AlawVoiceEnable	Indicates whether the codec can be selected for voice transmission.
Voice Priority	defaultCodecG711AlawVoicePriority epSpecificCodecG711AlawVoicePriority	Priority of this voice codec versus the other voice codecs.
Data Transmission	defaultCodecG711AlawDataEnable epSpecificCodecG711AlawDataEnable	Indicates whether the codec can be selected for data transmission.
Data Priority	defaultCodecG711AlawDataPriority epSpecificCodecG711AlawDataPriority	Priority of this data codec versus the other data codecs.

Field Name	SNMP Variable	Description
Minimum Packetization Time	defaultCodecG711AlawMinPTime epSpecificCodecG711AlawMinPTime	Lower boundary for the packetization period.
Maximum Packetization Time	defaultCodecG711AlawMaxPTime epSpecificCodecG711AlawMaxPTime	Upper boundary for the packetization period.

G.711 u-law Section

Field Name	SNMP Variable	Description
Use Endpoint Specific	epSpecificCodecG711MulawEnableConfig	Configuration to use for a specific endpoint.
Voice Transmission	defaultCodecG711MulawVoiceEnable epSpecificCodecG711MulawVoiceEnable	Indicates whether the codec can be selected for voice transmission.
Voice Priority	defaultCodecG711MulawVoicePriority epSpecificCodecG711MulawVoicePriority	Priority of this voice codec versus the other voice codecs.
Data Transmission	defaultCodecG711MulawDataEnable epSpecificCodecG711MulawDataEnable	Indicates whether the codec can be selected for data transmission.
Data Priority	defaultCodecG711MulawDataPriority epSpecificCodecG711MulawDataPriority	Priority of this data codec versus the other data codecs.
Minimum Packetization Time	defaultCodecG711MulawMinPTime epSpecificCodecG711MulawMinPTime	Lower boundary for the packetization period.
Maximum Packetization Time	defaultCodecG711MulawMaxPTime epSpecificCodecG711MulawMaxPTime	Upper boundary for the packetization period.

G.723 Section

Field Name	SNMP Variable	Description
Use Endpoint Specific	epSpecificCodecG723EnableConfig	Configuration to use for a specific endpoint.
Voice Transmission	defaultCodecG723VoiceEnable epSpecificCodecG723VoiceEnable	Indicates whether the codec can be selected for voice transmission.
Voice Priority	defaultCodecG723VoicePriority epSpecificCodecG723VoicePriority	Priority of this voice codec versus the other voice codecs.
Bit Rate	defaultCodecG723Bitrate epSpecificCodecG723Bitrate	G.723.1 bit rate to use.
Minimum Packetization Time	defaultCodecG723MinPTime epSpecificCodecG723MinPTime	Lower boundary for the packetization period.
Maximum Packetization Time	defaultCodecG723MaxPTime epSpecificCodecG723MaxPTime	Upper boundary for the packetization period.

G.726 16Kbps Section

Field Name	SNMP Variable	Description
Use Endpoint Specific	epSpecificCodecG726r16kbpsEnableConfig	Configuration to use for a specific endpoint.
Voice Transmission	defaultCodecG726r16kbpsVoiceEnable epSpecificCodecG726r16kbpsVoiceEnable	Indicates whether the codec can be selected for voice transmission.
Voice Priority	defaultCodecG726r16kbpsVoicePriority epSpecificCodecG726r16kbpsVoicePriority	Priority of this voice codec versus the other voice codecs.
Payload Type	defaultCodecG726r16kbpsPayloadType epSpecificCodecG726r16kbpsPayloadType	RTP dynamic payload type used in an initial offer.
Minimum Packetization Time	defaultCodecG726r16kbpsMinPTime epSpecificCodecG726r16kbpsMinPTime	Lower boundary for the packetization period.
Maximum Packetization Time	defaultCodecG726r16kbpsMaxPTime epSpecificCodecG726r16kbpsMaxPTime	Upper boundary for the packetization period.

G.726 24Kbps Section

Field Name	SNMP Variable	Description
Use Endpoint Specific	epSpecificCodecG726r24kbpsEnableConfig	Configuration to use for a specific endpoint.
Voice Transmission	defaultCodecG726r24kbpsVoiceEnable epSpecificCodecG726r24kbpsVoiceEnable	Indicates whether the codec can be selected for voice transmission.
Voice Priority	defaultCodecG726r24kbpsVoicePriority epSpecificCodecG726r24kbpsVoicePriority	Priority of this voice codec versus the other voice codecs.
Payload Type	defaultCodecG726r24kbpsPayloadType epSpecificCodecG726r24kbpsPayloadType	RTP dynamic payload type used in an initial offer.
Minimum Packetization Time	defaultCodecG726r24kbpsMinPTime epSpecificCodecG726r24kbpsMinPTime	Lower boundary for the packetization period.
Maximum Packetization Time	defaultCodecG726r24kbpsMaxPTime epSpecificCodecG726r24kbpsMaxPTime	Upper boundary for the packetization period.

G.726 32Kbps Section

Field Name	SNMP Variable	Description
Use Endpoint Specific	epSpecificCodecG726r32kbpsEnableConfig	Configuration to use for a specific endpoint.
Voice Transmission	defaultCodecG726r32kbpsVoiceEnable epSpecificCodecG726r32kbpsVoiceEnable	Indicates whether the codec can be selected for voice transmission.
Voice Priority	defaultCodecG726r32kbpsVoicePriority epSpecificCodecG726r32kbpsVoicePriority	Priority of this voice codec versus the other voice codecs.
Data Transmission	defaultCodecG726r32kbpsDataEnable epSpecificCodecG726r32kbpsDataEnable	Indicates whether the codec can be selected for data transmission.
Data Priority	defaultCodecG726r32kbpsDataPriority epSpecificCodecG726r32kbpsDataPriority	Priority of this data codec versus the other data codecs.
Payload Type	defaultCodecG726r32kbpsPayloadType epSpecificCodecG726r32kbpsPayloadType	RTP dynamic payload type used in an initial offer.
Minimum Packetization Time	defaultCodecG726r32kbpsMinPTime epSpecificCodecG726r32kbpsMinPTime	Lower boundary for the packetization period.
Maximum Packetization Time	defaultCodecG726r32kbpsMaxPTime epSpecificCodecG726r32kbpsMaxPTime	Upper boundary for the packetization period.

G.726 40Kbps Section

Field Name	SNMP Variable	Description
Use Endpoint Specific	epSpecificCodecG726r40kbpsEnableConfig	Configuration to use for a specific endpoint.
Voice Transmission	defaultCodecG726r40kbpsVoiceEnable epSpecificCodecG726r40kbpsVoiceEnable	Indicates whether the codec can be selected for voice transmission.
Voice Priority	defaultCodecG726r40kbpsVoicePriority epSpecificCodecG726r40kbpsVoicePriority	Priority of this voice codec versus the other voice codecs.
Data Transmission	defaultCodecG726r40kbpsDataEnable epSpecificCodecG726r40kbpsDataEnable	Indicates whether the codec can be selected for data transmission.
Data Priority	defaultCodecG726r40kbpsDataPriority epSpecificCodecG726r40kbpsDataPriority	Priority of this data codec versus the other data codecs.
Payload Type	defaultCodecG726r40kbpsPayloadType epSpecificCodecG726r40kbpsPayloadType	RTP dynamic payload type used in an initial offer.
Minimum Packetization Time	defaultCodecG726r40kbpsMinPTime epSpecificCodecG726r40kbpsMinPTime	Lower boundary for the packetization period.
Maximum Packetization Time	defaultCodecG726r40kbpsMaxPTime epSpecificCodecG726r40kbpsMaxPTime	Upper boundary for the packetization period.

G.729 Section

Field Name	SNMP Variable	Description
Use Endpoint Specific	epSpecificCodecG729EnableConfig	Configuration to use for a specific endpoint.
Voice Transmission	defaultCodecG729VoiceEnable epSpecificCodecG729VoiceEnable	Indicates whether the codec can be selected for voice transmission.
Voice Priority	defaultCodecG729VoicePriority epSpecificCodecG729VoicePriority	Priority of this voice codec versus the other voice codecs.
Minimum Packetization Time	defaultCodecG729MinPTime epSpecificCodecG729MinPTime	Lower boundary for the packetization period.
Maximum Packetization Time	defaultCodecG729MaxPTime epSpecificCodecG729MaxPTime	Upper boundary for the packetization period.
Built-In VAD	defaultCodecG729VoiceActivityDetection epSpecificCodecG729VoiceActivityDetection	G.729 VAD configuration.

T.38 Section

Field Name	SNMP Variable	Description
Use Endpoint Specific	epSpecificCodecT38EnableConfig	Configuration to use for a specific endpoint.
Enable	defaultCodecT38DataEnable epSpecificCodecT38DataEnable	If enabled, the T.38 protocol is used for fax transmission.
Priority	defaultCodecT38DataPriority epSpecificCodecT38DataPriority	Priority of this data codec versus the other data codecs.
Redundancy Level	defaultCodecT38RedundancyLevel epSpecificCodecT38RedundancyLevel	Number of redundancy packets.
Detection Threshold	defaultCodecT38DetectionThreshold epSpecificCodecT38DetectionThreshold	Sets the T.38 input signal detection threshold.
Frame Redundancy Level	defaultCodecT38FinalFramesRedundancy	Defines the number of times T.38 packets will be retransmitted.
No Signal	defaultCodecT38NoSignalEnable	Enables/disables the sending of T.38 no-signal packets.
No Signal Timeout	defaultCodecT38NoSignalTimeout	The period, in seconds, at which no-signal packets are sent during a T.38 transmission, in the absence of valid data.

Clear Mode Section

Field Name	SNMP Variable	Description
Use Endpoint Specific	epSpecificCodecClearModeEnableConfig	Configuration to use for a specific endpoint.
Voice Transmission	defaultCodecClearModeVoiceEnable epSpecificCodecClearModeVoiceEnable	Indicates whether the codec can be selected for voice transmission.
Voice Priority	defaultCodecClearModeVoicePriority epSpecificCodecClearModeVoicePriority	Priority of this voice codec versus the other voice codecs.
Data Transmission	defaultCodecClearModeDataEnable epSpecificCodecClearModeDataEnable	Indicates whether the codec can be selected for data transmission.
Data Priority	defaultCodecClearModeDataPriority epSpecificCodecClearModeDataPriority	Priority of this data codec versus the other data codecs.
Payload Type	defaultCodecClearModePayloadType epSpecificCodecClearModePayloadType	RTP dynamic payload type used in an initial offer.
Minimum Packetization Time	defaultCodecClearModeMinPTime epSpecificCodecClearModeMinPTime	Lower boundary for the packetization period.
Maximum Packetization Time	defaultCodecClearModeMaxPTime epSpecificCodecClearModeMaxPTime	Upper boundary for the packetization period.

Clear Channel Section

Field Name	SNMP Variable	Description
Use Endpoint Specific	epSpecificCodecClearChannelEnableConfig	Configuration to use for a specific endpoint.
Voice Transmission	defaultCodecClearChannelVoiceEnable epSpecificCodecClearChannelVoiceEnable	Indicates whether the codec can be selected for voice transmission.
Voice Priority	defaultCodecClearChannelVoicePriority epSpecificCodecClearChannelVoicePriority	Priority of this voice codec versus the other voice codecs.
Data Transmission	defaultCodecClearChannelDataEnable epSpecificCodecClearChannelDataEnable	Indicates whether the codec can be selected for data transmission.
Data Priority	defaultCodecClearChannelDataPriority epSpecificCodecClearChannelDataPriority	Priority of this data codec versus the other data codecs.
Payload Type	defaultCodecClearChannelPayloadType epSpecificCodecClearChannelPayloadType	RTP dynamic payload type used in an initial offer.
Minimum Packetization Time	defaultCodecClearChannelMinPTime epSpecificCodecClearChannelMinPTime	Lower boundary for the packetization period.
Maximum Packetization Time	defaultCodecClearChannelMaxPTime epSpecificCodecClearChannelMaxPTime	Upper boundary for the packetization period.

X CCD Section

Field Name	SNMP Variable	Description
Endpoint Specific	epSpecificCodecXCCDEnableConfig	Configuration to use for a specific endpoint.
Voice Transmission	defaultCodecXCCDVoiceEnable epSpecificCodecXCCDVoiceEnable	Indicates whether the codec can be selected for voice transmission.
Voice Priority	defaultCodecXCCDVoicePriority epSpecificCodecXCCDVoicePriority	Priority of this voice codec versus the other voice codecs.
Data Transmission	defaultCodecXCCDDataEnable epSpecificCodecXCCDDataEnable	Indicates whether the codec can be selected for data transmission.
Data Priority	defaultCodecXCCDDataPriority epSpecificCodecXCCDDataPriority	Priority of this data codec versus the other data codecs.
Payload Type	defaultCodecXCCDPayloadType epSpecificCodecXCCDPayloadType	RTP dynamic payload type used in an initial offer.
Minimum Packetization Time	defaultCodecXCCDMinPTime epSpecificCodecXCCDMinPTime	Lower boundary for the packetization period.
Maximum Packetization Time	defaultCodecXCCDMaxPTime epSpecificCodecXccdaxPTime	Upper boundary for the packetization period.

Security Sub-Page

Security Section

Field Name	SNMP Variable	Description
RTP		
Mode	defaultSecurityRtpMode epSpecificSecurityRtpMode	Defines the RTP payload mode (secure or not secure).
Key Management	defaultSecurityKeyManagement epSpecificSecurityKeyManagement	Defines the key management protocol for SRTP.
Encryption	defaultSecurityRtpEncryption epSpecificSecurityRtpEncryption	Defines the encryption type to be used with SRTP.
T.38		

Field Name	SNMP Variable	Description
Allow unsecure T.38 with secure RTP	allowUnsecureT38WithSrtp	Enables T38 even if the call has been established previously in SRTP.

RTP Stats

Collection Period Statistics

Field Name	SNMP Variable	Description
Period Beginning	lastPeriodsStatsPeriodBeginning	Date and time of the collection period beginning.
Period End	lastPeriodsStatsPeriodEnd	Date and time of the collection period end.
Octets Tx	lastPeriodsStatsOctetsTransmitted	Number of octets transmitted during the collection period.
Octets Rx	lastPeriodsStatsOctetsReceived	Number of octets received during the collection period.
Packets Tx	lastPeriodsStatsPacketsTransmitted	Number of packets transmitted during the collection period.
Packets Rx	lastPeriodsStatsPacketsReceived	Number of packets received during the collection period.
Packets Lost	lastPeriodsStatsPacketsLost	Number of packets lost during the collection period.
Min. Jitter	lastPeriodsStatsMinimumInterarrivalJitter	Minimum interarrival time, in milliseconds, during the collection period.
Max. Jitter	lastPeriodsStatsMaximumInterarrivalJitter	Maximum interarrival time, in milliseconds, during the collection period.
Avg. Jitter	lastPeriodsStatsAverageInterarrivalJitter	Average interarrival time, in milliseconds, during the collection period.
Min. Latency	lastPeriodsStatsMinimumLatency	Minimum latency, in milliseconds, during the collection period.
Max. Latency	lastPeriodsStatsMaximumLatency	Maximum latency, in milliseconds, during the collection period.
Avg. Latency	lastPeriodsStatsAverageLatency	Average latency, in milliseconds, during the collection period.

Connection Statistics

Field Name	SNMP Variable	Description
Octets Tx	lastConnectionsStatsOctetsTransmitted	Number of octets transmitted during the connection.
Octets Rx	lastConnectionsStatsOctetsReceived	Number of octets received during the connection.
Packets Tx	lastConnectionsStatsPacketsTransmitted	Number of packets transmitted during the connection.
Packets Rx	lastConnectionsStatsPacketsReceived	Number of packets received during the connection.
Packets Lost	lastConnectionsStatsPacketsLost	Number of packets lost during the connection.
Min. Jitter	lastConnectionsStatsMinimumInterarrivalJitter	Minimum interarrival time, in milliseconds, during the connection.
Max. Jitter	lastConnectionsStatsMaximumInterarrivalJitter	Maximum interarrival time, in milliseconds, during the connection.
Avg. Jitter	lastConnectionsStatsAverageInterarrivalJitter	Average interarrival time, in milliseconds, during the connection.
Min. Latency	lastConnectionsStatsMinimumLatency	Minimum latency, in milliseconds, during the connection.
Max. Latency	lastConnectionsStatsMaximumLatency	Maximum latency, in milliseconds, during the connection.
Avg. Latency	lastConnectionsStatsAverageLatency	Average latency, in milliseconds, during the connection.

Statistics Configuration Section

Field Name	SNMP Variable	Description
Collection Period (minutes)	statsCollectionPeriodDuration	Specifies the collection period duration (in minutes).
Generate Connection End Notification	statsPerConnectionNotificationEnable	Enables the generation of connection end statistics notification.
Generate Collection Period End Notification	statsPerPeriodNotificationEnable	Enables the generation of period statistics notification.

Misc Sub-Page

Jitter Buffer Section

Field Name	SNMP Variable	Description
Endpoint Specific	epSpecificJitterBufferEnableConfig	Configuration to use for a specific endpoint.
Level	defaultJitterBufferLevel epSpecificJitterBufferLevel	Jitter bufffer level.
Voice Call Minimum	defaultJitterBufferCustomMinLength epSpecificJitterBufferCustomMinLength	Jitter buffer minimum length.
Voice Call Maximum	defaultJitterBufferCustomMaxLength epSpecificJitterBufferCustomMaxLength	Jitter buffer maximum length.
Data Call Playout Type	defaultVbdJitterBufferType epSpecificCustomVbdJitterBufferType	Algorithm to use for managing the jitter buffer during a call.
Data Call Minimum	defaultVbdJitterBufferCustomMinLength epSpecificCustomVbdMinLength	The delay the jitter buffer tries to maintain.
Data Call Nominal	defaultVbdJitterBufferCustomNomLength epSpecificCustomVbdNomLength	The delay the jitter buffer uses when a call begins.
Data Call Maximum	defaultVbdJitterBufferCustomMaxLength epSpecificCustomVbdMaxLength	The highest delay the jitter buffer is allowed to introduce.

DTMF Transport Section

Field Name	SNMP Variable	Description
Endpoint Specific	epSpecificDtmfTransportEnableConfig	Configuration to use for a specific endpoint.
Transport Method	defaultDtmfTransportMethod epSpecificDtmfTransportMethod	Type of DTMF transport.
SIP Transport Method	interopDtmfTransportMethod	Defines the method used to transport DTMFs out-of-band over the SIP protocol
Payload Type	defaultDtmfTransportPayloadType epSpecificDtmfTransportPayloadType	RTP dynamic payload type used for telephone-event in an initial offer.

Machine Detection Section

Field Name	SNMP Variable	Description
Endpoint Specific	specificMachineDetectionEnableConfig	Configuration to use for a specific interface.
CNG Tone Detection	defaultMachineDetectionCngToneDetection specificMachineDetectionCngToneDetection	Enables fax calling tone (CNG tone) detection.
CED Tone Detection	defaultMachineDetectionCedToneDetection specificMachineDetectionCedToneDetection	Enables CED tone detection.

Field Name	SNMP Variable	Description
V.21 Modulation Detection	defaultMachineDetectionV21ModulationDetection specificMachineDetectionV21ModulationDetection	Enables fax V.21 modulation detection.
Behavior on CED Tone Detection	defaultMachineDetectionBehaviorOnCedToneDetection specificMachineDetectionBehaviorOnCedToneDetection	Defines the behavior of the unit upon detection of a CED tone.

Base Ports Section

Field Name	SNMP Variable	Description
RTP	ipTransportRtpBasePort	UDP base port for the RTP/RTCP protocols.
SRTP	ipTransportSrtpBasePort	UDP base port for the SRTP/SRTCP protocols.
T.38	ipTransportT38BasePort	T.38 base port.

Telephony Page

DTMF Maps Sub-Page

General Configuration Section

Field Name	SNMP Variable	Description
First DTMF Timeout	dtmfMapTimeoutFirstDtmf	Time the user has to enter the first DTMF after the dial tone.
Inter DTMF Timeout	dtmfMapTimeoutInterDtmf	Value of the “T” DTMF in the DTMF map strings.
Completion Timeout	dtmfMapTimeoutCompletion	Total time the user has to dial the DTMF sequence.
DTMF Maps Digit Detection (FXO/FXS)	DtmfMapDigitDetection	Determines when a digit is processed through the DTMF maps.

Allowed DTMF Map Section

Field Name	SNMP Variable	Description
Index	callDtmfMapAllowedIndex	Accepted DTMF map index for this row.
Enable	callDtmfMapAllowedEnable	Enables/Disables the row.
Apply to	callDtmfMapAllowedApplyTo	Entity to which apply the DTMF map.
Endpoint	callDtmfMapAllowedEpId	String that identifies an endpoint in other tables.
DTMF Map	callDtmfMapAllowedDtmfMap	DTMF map that is considered valid when dialed.
Transformation	callDtmfMapAllowedDtmfTransformation	Transformation to apply to the signalled DTMF before using it as call destination.
Target	callDtmfMapAllowedTargetHost	Target to use when the DTMF map matches.
Emergency	callDtmfMapAllowedEmergency	Enables/Disables the emergency process of the call.

Refused DTMF Map Section

Field Name	SNMP Variable	Description
Index	callDtmfMapRefuseIndex	Refused DTMF map index for this row.

Field Name	SNMP Variable	Description
Enable	callDtmfMapRefuseEnable	If enabled, this DTMF map is recognised and refused only if it is also valid.
Apply to	callDtmfMapRefuseApplyTo	Sets the entity to which apply the DTMF map.
Endpoint	callDtmfMapRefuseEpId	String that identifies an endpoint in other tables.
DTMF Map	callDtmfMapRefuseDtmfMap	DTMF map that is considered invalid when dialed.

DTMF Map Timeout Section

Field Name	SNMP Variable	Description
Endpoint	EpSpecificDtmfMapTimeoutEpId	String that identifies an endpoint in other tables.
Override	EpSpecificDtmfMapTimeoutEnableConfig	Defines the configuration to use for a specific endpoint.
First DTMF Timeout	EpSpecificDtmfMapTimeoutFirstDtmf	Time the user has to enter the first DTMF after the dial tone.
Inter DTMF Timeout	EpSpecificDtmfMapTimeoutInterDtmf	Value of the 'T' DTMF in the DTMF map strings.
Completion Timeout	EpSpecificDtmfMapTimeoutCompletion	Total time the user has to dial the DTMF sequence.

Call Forward Sub-Page

Field Name	SNMP Variable	Description
Select Endpoint	endpointEpId	String that identifies an endpoint in other tables.

Call Forward On Busy Section

Field Name	SNMP Variable	Description
Endpoint Specific	epSpecificForwardOnBusyEnableConfig	Defines the configuration to use for a specific endpoint.
Allow Activation via Handset	defaultForwardOnBusyEnable epSpecificForwardOnBusyEnable	Enables/Disables the call forward on busy service.
DTMF Map Activation	defaultForwardOnBusyDtmfMapActivation	DTMF map the user can dial to enable the application of the service.
DTMF Map Deactivation	defaultForwardOnBusyDtmfMapDeactivation	DTMF map the user can dial to disable the application of the service.
Activation	forwardOnBusyConfigActivation	Activation status of the call forward on busy service.
Forwarding Address:	forwardOnBusyConfigForwardingAddress	Address or telephone number to which the user wants to forward calls.

Call Forward On No Answer Section

Field Name	SNMP Variable	Description
Endpoint Specific	epSpecificForwardNoAnswerEnableConfig	Defines the configuration to use for a specific endpoint.
Allow Activation via Handset	defaultForwardNoAnswerEnable epSpecificForwardNoAnswerEnable	Enables/Disables the call forward on no answer service.
DTMF Map Activation	defaultForwardNoAnswerDtmfMapActivation	DTMF map the user can dial to enable the application of the service.
DTMF Map Deactivation	defaultForwardNoAnswerDtmfMapDeactivation	DTMF map the user can dial to disable the application of the service.
Timeout	defaultForwardNoAnswerTimeout epSpecificForwardNoAnswerTimeout	Time, in milliseconds, the telephone keeps ringing before the call forwarding activates.
Activation	forwardNoAnswerConfigActivation	Activation status of the call forward on no answer service.
Forwarding Address:	forwardNoAnswerConfigForwardingAddress	Address or telephone number to which the user wants to forward calls.

Call Forward Unconditional Section

Field Name	SNMP Variable	Description
Endpoint Specific	epSpecificForwardUnconditionalEnableConfig	Defines the configuration to use for a specific endpoint.
Allow Activation via Handset	defaultForwardUnconditionalEnable epSpecificForwardUnconditionalEnable	Enables/Disables the unconditional call forward service.
DTMF Map Activation	defaultForwardUnconditionalDtmfMapActivation	DTMF map the user can dial to enable the application of the service.
DTMF Map Deactivation	defaultForwardUnconditionalDtmfMapDeactivation	DTMF map the user can dial to disable the application of the service.
Activation	forwardUnconditionalConfigActivation	Activation state of the unconditional call forward service.
Forwarding Address:	forwardUnconditionalConfigForwardingAddress	Address or telephone number to which the user wants to forward calls.

Services Sub-Page

Field Name	SNMP Variable	Description
Select Endpoint	endpointEpId	String that identifies an endpoint in other tables.

Service Section

Field Name	SNMP Variable	Description
Blind Transfer	transferStatusBlindState	Status of the blind transfer service.
Attended Transfer	transferStatusAttendedState	Status of the attended transfer service.
Call Waiting	callWaitingStatusState	Status of the call waiting service.
Conference	conferenceStatusState	Status of the conference service.
Hold	holdStatusState	Status of the holding service.
Second Call	secondCallStatusState	Status of the second call service.

Active Call Completion Section

Field Name	SNMP Variable	Description
Endpoint	callCompletionConfigEpId	Identification of the endpoint using this call completion service.
Type	callCompletionConfigType	The type of the call completion.
Target Address	callCompletionConfigTargetAddress	The target address of the call completion.
Target State	callCompletionConfigTargetState	The state of the call completion target.

Services Configuration Section

Field Name	SNMP Variable	Description
General Configuration		
Endpoint Specific	epSpecificCallEnableConfig	Defines the configuration to use for a specific endpoint.
Hook Flash Processing	defaultCallHookFlashProcessing epSpecificCallHookFlashProcessing	Selects how to process hook-flash detection.
Automatic Call		
Endpoint Specific	epSpecificAutoCallEnableConfig	Defines the configuration to use for a specific endpoint.
Automatic Call Activation	defaultAutoCallEnable epSpecificAutoCallEnable	Enables/Disables the automatic call service. This service provides a 'redphone'-like experience.

Field Name	SNMP Variable	Description
Automatic Call Target	defaultAutoCallTargetAddress epSpecificAutoCallTargetAddress	Address or telephone number that the user wants to automatically call.
Call Completion		
Endpoint Specific	epSpecificCallCompletionEnableConfig	Defines the configuration to use for a specific endpoint.
Allow CCBS Activation Via Handset	defaultCallCompletionBusySubscriberEnable epSpecificCallCompletionBusySubscriberEnable	Enables/Disables the call completion busy subscriber (CCBS) service.
Allow CCNR Activation Via Handset	defaultCallCompletionNoResponseEnable epSpecificCallCompletionNoResponseEnable	Enables/Disables the call completion no response (CCNR) service.
CCBS DTMF Map Activation	defaultCallCompletionBusySubscriberDtmfMapActivation	DTMF map the user can dial to enable the application of the call completion busy subscriber (CCBS) service.
CCNR DTMF Map Activation	defaultCallCompletionNoResponseDtmfMapActivation	DTMF map the user can dial to enable the application of the call completion no response (CCNR) service.
DTMF Map Deactivation	defaultCallCompletionDtmfMapDeactivation	DTMF map the user can dial to disable the application of the call completion busy subscriber (CCBS) and call completion no response (CCNR) services.
Expiration Timeout	defaultCallCompletionExpirationTimeout	Defines the delay after the call completion activation to automatically deactivate the call completion if the call is not completed.
Method	defaultCallCompletionMethod	Selects the call completion method to detect that the call completion destination is ready to complete the call.
Auto Reactivate	defaultCallCompletionAutoReactivateEnable	Enables/Disables the call compleion auto reactivation.
Auto Reactivate Delay	defaultCallCompletionAutoReactivateDelay	Defines the minimal delay to wait before executing a call completion after its activation.
Early-Media Behaviour	defaultCallCompletionEarlyMediaBehaviour	Defines how the call completion service needs to interpret the reception of a progress message with early media.
Polling Interval	defaultCallCompletionPollingInterval	Defines the delay between the calls to the call completion target used for the polling mechanism.
Call Transfer		
Endpoint Specific	epSpecificTransferEnableConfig	Defines the configuration to use for a specific endpoint.
Blind Transfer Activation	defaultTransferBlindEnable epSpecificTransferBlindEnable	Enables/Disables the blind call transfer service.
Attended Transfer Activation	defaultTransferAttendedEnable epSpecificTransferAttendedEnable	Enables/Disables the attended call transfer service.
Call Waiting		
Endpoint Specific	epSpecificCallWaitingEnableConfig	Defines the configuration to use for a specific endpoint.
Call Waiting Activation	defaultCallWaitingEnable epSpecificCallWaitingEnable	Enables/Disables the call waiting service.
Cancel DTMF Map	defaultCallWaitingCancelDtmfMap	Default DTMF Map to Cancel the Call Waiting Service
Conference		
Endpoint Specific	epSpecificConferenceEnableConfig	Defines the configuration to use for a specific endpoint.
Conference Activation	defaultConferenceEnable epSpecificConferenceEnable	Enables/Disables the call conference service.
Delayed Hotline		
Endpoint Specific	epSpecificDelayedHotlineEnableConfig	Defines the configuration to use for a specific endpoint.
Delayed Hotline Activation	defaultDelayedHotlineEnable epSpecificDelayedHotlineEnable	Enables/Disables the delayed hotline service.
Delayed Hotline Condition	defaultDelayedHotlineCondition epSpecificDelayedHotlineCondition	Selects the condition(s) that activate the delayed hotline.
Delayed Hotline Target	defaultDelayedHotlineTargetAddress epSpecificDelayedHotlineTargetAddress	Address or telephone number of the target of the delayed hotline.
Direct IP Address Call		

Field Name	SNMP Variable	Description
Direct IP Address Call Activation	defaultCallAllowDirectIp	Enables/Disables the direct IP address call service.
Hold		
Endpoint Specific	epSpecificHoldEnableConfig	Defines the configuration to use for a specific endpoint.
Hold Activation	defaultHoldEnable epSpecificHoldEnable	Enables/Disables the holding service.
Second Call		
Endpoint Specific	epSpecificSecondCallEnableConfig	Defines the configuration to use for a specific endpoint.
Second Call Activation	defaultSecondCallEnable epSpecificSecondCallEnable	Enables/Disables the second call service.

Tone Customization Sub-Page

Field Name	SNMP Variable	Description
Select Tone	countryCustomizationToneTone	Tone to customize.
Override Current Tone Values	countryCustomizationToneOverride	Allows overriding the default country tone setting.

Current Tone Definition section

Field Name	SNMP Variable	Description
Frequencies	countryToneStatusPattern	Pattern description of the currently used tone for the country
Value		
Power		
Loop Count		

Current Tone States section

Field Name	SNMP Variable	Description
State	countryToneStatusPattern	Pattern description of the currently used tone for the country
On/Off		
Frequencies		
Duration		
Loop		
Next State		

Overriden Tone Definition section

Field Name	SNMP Variable	Description
Frequencies	countryCustomizationTonePattern	Pattern description of the custom tone.
Value		
Power		
Loop Count		

Overriden Tone States section

Field Name	SNMP Variable	Description
State	countryCustomizationTonePattern	Pattern description of the custom tone.
On/Off		
Frequencies		
Duration		
Loop		
Next State		

Music on Hold Sub-Page

Field Name	SNMP Variable	Description
Submit & Transfer Now	Transfer (command)	Saves the settings and transfers the MP3 file now.
Submit & Cancel Transfer	CancelTransfer (command)	Saves the settings and stops a file transfer in progress.

Status Section

Field Name	SNMP Variable	Description
File Status	fileStatus	Status of the MP3 file in the unit.
Last Transfer Result	lastTransferStatus	Status of the last file transfer attempt.
Last Successful Transfer	lastTransferDateTime	Date and time of the last successful music file transfer.

Music On Hold Configuration Section

Field Name	SNMP Variable	Description
Streaming	musicOnHoldStreamingEnable	Indicate whether or not the unit should play music when being put on hold.

Transfer Configuration Section

Field Name	SNMP Variable	Description
URL	fileUrl	URL to a MP3 file which will be loaded at unit startup and reloaded every time the ReloadInterval elapsed.
User Name	username	When authentication is required by the remote file server, this variable will be used as the username.
Password	password	When authentication is required by the remote file server, this variable will be used as the password.
Reload Interval	reloadInterval	Time, in hours, between attempts to load the MP3 file.

Misc Sub-Page

Country Section

Field Name	SNMP Variable	Description
Country Selection	countrySelection	List of predefined country settings.

Custom Tone Section

Field Name	SNMP Variable	Description
Override	countryCustomizationToneOverride	Overrides the default country tone setting.
Pattern	countryCustomizationTonePattern	Pattern description of the custom tone.

Call Detail Record Section

Field Name	SNMP Variable	Description
Syslog Remote Host	syslogRemoteHost	Host name and port number of the device that archives CDR log entries.
Syslog Format	syslogFormat	Specifies the format of the syslog Call Detail Record.
Syslog Facility	syslogFacility	Syslog facility used by the unit to route the Call Detail Record messages.

Call Router Page

Status Sub-Page

Field Name	SNMP Variable	Description
Config Modified	configModifiedStatus	Shows whether the configuration of the call routing was modified without being applied.

Route Section

Field Name	SNMP Variable	Description
Type	routeStatusType	Displays the associated route type.
Source	routeStatusSourceCriteria	Source criteria to match to apply the route.
Properties Criteria	routeStatusPropertiesCriteria	Call properties criteria to match to apply the route.
Expression Criteria	routeStatusExpressionCriteria	Expression criteria to match to apply the route.
Mappings	routeStatusMapping	Name of the properties manipulation to apply to the call if the criteria match.
Signaling Properties	routeStatusSignalingProperties	Name of the signaling properties to apply to the call.
Destination	routeStatusDestination	Destination to apply to the call if it matches the criteria.

Signaling Properties Section

Field Name	SNMP Variable	Description
Name	signalingPropertiesStatusName	Name of the Signaling properties defined by this row.
Early Connect	signalingPropertiesStatusEarlyConnect	Enables/Disables the early connect feature.
Early Disconnect	signalingPropertiesStatusEarlyDisconnect	Enables/Disables the early disconnect feature.
Destination Host	signalingPropertiesStatusDestinationHost	SIP messages destination.

Mapping Section

Field Name	SNMP Variable	Description
Criteria	mappingTypeStatusCriteria mappingExpressionStatusCriteria	Expression or call property to compare with the call and match in order to apply the properties manipulation.
Transformation	mappingTypeStatusTransformation mappingExpressionStatusTransformation	Call properties to transform and transformation to apply to the call properties.
Sub Mapping	mappingExpressionStatusSubMappings	Name of a subsequent properties manipulation to execute.

Hunt Section

Field Name	SNMP Variable	Description
Name	huntStatusName	Name of the hunt defined by this row.
Destinations	huntStatusDestinations	List of hunt destinations separated by comma.
Selection Algorithm	huntStatusSelectionAlgorithm	Destination selection algorithm.
Timeout	huntStatusTimeout	Maximal time allowed to the destination to handle the call.
Causes	huntStatusCauses	List of call rejection causes to continue the hunt.

SIP Redirects Section

Field Name	SNMP Variable	Description
Name	sipRedirectStatusName	Name of the SIP Redirect defined by this row.
Destination Host	sipRedirectStatusDestination	Host address inserted in the Moved Temporarily response.

Available Interfaces Section

Field Name	SNMP Variable	Description
Index	interfaceStatusIndex	Unique identifier of the row in the table.
Name	interfaceStatusName	Name of the insterface.

Route Configuration Sub-Page

Field Name	SNMP Variable	Description
Apply	ApplyConfig (command)	Applies the call routing configuration.
Rollback	RollbackConfig (command)	Rolls back the current configuration to the running configuration as showed in the status. The current configuration will be lost.

Route Section

Field Name	SNMP Variable	Description
^	routeUp	Moves the current row upside.
v	routeDown	Moves the current row downside.
+	routeInsert routeInsertRoute	Inserts a new row before this row. Inserts a new row at the end of the Route table.
−	routeDelete	Deletes this row.

Configure Route Panel

Field Name	SNMP Variable	Description
Source	routeSourceCriteria	Source criteria to match to apply the route.
Properties Criteria	routePropertiesCriteria	Call properties criteria to match to apply the route.
Expression Criteria	routeExpressionCriteria	Expression criteria to match to apply the route.
Mappings	routeMapping	Name of the properties manipulation to apply to the call if the criteria match.
Signaling Properties	routeSignalingProperties	Name of the signaling properties to apply to the call.
Destination	routeDestination	Destination to apply to the call if the call matches the criteria.
Config Status	routeConfigStatus	Configuration status of the row.

Mapping Type Section

Field Name	SNMP Variable	Description
	mappingTypeUp	Moves the current row upside.
	mappingTypeDown	Moves the current row downside.
	mappingTypeInsert mappingTypeInsertMappingType	Inserts a new row before this row. Inserts a new row at the end of the MappingType table.
	mappingTypeDelete	Deletes this row.

Configure Mapping Type Panel

Field Name	SNMP Variable	Description
Name	mappingTypeName	Name of the the properties manipulation.
Criteria	mappingTypeCriteria	Call properties that the service must compare with the call and match in order to apply the properties manipulation.
Transformation	mappingTypeTransformation	Call properties to transform.
Config Status	mappingTypeConfigStatus	It indicates whether the configuration of the row is valid.

Mapping Expression Section

Field Name	SNMP Variable	Description
	mappingExpressionUp	Moves the current row upside.
	mappingExpressionDown	Moves the current row downside.
	mappingExpressionInsert mappingExpressionInsertMappingExpression	Inserts a new row before this row. Inserts a new row at the end of the MappingExpression table.
	mappingExpressionDelete	Deletes this row.

Configure Mapping Expression Panel

Field Name	SNMP Variable	Description
Name	mappingExpressionName	Name of the properties manipulation.
Criteria	mappingExpressionExpressionCriteria	Expression to compare with the call and match in order to apply the properties manipulation.
Transformation	mappingExpressionTransformation	Transformation to apply to the call properties.

Field Name	SNMP Variable	Description
Sub Mappings	mappingExpressionSubMapping	Name of a subsequent properties manipulation to execute.
Config Status	mappingExpressionConfigStatus	It indicates whether the configuration of the row is valid.

Signaling Properties Section

Field Name	SNMP Variable	Description
	signalingPropertiesUp	Moves the current row upside.
	signalingPropertiesDown	Moves the current row downside.
	signalingPropertiesInsert signalingPropertiesInsertSignalingProperties	Inserts a new row before this row. Inserts a new row at the end of the Signaling Properties table.
	signalingPropertiesDelete	Deletes this row.

Configure Signaling Properties Panel

Field Name	SNMP Variable	Description
Name	signalingPropertiesName	Name of the Signaling properties defined by this row.
Early Connect	signalingPropertiesEarlyConnect	Enables/Disables the early connect feature.
Early Disconnect	signalingPropertiesEarlyDisconnect	Enables/Disables the early disconnect feature.
Destination Host	signalingPropertiesDestinationHost	SIP messages destination.
Allow 180 with SDP	signalingPropertiesAllow180Sdp	Enables/Disables the 180 with SDP allowed.
Allow 183 without SDP	signalingPropertiesAllow183NoSdp	Enables/Disables the 183 without SDP allowed.
Privacy	signalingPropertiesPrivacy	Sets the privacy level of the call.
SIP Headers Translations	signalingPropertiesSipHeadersTranslation	Name of the SIP headers translation to apply to the call.
Call Properties Translations	signalingPropertiesCallPropertiesTranslation	Name of the call properties translation to apply to the call.
Config Status	signalingPropertiesConfigStatus	Configuration status of the row.

SIP Headers Translations Section

Field Name	SNMP Variable	Description
	sipHeadersTranslationUp	Moves the current row upside.
	sipHeadersTranslationDown	Moves the current row downside.
	sipHeadersTranslationInsert sipHeadersTranslation	Inserts a new row before this row. Inserts a new row at the end of the SIP Headers Translation table.
	sipHeadersTranslationDelete	Deletes this row.

Configure SIP Headers Translation Panel

Field Name	SNMP Variable	Description
Name	sipHeadersTranslationName	Name of the SIP headers translation defined by this row.
SIP Header	sipHeadersTranslationSipHeader	Sets which SIP header is modified by this translation.
Built From	sipHeadersTranslationBuiltFrom	Sets what information is used to build the selected SIP header.

Field Name	SNMP Variable	Description
Fix Value	sipHeadersTranslationFixValue	Fix value to be inserted in the SIP header.
Config Status	sipHeadersTranslationConfigStatus	Configuration status of the row.

Call Properties Translations Section

Field Name	SNMP Variable	Description
	callPropertiesTranslationUp	Moves the current row upside.
	callPropertiesTranslationDown	Moves the current row downside.
	callPropertiesTranslationInsert callPropertiesTranslationInsertCallPropertiesTranslation	Inserts a new row before this row. Inserts a new row at the end of the SIP Headers Translation table.
	callPropertiesTranslationDelete	Deletes this row.

Configure Call Properties Translations Panel

Field Name	SNMP Variable	Description
Name	callPropertiesTranslationName	Name of the call properties translation defined by this row.
Call Property	callPropertiesTranslationCallProperty	Sets which call property is modified by this translation.
Built From	callPropertiesTranslationBuiltFrom	Sets what information is used to build the selected call property.
Fix Value	callPropertiesTranslationFixValue	Fix value to be inserted in the call property.
Config Status	callPropertiesTranslationConfigStatus	Configuration status of the row.

Hunt Section

Field Name	SNMP Variable	Description
	huntUp	Moves the current row upside.
	huntDown	Moves the current row downside.
	huntInsert huntInsertHunt	Inserts a new row before this row. Inserts a new row at the end of the Hunt table.
	huntDelete	Deletes this row.

Configure Hunt Panel

Field Name	SNMP Variable	Description
Name	huntName	Name of the hunt defined by this row.
Destinations	huntDestinations	List of hunt destinations separated by comma.
Selection Algorithm	huntSelectionAlgorithm	Destination selection algorithm.
Timeout	huntTimeout	Maximal time allowed to the destination to handle the call.
Causes	huntCauses	List of call rejection causes to continue the hunt.
Config Status	huntConfigStatus	Configuration status of the row.

SIP Redirects Section

Field Name	SNMP Variable	Description
	sipRedirectUp	Moves the current row upside.
	sipRedirectDown	Moves the current row downside.
	sipRedirectInsert sipRedirectInsertSipRedirect	Inserts a new row before this row. Inserts a new row at the end of the SIP Redirects table.
	sipRedirectDelete	Deletes this row.

Configure SIP Redirects Panel

Field Name	SNMP Variable	Description
Name	sipRedirectName	Name of the SIP Redirect defined by this row.
Destination Host	sipRedirectDestinations	Host address to be inserted in the Moved Temporarily response.
Config Status	sipRedirectConfigStatus	Configuration status of the row. It indicates whether the configuration of the row is valid.

Auto-Routing Sub-Page

Field Name	SNMP Variable	Description
Auto-routing	autoRoutingEnable	Enables/Disables the automatic insertion of default routes for selected endpoints.
Criteria Type	autoRoutingCriteriaType	Determines the type of criteria to use to create automatic rule from SIP to the telephony endpoints.
Incoming Mappings	autoRoutingIncomingMappings	Name of the properties manipulations associated with the route from the SIP gateway to the endpoint.
Outgoing Mappings	autoRoutingOutgoingMappings	Name of the properties manipulations associated with the route from the endpoint to the SIP gateway.
Incoming Signaling Properties	autoRoutingIncomingSignalingProperties	Name of the signaling properties associated with the route from the SIP gateway to the endpoint.
Outgoing Signaling Properties	autoRoutingOutgoingSignalingProperties	Name of the signaling properties associated with the route from the endpoint to the SIP gateway.

Endpoints auto-routing section

Field Name	SNMP Variable	Description
Endpoint	autoRoutingEpId	Character string that identifies an endpoint in other tables.
Auto-routable	autoRoutingAutoroutable	Determines whether or not automatic routes are generated for the endpoint when auto-routing is enabled.
Auto-routing Gateway	autoRoutingAutoRoutingGateway	Name of the SIP gateway to use as the destination of outgoing calls and the source of incoming calls when generating auto-routing rules.
E164	autoRoutingE164	The telephone number associated with this endpoint, if any.
SIP Username	autoRoutingSipUsername	The SIP username associated with this endpoint, if any.
Name	autoRoutingName	The FriendlyName associated with this endpoint, if any.

Management Page

Configuration Scripts Sub-Page

Field Name	SNMP Variable	Description
Submit & Export Now	ConfiguredScriptExport (command)	Command to export the configuration script.
Submit & Execute Now	ConfiguredScriptsTransferAndRun (command)	Command to launch the configuration scripts download.

Scripts Status Section

Field Name	SNMP Variable	Description
Current State (Export)	scriptsStatsCurrentTransferState	The current state of the configuration script transfer and execution.
Current State (Execute)	ScriptsStatsCurrentExportState	The current state of the configuration script exportation.
Last Result (Export)	scriptsStatsLastTransferResult	Result of the last configuration scripts transfer command.
Last Result (Execute)	ScriptsStatsLastExportResult	Result of the last configuration script exportation command.
Last Successful (Export)	scriptsStatsLastTransferDateTime	Date and time of the last successful configuration script transfer command.
Last Successful (Execute)	ScriptsStatsLastExportDateTime	Date and time of the last successful configuration script exportation and transfer command since the last reset to default settings.

Export Script Section

Field Name	SNMP Variable	Description
Content	scriptExportContent	Content to export in the generated configuration script.
Service Name	ScriptExportServiceName	Name of the service from which to export configuration.
Send To URL	scriptExportUrl	URL where to send the configuration script exported.
Privacy Key	scriptExportSecretKey	Key used to encrypt the configuration script to export.

Execute Scripts Section

Field Name	SNMP Variable	Description
Generic File Name	scriptGenericFileName	Name of the generic configuration script.
Specific File Name	scriptSpecificFileName	Name of the specific configuration script.
Transfer Protocol	scriptsTransferProtocol	Protocol used to transfer the configuration script files.
Host Name	scriptsTransferSrvHostname	Configuration scripts server hostname and port.
Location	scriptsLocation	Path to the location of the configuration scripts.
User Name	scriptsTransferUsername	User name used to transfer the configuration script.
Password	scriptsTransferPassword	Password used to transfer the configuration script.
Privacy Key	scriptsSecretKey	Key used to decrypt encrypted configuration scripts.
Allow Repeated Execution	scriptsAllowRepeatedExecution	Allows the execution of a script even if it is identical to the last executed script.

Automatically Update Scripts Section

Field Name	SNMP Variable	Description
Update On Restart	scriptsTransferOnRestartEnable	Enables automatic configuration scripts transfer on restart.
Update Periodically	scriptsTransferPeriodicEnable	Enables automatic periodic configuration scripts transfer.

Field Name	SNMP Variable	Description
Time Unit	scriptsTransferPeriodicTimeUnit	Time unit for the variable scriptsTransferInterval.
Period	scriptsTransferInterval	Time interval between automatic configuration scripts transfer.
Time Of Day	scriptsTransferTimeOfDay	Time when the automatic configuration scripts transfer occurs.
DHCP Download Enable	scriptsDhcpDownloadEnable	DHCP Triggered Script Support.

Transfer Scripts Through Web Browser Section

Field Name	SNMP Variable	Description
Upload Parameters	N/A	N/A
Content	scriptExportContent	Content to export in the generated configuration script.
Privacy Key	scriptsSecretKey	Key used to decrypt encrypted configuration scripts.

Backup / Restore Sub-Page

Field Name	SNMP Variable	Description
Submit & Backup Now	ConfiguredBackupImage (command)	Command to launch the configuration backup.
Submit & Restore Now	ConfiguredRestoreImage (command)	Command to launch the configuration restore.

Status Section

Field Name	SNMP Variable	Description
Last Backup Result	imageBackupStatus	Result of the last configuration backup command.
Last Restore Result	imageRestoreStatus	Result of the last configuration restore command.

Image Configuration Section

Field Name	SNMP Variable	Description
File Name	imageFileName	Name of the file used to backup (save) and restore (load) the unit's configuration.
Transfer Protocol	imageTransferProtocol	Protocol used to upload a configuration image during backup and transfer during restore.
Host Name	imageTransferSrvHostname	Configuration backup/restore server hostname and port.
Location	imageLocation	Path to the location of the configuration image file.
User Name	imageTransferUsername	User name used to transfer the configuration image.
Password	imageTransferPassword	Password used to transfer the configuration image.
Content	imageBackupContent	Defines what to include in the backup.
Privacy Algorithm	imagePrivacyAlgo	Enables/disables decryption of the configuration image.
Privacy Key	imageSecretKey	Key used to decrypt or encrypt a configuration image.

Firmware Upgrade Sub-Page

Field Name	SNMP Variable	Description
Submit & Install Now	Install (command)	Command to launch the firmware download.

Status Section

Field Name	SNMP Variable	Description
Firmware Pack Updater Status	status	Indicates the current status of the Firmware Pack Updater.
Last Installation Result	mfpLastInstallationResult	Result of the last install command.
Last Successful Installation	mfpLastInstallationDateTime	Date and time of the last successful install command.

Firmware Packs Installed

Field Name	SNMP Variable	Description
Name	mfpSelectionMfpname	Name of the Firmware Pack to install.
Version	mfpVersion	Version of the MFP to install.
Profile	mfpProfileName	Name of the profile.
Bank	mfpInstalledInfoMfpBank	Bank where the MFP is installed.
Rollback	Rollback (command)	Launches the rollback of the previously installed MFP found in recovery bank.

Firmware Packs Configuration

Field Name	SNMP Variable	Description
Language	languageSelection	Language.
Version	mfpVersion	Version of the MFP to install.
Automatic Restart Enable	automaticRestartEnable	Enables the firmware pack updater to automatically restart the system when needed for completing a firmware update operation.
Automatic Restart Grace Delay	automaticRestartGraceDelay	Configures the grace delay in minutes that the unit waits for all telephony calls to be terminated before the automatic restart can occur.
Firmware Pack 1	mfpSelectionMfpName	Name of the Firmware Pack to install.
Firmware Pack 2	mfpSelectionMfpName	Name of the Firmware Pack to install.
Firmware Pack 3	mfpSelectionMfpName	Name of the Firmware Pack to install.
Firmware Pack 4	mfpSelectionMfpName	Name of the Firmware Pack to install.
Firmware Pack 5	mfpSelectionMfpName	Name of the Firmware Pack to install.

Transfer Configuration

Field Name	SNMP Variable	Description
Location	mfpLocation	Path to the directory containing MFPs.
Transfer Protocol	mfpTransferProtocol	Protocol to use to access the update tree.
User Name	mfpTransferUsername	User name to use to access the update tree.
Password	mfpTransferPassword	Password to use to access the update tree.
Host Name	mfpTransferSrvHostname	Name or IP address and port of the Update Files server.

Certificates Sub-Page

Host Certificates Section

Field Name	SNMP Variable	Description
File Name	hostCertificatesInfoFileName	Name of the certificate file.
Issued To	hostCertificatesInfoIssuedTo	Certificate subject name. This is the common name that must match the host being authenticated.
Issued By	hostCertificatesInfoIssuedBy	Certificate issuer name. This is the certificate authority that signed this certificate.
Valid From	hostCertificatesInfoValidFrom	Certificate lower bound validity duration range.
Valid To	hostCertificatesInfoValidTo	Certificate higher bound validity duration range.
Usage	hostCertificatesAuthenticationUsage	Identifies in which role or context a certificate can be used by the host it authenticates.
	hostCertificatesInfoDelete	Removes the certificate from the unit.

Others Certificates Section

Field Name	SNMP Variable	Description
File Name	othersCertificatesInfoFileName	Name of the certificate file.
Issued To	othersCertificatesInfoIssuedTo	Certificate subject name. This is the common name that must match the host being authenticated.
Issued By	othersCertificatesInfoIssuedBy	Certificate issuer name. This is the certificate authority that signed this certificate.
Valid From	othersCertificatesInfoValidFrom	Certificate lower bound validity duration range.
Valid To	othersCertificatesInfoValidTo	Certificate higher bound validity duration range.
Usage	othersCertificatesAuthenticationUsage	Identifies in which role or context a certificate can be used by the host it authenticates.
CA	othersCertificatesInfoCertificateAuthority	Indicates if the certificate is a CA certificate.
	othersCertificatesInfoDelete	Removes the certificate from the unit.

Host Certificate Associations Section

Field Name	SNMP Variable	Description
File Name	hostCertificateAssociationFileName	Certificate file name.
SIP	hostCertificateAssociationSip	Specifies if this certificate can be used for SIP security.
Web	hostCertificateAssociationWeb	Specifies if this certificate can be used for Web security.
EAP	hostCertificateAssociationEap	Specifies if this certificate can be used for EAP security.

Certificate Authorities Section

Field Name	SNMP Variable	Description
File Name	certificateAuthoritiesFileName	Certificate authority (CA) file name.
Override OCSP URL	certificateAuthoritiesOverrideIssuedCertificateOcspUrl	Defines a specific OCSP URL to use for certificate revocation status of certificates issued by this certificate authority (CA).

SNMP Configuration Section

Field Name	SNMP Variable	Description
SNMP Listening Port	port	Port on which the SNMP service should listen for incoming SNMP requests.
Enable SNMP V1	enableSnmpV1	Specifies if a user can connect to the system by using SNMPv1.
Enable SNMP V2	enableSnmpV2	Specifies if a user can connect to the system by using SNMPv2.
Enable SNMP V3	enableSnmpV3	Specifies if a user can connect to the system by using SNMPv3.
Authentication Protocol	authProtocol	Protocol to use with SNMPv3.
Privacy Protocol	privProtocol	Protocol to use with SNMPv3.
Privacy Password	privPassword	Password to use with SNMPv3 when using DES privacy.
Community	community	String to use for the community field of SNMPv1 and SNMPv2 read-write commands and traps.
Enable SNMP Trap	enableTrap	Specifies if traps can be sent.
Trap Destination	trapDest	Addresses/FQDNs and ports where to send traps.Up to 5 destinations can be specified by using a comma between them. The port numbers are optional.

Access Control Sub-Page

Users Section

Field Name	SNMP Variable	Description
User Name	usersUserName	Contains the user name.
Password	usersPassword	Contains the user's password.
Access Rights	usersAccessRights	Defines the access rights template applying to a user.
+	InsertUser	Inserts a new user in the Users table.
−	Delete (Row Command)	Deletes this row.

Services Access Control Type Section

Field Name	SNMP Variable	Description
Service	servicesAaaTypeService	Service name for which the Aaa types are configured.
Authentication Type	servicesAaaTypeAuthenticationType	Authentication type a service uses for incoming authentication requests.
Accounting Type	servicesAaaTypeAccountingType	Accounting type a service uses once a user is successfully authenticated on the unit.

Radius Servers Section

Field Name	SNMP Variable	Description
Authentication		
Host	radiusServersAuthenticationHost	Hostname and port of a Radius server used for authentication requests.
Server Secret	radiusServersAuthenticationSecret	Secret key shared between the Radius server and the unit.
Accounting		

Field Name	SNMP Variable	Description
Host	radiusServersAccountingHost	Hostname and port of a Radius server used for accounting requests.
Server Secret	radiusServersAccountingSecret	Secret key shared between the Radius server and the unit.
General		
Server Request Timeout	radiusServersTimeoutS	Maximum time, in seconds, the unit waits for a reply from a Radius server.
Radius Users Access Rights	radiusUserAccessRights	Defines the access rights template applying to all Radius users.

File Sub-Page

Internal Files Section

Field Name	SNMP Variable	Description
Name	filesFilename	Relative path and name of the file.
Description	filesFileDescription	Textual description describing the content of the file.
Size	filesFileSize	File size of the associated file.
	filesDelete	Deletes this row.

Misc Sub-Page

System Management Section

Field Name	SNMP Variable	Description
Network Interface	managementInterface	Specifies to which network interface system management services are bound.

APPENDIX

E

Glossary

10 BaseT

An Ethernet local area network that works on twisted pair wiring.

100 BaseT

A newer version of Ethernet that operates at 10 times the speed of a 10 BaseT Ethernet.

Access Device

Device capable of sending or receiving data over a data communications channel.

Accounting

Accounting measures the resources a user consumes during access. This can include the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging of session statistics and usage information and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

A-Law

The ITU-T companding standard used in the conversion between analog and digital signals in PCM (Pulse Code Modulation) systems. A-law is used primarily in European telephone networks and contrasts with the North American mu (μ)-law standard. See also *mu (μ)-law*.

ANI

In CAS signalling, the sending of the calling numbers is known as Automatic Number Identification.

AOC

In ISDN signalling, an Advice Of Charge (AOC-D) message is sent to advise of the current charge (D)uring a call or an AOC-E message is sent to advise of the total charge at the (E)nd of a call.

Area Code

The preliminary digits that a user must dial to be connected to a particular outgoing trunk group or line. In North America, an area code has three digits and is used with a NXX (office code) number. For instance, in the North American telephone number *561-955-1212*, the numbers are defined as follows:

Table 351: North American Numbering Plan

No.	Description
561	Area Code, corresponding to a geographical zone in a non-LNP (Local Number Portability) network.
955	NXX (office code), which corresponds to a specific area such as a city region.
1212	Unique number to reach a specific destination.

Outside North America, the area code may have any number of digits, depending on the national telecommunication regulation of the country. In France, for instance, the numbering terminology is *xZABPQ 12 34*, where:

Table 352: France Numbering Plan

No.	Description
x	Operator forwarding the call. This prefix can be made of 4 digits.
Z	Geographical (regional) zone of the number (in France, there are five zones). It has two digits.
ABPQ	First four digits corresponding to a local zone defined by central offices.
12 34	Unique number to reach a specific destination.

In this context, the area code corresponds to the *Z* portion of the numbering plan. Because virtually every country has a different dialing plan nomenclature, it is recommended to identify the equivalent of an area code for the location of your communication unit.

Authentication

Authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted. The process of authentication is based on each user having a unique set of criteria for gaining access. The AAA server compares a user's authentication credentials with other user credentials stored in a database. If the credentials match, the user is granted access to the network. If the credentials are at variance, authentication fails and network access is denied.

Basic Rate Interface (BRI)

An Integrated Services Digital Network configuration defined in the physical layer standard I.430 produced by the ITU. This configuration consists of two 64 kbit/s “bearer” channels (B channels) and one 16 kbit/s “data” channel (D channel). The B channels are used for voice or user data, and the D channel is used for any combination of: data, control/signalling and X.25 packet networking. The two B channels can be bonded together giving a total data rate of 128 kbit/s. BRI is the kind of ISDN interface most likely to be found in residential service.

Call Routing

Calls through the Aastra can be routed based on a set of routing criteria.

Channel Associated Signalling (CAS)

With this method of signalling, each traffic channel has a dedicated signalling channel. In other words the signalling for a particular traffic circuit is permanently associated with that circuit. Channel-associated call-control is still widely used today mostly in South America, Africa, Australia and in Europe.

Country Code (CC)

In international direct telephone dialing, a code that consists of 1-, 2-, or 3-digit numbers in which the first digit designates the region and succeeding digits, if any, designate the country.

Dialed Number Identification Service (DNIS)

DNIS is a telephone service that identifies for the receiver of a call the number that the caller dialed. It's a common feature of 800 and 900 lines. If you have multiple 800 or 900 numbers to the same destination, DNIS tells which number was called. DNIS works by passing the touch tone digits (dual tone multi frequency or MF digits) to the destination where a special facility can read and display them or make them available for call center programming.

Digital Subscriber Lines (DSL)

A technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines. xDSL refers to different variations of DSL, such as ADSL, HDSL, and RADSL.

Distinguished Encoding Rules (DER)

DER for ASN.1, as defined in ITU-T Recommendation X.509, is a more restrictive encoding standard than the alternative BER (Basic Encoding Rules) for ASN.1, as defined in ITU-T Recommendation X.209, upon which DER is based. Both BER and DER provide a platform-independent method of encoding objects such as certificates and messages for transmission between devices and applications.

Domain Name Server (DNS)

Internet service that translates domain names into IP addresses. For instance, the domain name *www.example.com* might translate to 198.105.232.4.

Dual-Tone Multi-Frequency (DTMF)

In telephone systems, multi-frequency signalling in which a standard set combinations of two specific voice band frequencies, one from a group of four low frequencies and the other from a group of four higher frequencies, are used. Although some military telephones have 16 keys, telephones using DTMF usually have 12 keys. Each key corresponds to a different pair of frequencies. Each pair of frequencies corresponds to one of the ten decimal digits, or to the symbol "#" or "*", the "*" being reserved for special purposes.

Dynamic Host Configuration Protocol (DHCP)

TCP/IP protocol that enables PCs and workstations to get temporary or permanent IP addresses (out of a pool) from centrally-administered servers.

Echo Cancellation

Technique that allows for the isolation and filtering of unwanted signals caused by echoes from the main transmitted signal.

Far End Disconnect

Refers to methods for detecting that a remote party has hung up. This is also known as Hangup Supervision. There are several methods that may be used by a PBX/ACD/CO to signal that the remote party has hung up, including cleardown tone, or a wink.

Federal Communications Commission (FCC)

U.S. government regulatory body for radio, television, interstate telecommunications services, and international services originating in the United States.

Firewall

A firewall in a networked environment prevents some communications forbidden by the security policy. It has the basic task of controlling traffic between different zones of trust. Typical zones of trust include the Internet (a zone with no trust) and an internal network (a zone with high trust).

Foreign Exchange Office (FXO)

A network-provided service in which a telephone in a given local exchange area is connected, via a private line, to a central office in another, i.e., "foreign", exchange, rather than the local exchange area's central office. This is the office end of an FX circuit (frequently a PBX).

Foreign Exchange Service/Station (FXS)

A network-provided service in which a telephone in a given local exchange area is connected, via a private line, to a central office in another, i.e., "foreign", exchange, rather than the local exchange area's central office. This is the station (telephone) end of an FX circuit. An FXS port will provide dial tone and ring voltage.

Full-Duplex Connection

Refers to a transmission using two separate channels for transmission and reception and that can transmit in both ways at the same time. See also *Half-Duplex Connection*.

G.703

ITU-T recommendation for the physical and electrical characteristics of hierarchical digital interfaces at rates up to 140Mbit/s.

G.704

ITU-T recommendation for synchronous frame structures on G.703 interfaces up to 45Mbit/s. The conventional use of G.704 on a 2Mbit/s primary rate circuit provides 30 discrete 64kbit/s channels, with a further 64kbit/s channel available for common channel signalling.

G.711

Algorithm designed to transmit and receive A-law PCM (Pulse Code Modulation) voice at digital bit rates of 48 kbps, 56 kbps, and 64 kbps. It is used for digital telephone sets on digital PBX and ISDN channels.

G.723.1

A codec that provides the greatest compression, 5.3 kbps or 6.3 kbps; typically specified for multimedia applications such as H.323 videoconferencing.

G.726

An implementation of ITU-T G.726 standard for conversion linear or A-law or µ-law PCM to and from a 40, 32, 24 or 16 kbit/s channel.

G.729

A codec that provides near toll quality at a low delay which uses compression to 8 kbps (8:1 compression rate).

Gateway

A device linking two different types of networks that use different protocols (for example, between the packet network and the Public Switched Telephone Network).

Half-Duplex Connection

Refers to a transmission using the same channel for both transmission and reception therefore it can't transmit and receive at the same time. See also *Full-Duplex Connection*.

Hunt Group

The hunt group hunts an incoming call to multiple interfaces. It accepts a call routed to it by a routing table or directly from an interface and creates another call that is offered to one of the configured destination interfaces. If this destination cannot be reached, the hunt group tries another destination until one of the configured destinations accepts the call. When an interface accepts a call, the interface hunting is complete and the hunt group service merges the original call with the new call to the interface that accepted the call.

Impedance

Impedance is the apparent resistance, in an electric circuit, to the flow of an alternating current, analogous to the actual electrical resistance to a direct current, being the ratio of electromotive force to the current.

Information Transfer Capability (ITC)

A request to the network exchange equipment to ask if a particular type of encoding is allowed. It is also called ISDN bearer capability or ISDN service.

Integrated Services Digital Network (ISDN)

A set of digital transmission protocols defined by the international standards body for telecommunications, the ITU-T (formerly called the CCITT). These protocols are accepted as standards by virtually every telecommunications carrier all over the world.

ISDN complements the traditional telephone system so that a single pair of telephone wires is capable of carrying voice and data simultaneously. It is a fully digital network where all devices and applications present themselves in a digital form.

International Telecommunication Union (ITU)

Organization based in Geneva, Switzerland, that is the most important telecom standards-setting body in the world.

Internet-Drafts

Internet-Drafts are working documents of the IETF, its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet Protocol (IP)

A standard describing software that keeps track of the Internet's addresses for different nodes, routes outgoing messages, and recognizes incoming messages.

IP Forwarding

Allows the packet to be forwarded to a specific network based on the packet's criteria (source IP address and source Ethernet link).

Jitter

A distortion caused by the variation of a signal from its references which can cause data transmission errors, particularly at high speeds.

Light Emitting Diode (LED)

A semiconductor diode that emits light when a current is passed through it.

Local Area Network (LAN)

Data-only communications network confined to a limited geographic area, with moderate to high data rates. See also WAN.

Local Firewall

Allows you to dynamically create and configure rules to filter incoming packets with the unit as destination. The traffic is analyzed and filtered by all the rules configured.

Management Information Base (MIB)

Specifications containing definitions of management information so that networked systems can be remotely monitored, configured and controlled.

Media Access Control (MAC) Address

A layer 2 address, 6 bytes long, associated with a particular network device; used to identify devices in a network; also called hardware or physical address.

Mu (μ)-Law

The PCM (Pulse Code Modulation) voice coding and companding standard used in Japan and North America. See also *A-Law*.

Music on Hold (MoH)

Refers to the practice of playing pre-recorded music to fill the silence that would be heard by telephone callers who have been placed on hold. It is especially common in situations involving customer service.

Network

A group of computers, terminals, and other devices and the hardware and software that enable them to exchange data and share resources over short or long distances. A network can consist of any combination of local area networks (LAN) or wide area networks (WAN).

Network Address Translation (NAT)

NAT, also known as network masquerading or IP masquerading, rewrites the source and/or destination addresses/ports of IP packets as they pass through a router or firewall. It is most commonly used to connect multiple computers to the Internet (or any other IP network) by using one IP address. This allows home users and small businesses to cheaply and efficiently connect their network to the Internet. The basic purpose of NAT is to multiplex traffic from the internal network and present it to the Internet as if it was coming from a single computer having only one IP address.

There are two types of NAT rules:

- ***Source rules***: They are applied on the source address of outgoing packets.
- ***Destination rules***: They are applied on the destination address of incoming packets.

Network Firewall

Allows dynamically creating and configuring rules to filter packets forwarded by the unit. Since this is a network firewall, rules only apply to packets forwarded by the unit. The traffic is analyzed and filtered by all the rules configured.

Off-hook

A line condition caused when a telephone handset is removed from its cradle.

On-hook

A line condition caused when a telephone handset is resting in its cradle.

Packet

Includes three principal elements: control information (such as destination, origin, length of packet), data to be transmitted, and error detection. The structure of a packet depends on the protocol.

Plain Old Telephone System (POTS)

Standard telephone service used by most residential locations; basic service supplying standard single line telephones, telephone lines, and access to the public switched network.

Point to Point Protocol over Ethernet (PPPoE)

A proposal specifying how a host personal computer interacts with a broadband modem (i.e., DSL, cable, wireless, etc.) to access the growing number of Highspeed data networks. Relying on two widely accepted standards, Ethernet and the point-to-point protocol (PPP), the PPPoE implementation requires virtually no more knowledge on the part of the end user other than that required for standard Dialup Internet access. In addition, PPPoE requires no major changes in the operational model for Internet Service Providers (ISPs) and carriers. The base protocol is defined in RFC 2516.

Port

Network access point, the identifier used to distinguish among multiple simultaneous connections to a host.

Portable Operating System Interface (POSIX)

POSIX is a set of standard operating system interfaces based on the UNIX operating system. The need for standardization arose because enterprises using computers wanted to be able to develop programs that could be moved among different manufacturer's computer systems without having to be recoded.

Primary Rate Interface (PRI)

A telecommunications standard for carrying multiple DS0 voice and data transmissions between two physical locations. All data and voice channels are (ISDN) and operate at 64 kbit/s.

North America and Japan use a T1 of 23 B channels and one D channel which corresponds to a T1 line. Europe, Australia and most of the rest of the world use the slightly higher capacity E1, which is composed of 31 B channels and one D channel.

Fewer active B channels (also called user channels) can be used for a fractional T1. More channels can be used with more T1's, or with a fractional or full T3 or E3.

Presentation Indicator (PI)

An information element (IE) field that determines whether a caller's CLI can be displayed on a Caller ID device or otherwise presented to the called party.

Private Branch Exchange (PBX)

A small to medium sized telephone system and switch that provides communications between onsite telephones and exterior communications networks.

Protocol

A formal set of rules developed by international standards bodies, LAN equipment vendors, or groups governing the format, control, and timing of network communications. A set of conventions dealing with transmissions between two systems. Typically defines how to implement a group of services in one or two layers of the OSI reference model. Protocols can describe low-level details of machine-to-machine interfaces or high-level exchanges between allocation programs.

Proxy Server

An intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them on, possibly after translation, to other servers. A proxy interprets, and, if necessary, rewrites a request message before forwarding it.

Public Switched Telephone Network (PSTN)

The local telephone company network that carries voice data over analog telephone lines.

QSIG

QSIG is an ISDN based signaling protocol for signaling between private branch exchanges (PBXs) in a Private Integrated Services Network (PISN). It makes use of the connection-level Q.931 protocol and the application-level ROSE protocol. ISDN "proper" functions as the physical link layer.

Quality of Service (QoS)

Measure of the telephone service quality provided to a subscriber. This could be, for example, the longest time someone should wait after picking up the handset before they receive dial tone (three seconds in most U.S. states).

Real Time Control Protocol (RTCP)

RTCP is the control protocol designed to work in conjunction with RTP. It is standardized in RFC 1889 and 1890. In an RTP session, participants periodically send RTCP packets to convey feedback on quality of data delivery and information of membership.

Realtime Transport Protocol (RTP)

An IETF standard for streaming realtime multimedia over IP in packets. Supports transport of real-time data like interactive voice and video over packet switched networks.

Registrar Server

A server that accepts REGISTER requests. A registrar is typically co-located with a proxy or redirect server and MAY offer location services.

Request for Comment (RFC)

A formal document from the IIETF that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final version of the RFC becomes the standard and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs that supersede or elaborate on all or parts of previous RFCs.

Screening Indicator (SI)

A service provided by ISDN that can be used to test the trustworthiness of the calling party's number. This signalling-related information element is found in octet 3a of the ISDN SETUP message.

Server

A computer or device on a network that works in conjunction with a client to perform some operation.

Session Description Protocol (SDP)

Describes multimedia sessions for the purpose of session announcement, session invitation and other forms of multimedia session initiation. SDP communicates the existence of a session and conveys sufficient information to enable participation in the session. SDP is described in RFC 2327.

Session Initiation Protocol (SIP)

A protocol for transporting call setup, routing, authentication, and other feature messages to endpoints within the IP domain, whether those messages originate from outside the IP cloud over SCN resources or within the cloud.

Simple Network Management Protocol (SNMP)

A standard of network management that uses a common software agent to manage local and wide area network equipment from different vendors; part of the Transmission Control Protocol / Internet Protocol (TCP/IP) suite and defined in RFC 1157.

Simple Network Time Protocol (SNTP)

SNTP, which is an adaptation of the Network Time Protocol (NTP), is widely used to synchronize computer clocks in the global Internet. It provides comprehensive mechanisms to access national time and frequency dissemination services, organize the time-synchronization subnet and adjust the local clock in each participating subnet peer. In most places of the Internet of today, NTP provides accuracies of 1-50 ms, depending on the characteristics of the synchronization source and network paths.

Subnet

An efficient means of splitting packets into two fields to separate packets for local destinations from packets for remote destinations in TCP/IP networks.

Switched Circuit Network (SCN)

A communication network, such as the public switched telephone network (PSTN), in which any user may be connected to any other user through the use of message, circuit, or packet switching and control devices.

T.38

An ITU-T Recommendation for Real-time fax over IP. T.38 addresses IP fax transmissions for IP-enabled fax devices and fax gateways, defining the translation of T.30 fax signals and Internet Fax Protocols (IFP) packets.

Telephony

The science of translating sound into electrical signals, transmitting them, and then converting them back into sound.

Transmission Control Protocol/Internet Protocol (TCP/IP)

The basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet).

Trivial File Transfer Protocol (TFTP)

A simplified version of FTP that transfers files but does not provide password protection, directory capability, or allow transmission of multiple files with one command.

User Datagram Protocol (UDP)

An efficient but unreliable, connectionless protocol that is layered over IP, as is TCP. Application programs are needed to supplement the protocol to provide error processing and retransmission of data. UDP is an OSI layer 4 protocol.

Virtual LAN (VLAN)

A network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. One of the biggest advantages of VLANs is that when a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration.

Virtual Private Network (VPN)

A private communications network usually used within a company, or by several different companies or organizations, to communicate over a public network. VPN message traffic is carried on public networking infrastructure (e.g. the Internet) using standard (often insecure) protocols, or over a service provider's network providing VPN service guarded by well defined Service Level Agreement (SLA) between the VPN customer and the VPN service provider.

Voice Over IP (VoIP)

The technology used to transmit voice conversations over a data network using the Internet Protocol. Such data network may be the Internet or a corporate Intranet.

Wide Area Network (WAN)

A large (geographically dispersed) network, usually constructed with serial lines, that covers a large geographic area. A WAN connects LANs using transmission lines provided by a common carrier.

APPENDIX

F

List of Acronyms

AC	Access Concentrator
AES	Advanced Encryption Standard
ANI	Automatic Number Identification
BRI	Basic Rate Interface
CA	Certification Authority
CAS	Channel Associated Signalling
CCBS	Completion of Calls to Busy Subscriber
CCNR	Completion of Calls on No Reply
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface
CLIP	Calling Line Information Presentation
CLIR	Calling Line Information Restriction
CNG	Comfort Noise Generator
COLP	Connected Line Identification Presentation
COLR	Connected Line Identification Restriction
CS-ACELP	Conjugate Structure-Algebraic Code Excited Linear Prediction
DER	Distinguished Encoding Rules
DNIS	Dialed Number Identification Service
DNS	Domain Name Server
DSCP	Differentiated Services Code Point
DSS1	Digital Subscriber Signaling System No.1
DST	Daylight Saving Time
DTMF	Dual Tone Multi-Frequency
FQDN	Fully Qualified Domain Name
FSK	Frequency Shift Keying
GMT	Greenwich Mean Time
HTML	Hyper Text Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HTTP over the Transport Layer Security
Hz	Hertz
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical & Electronics Engineers
IETF	Internet Engineering Task Force
ISDN	Integrated Services Digital Network
ITC	Information Transfer Capability
ITU	International Telecommunication Union
kbps	KiloBits Per Second
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Media Access Control
MFC	Multi-Frequency Code

MIB	Management Information Base
MIKEY	Multimedia Internet KEYing
MSN	Multiple Subscriber Number
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NBNS	NetBIOS Name Server
NPI	Numbering Plan Indicator
NT	Network Termination
NTP	Network Time Protocol
PAP	Password Authentication Protocol.
PBX	Private Branch eXchange
PEM	Privacy Enhanced Mail
PI	Presentation Indicator
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PRACk	Provisional Response Acknowledgement
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RFC 3711 - The Secure Real-time Transport Protocol (SRTP)	
RFC	Request For Comment
RTCP	Real Time Control Protocol
SCN	Switched Circuit Network
SDES	Secure Description
SDP	Session Description Protocol
SHA	Secure Hash Algorithm
SI	Screening Indicator
SIP	Session Initiation Protocol
SNTP	Simple Network Time Protocol
SRTCP	Secure Real-Time Transport Control Protocol
SRTP	Secure Real-Time Transport Protocol
SSH	Secure Socket Shell
SSL	Secure Sockets Layer
STD	Standard Saving Time
STP	Spanning Tree Protocol
TBRL	Terminal Balance Return Loss
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TE	Terminal Equipment
TEI	Terminal Endpoint Identifier
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TON	Type of Number
UDP	User Datagram Protocol
UMN	Unit Manager Network
UNI	User-Network Interface
URI	Uniform Resource Identifier
UTC	Universal Time Coordinated
VAD	Voice Activity Detector
VLAN	Virtual Local Area Network
WAN	Wide Area Network

WINS	Windows Internet Name Service

APPENDIX

G

List of Standards Supported

RFC 2131 - Dynamic Host Configuration Protocol 107, 147
RFC 2132 - DHCP Options and BOOTP Vendor Extensions 107, 147
RFC 2181 - Clarifications to the DNS Specification 90
RFC 2246 - The TLS Protocol Version 1.0 .... 303, 520, 536, 545
RFC 2459 - X.509 Digital Certificates 520, 536, 545
RFC 2460 - IPv6 98
RFC 2464 - Transmission of IPv6 Packets over Ethernet Networks 98
RFC 2475 - An Architecture for Differentiated Services 113
RFC 2516 - A Method for Transmitting PPP Over Ethernet (PPPoE) 103
RFC 2543 - SIP, Session Initiation Protocol 279, 285, 287, 319
RFC 2576 - Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework 559
RFC 2616 - Hypertext Transfer Protocol - HTTP/1.1 .... 41, 441, 519, 535, 543
RFC 2617 - HTTP Authentication - Basic and Digest Access Authentication 519, 535, 543, 583
RFC 2705 - Media Gateway Control Protocol (MGCP) Version 1.0 395
RFC 2741 - Agent Extensibility (AgentX) Protocol Version 1 559
RFC 2818 - HTTP Over TLS 520, 536, 545
RFC 2833 - RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals 354
RFC 2865 - Remote Authentication Dial In User Service (RADIUS) 583
RFC 2866 - RADIUS Accounting 583
RFC 2976 - The SIP INFO Method 411
RFC 3164 - The BSD Syslog Protocol 71
RFC 3261 - SIP, Session Initiation Protocol 279, 285, 287, 299, 303, 310, 318
RFC 3262 - Reliability of Provisional Responses in the Session Initiation Protocol (SIP) 340
RFC 3263 - Session Initiation Protocol (SIP) - Locating SIP Servers 324
RFC 3264 - An Offer/Answer Model with the Session Description Protocol (SDP) 309, 312, 318, 319, 321, 322
RFC 3265 - Session Initiation Protocol (SIP)-Specific Event Notification 432
RFC 3268 - Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS) 520, 536, 545
RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile ..... 520, 536, 545, ... 553
RFC 3311 - The Session Initiation Protocol (SIP) UPDATE Method 340
RFC 3315 - DHCPv6 107
RFC 3323 - A Privacy Mechanism for the Session Initiation Protocol (SIP) 488
RFC 3325 - Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks .. 488
RFC 3398 - Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping 332
RFC 3411 - An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks 559
RFC 3412 - Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) 559
RFC 3413 - Simple Network Management Protocol (SNMP) Applications 559
RFC 3414 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) 559
RFC 3415 - View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) 559
RFC 3416 - Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) 559
RFC 3417 - Transport Mappings for the Simple Network Management Protocol (SNMP) 559
RFC 3442 - The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4 129
RFC 3515 - The Session Initiation Protocol (SIP) Refer Method 309
RFC 3550 - RTP - A Transport Protocol for Real-Time Applications 349
RFC 3551 - RTP Profile for Audio and Video Conferences with Minimal Control 349
RFC 3617 - Uniform Resource Identifier (URI) Scheme for the Trivial File Transfer Protocol 519, 535, 543
RFC 3711 - The Secure Real-time Transport Protocol (SRTP) 373
RFC 3826 - The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model 559
RFC 3830 - MIKEY - Multimedia Internet KEYing 373
RFC 3842 - The Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP) 432
RFC 3863 - Presence Information Data Format (PIDF) 287
RFC 3903 - Session Initiation Protocol (SIP) Extension for Event State Publication 279, 287
RFC 4040 - RTP Payload Format for a 64 kbit/s Transparent Call 352, 353
RFC 4193 - Unique_local_address 98
RFC 4235 - An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP) 414
RFC 4251 - The Secure Shell (SSH) Protocol Architecture 22
RFC 4291 - IP Version 6 Addressing Architecture 98
RFC 4443 - ICMPv6 98
RFC 4567 - Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP) 373
RFC 4568 - SDES - Security Descriptions for Media Streams 373
RFC 4579 - Session Initiation Protocol (SIP) - Call Control - Conferencing for User Agents 425
RFC 4861 - IPv6_neighbor_discovery 98
RFC 4862 - IPv6_stateless_autoconf 98

T

B

D

E

I

R

T

Index

Numerics

A

B

C

D

E

F

J

K

O

P

Q

R

T