



media5
corporation
Discover the Power of 5

Software Configuration Guide

Dgw v2.0 Application

Document Revision 51

September 26, 2016

Dgw v2.0 Application Software Configuration Guide

© 2016, Media5 Corporation

All rights reserved. No part of this publication may be reproduced or used in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the express written permission of the publisher.

Media5 Corporation reserves the right to revise this publication and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes.

Trademarks

Microsoft and Windows are registered trademarks of Microsoft Corporation.

Adobe and Acrobat are registered trademarks of Adobe Systems Incorporated.

All other trademarks and registered trademarks are the property of their respective owners.

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 available on the Mediatrix Download Portal, which lists the third-party software modules along with any copyright and license information.

Contents

Preface

About this Manual	xix
Intended Audience	xix
Related Documentation	xix
Document Conventions	xx
Warning Definition	xx
Other Conventions	xx
SCN vs. PSTN.....	xx
Supported Standards	xx
Naming Conventions	xxi

Chapter 1

Information Important to Know.....	1
Introduction	1
Bypass Feature (Mediatrix 4100 Series)	1
Management Choices	2
RESET/DEFAULT Button	4
User Access.....	4
Secure Password Policies.....	5

Chapter 2

Command Line Interface (CLI)	7
Introduction	7
Configuring the CLI.....	7
Partial Reset.....	8
Accessing the CLI	8
Accessing the CLI through the Serial Console Port (Mediatrix 3000 Series only)	8
Accessing the CLI via a Telnet Session	9
Accessing the CLI via a SSH Session.....	10
Working in the CLI	11

Chapter 3

Web Interface Configuration	13
Introduction	13
Tls Version Settings	15
.....	16
HTTP User-Agent Header Format.....	16
Using the Web Interface	18
Submitting Changes	19

System Parameters

Chapter 4

Services	23
Services Table	23
Graceful Restart of Services	26
Restarting a Service via MIB	26

Chapter 5

Hardware Parameters	29
----------------------------------	-----------

Chapter 6

Endpoints State Configuration	31
Unit Configuration	31
Endpoints Configuration	31
Administration	32
Unit Shutting Down Behaviour	33

Chapter 7

Syslog Configuration	35
Syslog Daemon Configuration	35
Configuring PCM Capture	38
Configuring the Syslog Daemon Application	38

Chapter 8

Events Configuration	39
Notification Events	39
Deleting a Rule	41
Monitoring Parameters	41

Chapter 9

Local Log	43
Local Log Status and Entries	43

Chapter 10

VM.....	45
---------	----

Network Parameters

Chapter 11

IPv4 vs. IPv6	49
Introduction	49
IPv4 vs. IPv6 Availability	49
IPv6 Scope Identifier	50
When Contacting the unit using its IPv6 link-local Address	50
When Configuring the Mediatrix unit to use an IPv6 link-local Address	50

Chapter 12

Host Parameters	53
General Configuration	53
Host Configuration	53
Default Gateway Configuration	55
DNS Configuration	56
SNTP Configuration	57
Time Configuration	58
STD / DST	59
OFFSET	59
START / END	59
Example	59
Additional Parameters	60
Configuring DNS Records Randomization	60
Configuring Pre-resolved Static FQDNs	61
Updating the "sysname" or "syslocation"	61

Chapter 13

Interface Parameters	63
Reserving an IP Address	63
Link Connectivity Detection	63
Partial Reset	63
Interfaces Configuration	64
IPv6 Autoconfiguration Interfaces	67
Network Interface Priority	68
Rescue Interface Configuration	68
PPPoE Configuration	69
PPP Negotiation	70
DHCP Client Identifier Presentation	70
LLDP Configuration	71
Ethernet Link Configuration	72
EAP 802.1x Configuration	73
DHCP Server Configuration	73

DHCP Negotiation	74
Ethernet Connection Speed.....	75
Speed and Duplex Detection Issues	76

Chapter 14

VLAN Parameters	77
------------------------------	-----------

Chapter 15

Local QoS (Quality of Service) Configuration	79
Introduction	79
Differentiated Services (DS) Field	79
IEEE 802.1q.....	81
Specific Service Class Configuration.....	81
Network Traffic Control Configuration.....	82

Chapter 16

Local Firewall Configuration	85
Managing the Local Firewall	85
Partial Reset.....	85
Setting the Default Policy	85
Creating/Editing a Firewall Rule	86
Moving a Firewall Rule	88
Deleting a Firewall Rule	89
Disabling the Local Firewall	89

Chapter 17

IP Routing Configuration	91
Managing IP Routing	91
IPv4 Forwarding	91
Creating/Editing an IP Routing Rule.....	92
Moving an IP Routing Rule.....	93
Deleting an IP Routing Rule	93
Static IPv4 Routes.....	94
DHCPv4 Classless Static Route Option	95
DHCPv4 User Class Route Option.....	95
Network Configuration Examples	96
Forward Packets from the Lan1 Network to the Uplink Network with NAT	96
Configure Port Forwarding for a Web Server Located on the LAN	96

Chapter 18

Network Firewall Configuration	99
Managing the Network Firewall	99
Setting the Default Policy	99
Creating/Editing a Network Firewall Rule.....	100
Moving a Network Firewall Rule.....	103
Deleting a Network Firewall Rule	103
Disabling the Network Firewall	103

Chapter 19

NAT Configuration	105
Introduction	105
Partial Reset	105
Creating/Editing a Source NAT Rule	105
Creating/Editing a Destination NAT Rule	109
Moving a NAT Rule	112
Deleting a NAT Rule	112
Disabling the NAT	112

Chapter 20

DHCP Server Settings	113
Introduction	113
Subnet Server	113
Leases	113
Configuration Parameters	113
Default vs. Specific Configurations	114
DHCP Basic Configuration	115
Lease Time (Option 51)	115
Domain Name (Option 15)	116
Default Gateway (Option 3)	116
DNS (Option 6)	117
NTP (Option 42)	118
NBNS (Option 44)	119
DHCP Static Leases Configuration	120

SBC Parameters

Chapter 21

SBC Configuration	123
--------------------------------	------------

POTS Parameters

Chapter 22

POTS Configuration	127
POTS Status	127
Line Status	127
FXO Line Status	128
General POTS Configuration	128
Caller ID Information	130
FXS Configuration	131
FXS Country Customization	133
Calling Party Name of the Caller ID	134

FXS Bypass	135
FXS Emergency Call Override	136
FXS Distinctive Ring	137
FXO Configuration	139
FXO Dialing Configuration	139
FXO Answering Configuration	140
FXO Incoming Call Configuration	142
FXO Custom Basic Parameters	142
FXO Line Verification	143
FXO Force End of Call	144

ISDN Parameters

Chapter 23

ISDN Configuration	149
Introduction	149
ISDN Reference Points	149
Inband Tones Generation	150
Setting PRI Hardware Parameters	151
ISDN Auto-Configuration	152
Preset	153
Partial Reset	153
PRI ISDN Statistics	153
PRI Configuration	155
InformationFollowing Operation	166
BRI Configuration	167
Bypass Feature (Mediatrix 3404/3408/3734/3741/3742 Models)	177
Bypass Feature (Mediatrix 4402plus / 4404plus Models)	177
Interop Parameters Configuration	178
Play Local Ringback when no Media Stream	180
ISDN Timers Configuration	182
Services Configuration	183

R2 CAS Parameters

Chapter 24

R2 CAS Configuration	191
Introduction	191
Line Signals for the Digital Version of MFC/R2	191
Interregister Signals	191
Selecting the R2 Signaling Protocol	192
R2 Auto-Configuration	193
Preset	193
Partial Reset	194
R2 Channel Associated Signaling	194
R2 Signaling Variants	198
Override Default Country Settings	199

R2 Signaling Variants	199
R2 Timers Variants	202
Override Default Country Settings	203
R2 Timers Variants	204
R2 Digit Timers Variants	207
Override Default Country Settings	207
R2 Digit Timers Variants	208
R2 Link Timers Variants	209
Override Default Country Settings	209
R2 Link Timers Variants	210
R2 Tones Variants	210
Override Default Country Settings	212
R2 Tones Forward Groups	213
R2 Tones Backward Groups	214
PRI R2 CAS Statistics	218

E&M CAS Parameters

Chapter 25

E&M CAS Configuration	223
Introduction	223
Line Signals for the Digital Version of E&M	223
Selecting the E&M Signalling Protocol	223
E&M Auto-Configuration	224
Preset	225
Partial Reset	226
E&M Channel Associated Signaling	226
E&M Signalling Variants	229
Override Default Signaling Settings	229
E&M Signalling Variants	230
E&M Timers Variants	232
Override Default Signaling Settings	233
E&M Timers Variants	233
E&M Digit Timers Variants	234
Override Default Signaling Settings	235
E&M Digit Timers Variants	235
E&M Link Timers Variants	236
Override Default Signalling Settings	236
E&M Link Timers Variants	237
E&M Tones Variants	237
Override Default Signalling Settings	237
E&M Tones Variants	238
PRI E&M Statistics	239

SIP Parameters

Chapter 26

SIP Gateways.....	243
SIP Gateways Configuration.....	243

Chapter 27

SIP Servers	247
Introduction	247
TLS Persistent Connections Status	248
SIP Servers Configuration	248
Multiple SIP Gateways.....	249
SIP Gateway Specific Registrar Servers.....	249
SIP Gateway Specific Messaging Servers.....	250
SIP Gateway Specific Proxy Servers	251
Keep Alive	251
SIP Gateway Specific Keep Alive Destinations.....	253
Outbound Proxy Loose Router Configuration.....	253

Chapter 28

SIP Registration.....	255
Endpoints Registration.....	255
Contact Domain.....	256
Accept Language	257
Unit Registration	257
Registration Configuration	258
Number of Registrations	259
Additional Registration Refresh Parameters.....	260
Default Registration Retry Time	260
Default vs. Specific Configurations.....	260
Registration Refresh.....	261
Registration Expiration	261
Expiration Value in Registration	261
Gateway Specific Registration Retry Time.....	262
Unregistered Endpoint Behaviour	262
Unregistered Unit Behaviour	263
Behaviour on Initial-Registration Reception	264
Registration Delay Value.....	265
SIP User Agent Header	265

Chapter 29

SIP Authentication	267
Authentication Configuration.....	267
Creating/Editing an Authentication Entry.....	268
Moving an Authentication Entry.....	270

Deleting an Authentication Entry	270
--	-----

Chapter 30

SIP Transport Parameters 271

SIP Transport Type.....	271
Additional Transport Parameters	273
Transport TLS Cipher Suite Settings.....	273
Transport Tls Version Settings	274
.....	275
UDP Source Port Behaviour.....	275
TLS Client Authentication.....	276
Force DNS NAPTR In TLS.....	276
SIP Failover Conditions.....	277
Persistent Port Interval.....	278

Chapter 31

Interop Parameters..... 279

Behavior on T.38 INVITE Not Accepted	279
SIP Interop.....	279
SDP Interop	282
TLS Interop	286
Misc Interop	287
Additional Interop Parameters	288
Call Waiting Private Number Criteria for SIP INFO	288
Max-Forwards Header.....	288
Direction Attributes in a Media Stream.....	289
Local Ring Behaviour on Provisional Response	292
Session ID and Session Version Number in the Origin Field of the SDP.....	293
Register Home Domain Override	294
DNS SRV Record Lock	294
Listening for Early RTP	294
Resolve Route Header.....	295
ACK Branch Matching.....	296
Ignore Require Header.....	296
Reject Code for Unsupported SDP Offer	297
SIP User-Agent Header Format	297
SIP INFO Without Content Answer	298
Keep Alive Option Format	298
Unsupported Content-Type	299

Chapter 32

Miscellaneous SIP Parameters 301

SIP Penalty Box.....	301
Penalty Box vs Transport Types	301
Penalty Box Configuration.....	302
Error Mapping	302
SIP to Cause Error Mapping	304
Cause to SIP Error Mapping	306
Additional Headers	309
PRACK	310
Forked Provisional Responses Behaviour	311

Session Refresh	311
Background Information	312
SIP Gateway Configuration	313
SIP Blind Transfer Method.....	314
Diversion Configuration	314
DNS Configuration.....	315
Event Handling Configuration	315
Messaging Subscription.....	317
Advice of Charge Configuration.....	317
Additional DNS Parameters.....	318
DNS Failure Concealment.....	318

Media Parameters

Chapter 33

Voice & Fax Codecs Configuration	321
Codec Descriptions.....	321
G.711 A-Law and μ -Law.....	321
G.723.1.....	322
G.726.....	322
G.729.....	322
Clear Mode.....	323
Clear Channel	323
X-CCD Clear Channel	324
T.38	324
Codec Parameters.....	325
Codec vs. Bearer Capabilities Mapping.....	326
Generic Voice Activity Detection (VAD).....	328
G.711 Codec Parameters	328
G.723 Codec Parameters	330
G.726 Codecs Parameters	331
G.729 Codec Parameters	333
Clear Mode Codec Parameters	334
Clear Channel Codec Parameters.....	335
X-CCD Clear Channel Codec Parameters	337
Fax Parameters	338
Clear Channel Fax	339
T.38 Fax	339
T.38 Parameters Configuration	340
Data Codec Selection Procedure	342

Chapter 34

Security	345
Introduction	345
Security Parameters	345
Enforcing Symmetric RTP	347

Chapter 35

RTP Statistics Configuration.....	349
Statistics Displayed.....	349
Statistics Configuration	351
Channel Statistics	352

Chapter 36

Miscellaneous Media Parameters	355
Jitter Buffer Configuration	355
About Changing Jitter Buffer Values	357
Starting a Call in Voiceband Data Mode	358
DTMF Transport Configuration	358
DTMF Transport over the SIP Protocol	360
DTMF Detection	360
Using the Payload Type Found in the Answer	363
Quantity of initial packets sent to transmit a DTMF Out-of-Band using RTP	363
Machine Detection Configuration.....	364
Base Ports Configuration.....	365

Telephony Parameters

Chapter 37

DTMF Maps Configuration.....	369
Introduction	369
Syntax.....	369
Special Characters	370
How to Use a DTMF Map	370
General DTMF Maps Parameters.....	372
Configuring Timeouts per Endpoint.....	373
Allowed DTMF Maps	373
Refused DTMF Maps.....	375

Chapter 38

Call Forward Configuration	377
Call Forward On Busy.....	377
Configuring Call Forward on Busy via Handset.....	379
Call Forward On No Answer	380
Configuring Call Forward on Answer via Handset.....	381
Call Forward Unconditional.....	382
Configuring Call Forward on Unconditional via Handset.....	383

Chapter 39

Telephony Services Configuration	385
General Configuration	385
Automatic Call	387
Call Completion	387
Call Transfer	391
Call Waiting	393
Conference	397
Delayed Hot Line	401
Direct IP Address Call	402
Call Hold	403
Second Call	404
Message Waiting Indicator	405
Visual Message Waiting Indicator Type	407
Distinctive Call Waiting Tone	407
Call Statistics	408
Default Outbound Priority Call Routing	409

Chapter 40

Tone Customization Parameters Configuration	411
Current Tone Definition	411
Tone Override	412

Chapter 41

Music on Hold Parameters Configuration	415
MP3 File Download Server	415
Configuring the TFTP Server	415
Configuring the HTTP Server	415
Music on Hold Configuration	415

Chapter 42

Country Parameters Configuration	419
Country Configuration	419
Additional Country Settings	421
Default vs. Specific Configurations	421
Input/Output User Gain	421
Dialing Settings	422
Fax Calling Tone Detection	424

Chapter 43

Call Detail Record	425
CDR (Call Detail Record)	425

Call Router Parameters

Chapter 44

Call Router Configuration.....	431
Introduction	431
Limitations	432
Regular Expressions	432
Routing Type	434
Call Properties Parameters	440
SIP/ISDN Call Default Values	447
Call Routing Status.....	448
Routes	449
Creating/Editing a Route	450
Moving a Route	454
Deleting a Route.....	455
Mappings	455
Creating/Editing a Mapping Type	455
Creating/Editing a Mapping Expression	457
Moving a Mapping Type or Expression Row	464
Deleting a Mapping Type or Expression Row	464
Signalling Properties	465
Creating/Editing a Signalling Property.....	465
Moving a Signalling Property Row	469
Deleting a Signalling Property Row	469
SIP Headers Translations	469
Creating/Editing a SIP Headers Translation.....	469
Moving a SIP Headers Translation Row	471
Deleting a SIP Headers Translation Row	471
Call Properties Translations.....	472
Creating/Editing a Call Properties Translation	472
Moving a Call Properties Translation Row	474
Deleting a Call Properties Translation Row.....	474
Hunt Service	475
Creating/Editing a Hunt	475
Call Rejection (Drop) Causes	478
Moving a Hunt	482
Deleting a Hunt.....	482
SIP Redirects	483
Creating/Editing a SIP Redirect.....	483
Moving a SIP Redirect.....	484
Deleting a SIP Redirect	484
Hairpinning.....	485
Configuration Examples.....	485

Chapter 45

Auto-Routing Configuration.....	487
Auto-Routing	487
Endpoints Auto-Routing	488
Manual Routing	490

Management Parameters

Chapter 46

Configuration Script.....	495
----------------------------------	------------

Chapter 47

Configuration Backup/Restore	497
---	------------

Chapter 48

Firmware Download	499
--------------------------------	------------

Chapter 49

Certificates Management.....	501
Introduction	501
HTTPS Transfer Cipher Suite Settings	502
HTTPS Transfer Tls Version Settings	503
.....	504
Managing Certificates	504
Certificate Authorities.....	505
Certificate Upload through the Web Browser	506
Transferring a Certificate via Configuration Script.....	506
Host Certificate Associations	507

Chapter 50

SNMP Configuration	509
Introduction	509
SNMP Configuration Section	509
Partial Reset.....	513
SNMP Statistics	514

Chapter 51

CWMP Configuration	515
Introduction	515
Licence Key Activation of TR-069	515
CWMP Configuration Section	516
General Configuration	516
ACS Configuration.....	517
ACS Configuration Parameters	520
Periodic Inform Configuration	521
TR-069 Configuration	523
TR-104 Configuration	524
TR-106 Configuration	525

TR-111 Configuration	526
Transport HTTPS Cipher Suite Settings	528
HTTPS Transport Tls Version Settings	530
.....	531
Transport Certificate Validation	531
Allow Unauthenticated UDP Connection Requests	532
Parameter Type Validation	533
MAC Address Format	533
ACS Access to the Local Log Table	534
Supported TR-069 Methods and Parameters	535

Chapter 52

Access Control Configuration	537
Users	537
Partial Reset	538
Services Access Control Type	538
Partial Reset	539
Radius Servers	539
Access Rights Description	541

Chapter 53

File Manager	543
File Manager	543
Partial Reset	545
Transfer Protocols	546
Security Certificates	546
HTTPS Transfer Settings	546
HTTPS Transfer Cipher Suite Settings	546
HTTPS Transfer Tls Version Settings	548
.....	549

Chapter 54

Miscellaneous	551
Management Interface Configuration	551
Activate Licence	552

P R E F A C E



About this Manual

Thank you for purchasing one or more Mediatrix units supporting the Dgw v2.0 application. The Dgw v2.0 application runs on several Mediatrix devices. Provider-specific profiles ensure that the Mediatrix unit is a genuine plug and play solution. It offers a low total cost of ownership as it reduces installation and maintenance costs.

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 Mediatrix unit.
- ▶ System administrators with a basic networking background and experience, but who might not be familiar with the Mediatrix unit.
- ▶ Operators.
- ▶ Installers.
- ▶ Maintenance technicians.

Related Documentation

In addition to this manual, the Mediatrix unit documentation, available at <http://www.media5corp.com/documentation> set includes the following:

- ▶ *Hardware Installation Guides* for each specific Mediatrix unit to install the hardware of your specific Mediatrix unit.
- ▶ *Quick Starts* for each specific Mediatrix unit to quickly setup and work with the Mediatrix unit.
- ▶ *The DGW v2.0 Reference Guide* providing the complete description of:
 - Parameters, tables, commands and available Country Specifications
 - Error messages
 - Notification messages
 - Country Tone Definitions
- ▶ *Third Party Software Copyright Information* listing the third-party software modules used in the Mediatrix unit along with any copyright and license information.
- ▶ *Configuration Notes* providing specific hands-on configuration scenarios.
- ▶ *Technical Bulletins* providing information on a specific use of the DGW v2.0 software.
- ▶ *Release notes*

Supported Standards providing information of the RFCs (Request for Comments) standards, Internet-Drafts, or other standard documents the Dgw v2.0 application is **based** on. This document is available upon request from our technical support team. Therefore, it is 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>.

Document Conventions

The following information provides an explanation of the symbols that appear on the Mediatrix 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 the Mediatrix unit *Hardware Installation Guide*. These documents describe the international agency compliance and safety information for the Mediatrix unit. They also include 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 Media5' 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.

Supported Standards

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>.

Refer to the Supported Standards document at <http://www.media5corp.com/documentation>

Naming Conventions

When defining a name for a parameter, only ascii characters are authorised. This is valid when defining a name for a parameter in a Web Page of the Management interface, but also for parameters accessed via the CLI, the MIB, or a script.

For example, to be valid, the Service Name defined during PPPoE configuration must only contain ascii characters. Special characters such as " " (space), "" (double quote), "" (left double quote), "" (left single quote), "#", "£", "¢", "¿", "¡", "«", "»" will cause the system to display a syntax error message.

CHAPTER

1

Information Important to Know

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

- ▶ Description of the Bypass feature for models that support it.
- ▶ Description of the various ways to manage the Mediatrix unit.
- ▶ How to use the DEFAULT/RESET button (partial reset and factory reset procedures).
- ▶ How to configure user access to the Mediatrix unit.

Introduction

The Dgw v2.0 application runs on all Mediatrix devices. Provider-specific profiles ensure that the Mediatrix unit is a genuine plug and play solution. It offers a low total cost of ownership as it reduces installation and maintenance costs.

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

For the complete list of Mediatrix unit brochures and technical specifications go to the at <http://www.media5corp.com/documentation>

Bypass Feature (Mediatrix 4100 Series)

During normal operation, the SCN line connected to the *Bypass* connector is switched out of the circuit through commuting relays. The *Bypass* connector can be activated by two different conditions:

- ▶ When power is removed from the Mediatrix unit.
- ▶ When the IP network is down.



Note: The Mediatrix 4102S does not have the Bypass feature.

This is indicated by the *In Use* LED being steady ON (except when the power is removed). If one of these conditions is met, a phone/fax used on FXS connector 1 (Mediatrix 4104/4108/4116) or analog line 1 (Mediatrix 4124) is directly connected to the SCN Bypass line. FXS connector 1 (Mediatrix 4104/4108/4116) or analog line 1 (Mediatrix 4124) stays in Bypass connection until:

- ▶ The error conditions have been cleared.
- ▶ The device connected to it is on-hook and a delay has elapsed.

Management Choices

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

Figure 1: Management Interfaces

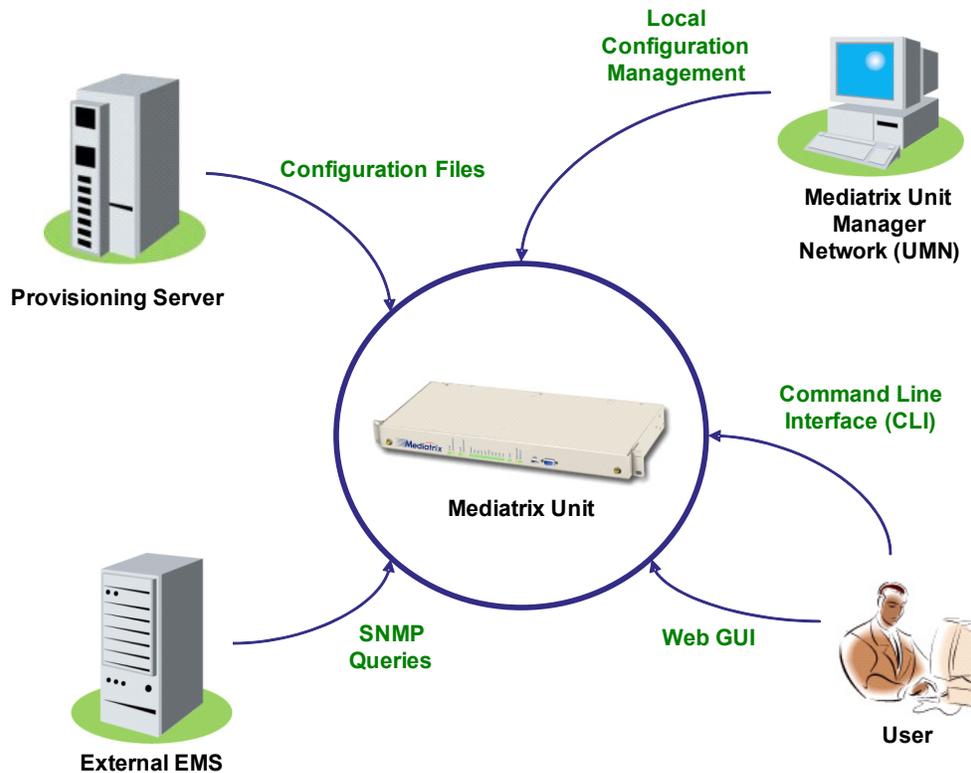


Table 1: Management Options

Management Choice	Description	Features
Web GUI	<p>The Mediatrix unit web interface offers the following options:</p> <ul style="list-style-type: none"> • Password-protected access via basic HTTP authentication, as described in RFC 2617 • User-friendly GUI <p>Refer to "Chapter 3 - Web Interface Configuration" on page 13 for more details.</p>	<p>The Mediatrix unit web interface allows you to configure the following information:</p> <ul style="list-style-type: none"> • Network attributes • SIP parameters • VoIP settings • Management settings such as configuration scripts, restore / backup, etc.
SNMPv1/2/3	<p>The Mediatrix unit SNMP feature offers the following options:</p> <ul style="list-style-type: none"> • Password-protected access • Remote management • Simultaneous management <p>Refer to "Chapter 50 - SNMP Configuration" on page 509 for more details.</p>	<p>The Mediatrix unit SNMP feature allows you to configure all the MIB services.</p>

Table 1: Management Options (Continued)

Management Choice	Description	Features
Command Line Interface (CLI)	<p>The Mediatix unit uses a proprietary CLI to configure all the unit's parameters.</p> <p>Refer to "Chapter 2 - Command Line Interface (CLI)" on page 7 for more details.</p>	<p>The Mediatix unit CLI feature allows you to configure all the MIB services.</p>
Unit Manager Network	<p>The Unit Manager Network (UMN) is a PC-Windows based element management system designed to facilitate the deployment, configuration and provisioning of Mediatix access devices and gateways.</p> <p>The UMN enables the simple and remote configuration and deployment of numerous Mediatix units.</p>	<p>The UMN offers the following:</p> <ul style="list-style-type: none">• 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 Mediatrix unit refuses to work properly for any reason or the connection to the network is lost.
- ▶ Reconfigure a unit.

The Partial reset provides a way to contact the Mediatrix unit in a known and static state while keeping most of the configuration unchanged. Refer to the *Performing a Partial Reset* Technical Bulletin <http://www.media5corp.com/documentation>

The Factory reset reverts the Mediatrix unit back to its default factory settings. Refer to *Performing a Factory Reset* at <http://www.media5corp.com/documentation>.

For the complete details on the RESET/DEFAULT button, refer to *Using the RESET/DEFAULT Button* Technical Bulletin at <http://www.media5corp.com/documentation>.

User Access

This section describes configuration that is available only in the MIB parameters of the Mediatrix 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 Mediatrix 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 Mediatrix 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 Media5. The available policies are:

Table 2: 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'.
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 Media5 representative.

CHAPTER

2

Command Line Interface (CLI)

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

- ▶ Introduction
- ▶ Configuring the CLI
- ▶ Accessing the CLI
 - Accessing the CLI through the Serial Console Port (Mediatix 3000 Series only)
 - Accessing the CLI via a Telnet Session
 - Accessing the CLI via a SSH Session
- ▶ Working in the CLI
 - Contexts
 - Exiting from the CLI
 - Command Completion
 - Macros
 - History
 - Service Restart
 - Configuring the Mediatix unit with the CLI
- ▶ List of Commands / Keywords

Introduction

You can configure the Mediatix unit parameters through a proprietary Command Line Interface (CLI) environment. It allows you to configure the unit parameters by Serial port (Mediatix 3000 Series only), Telnet or SSH.

The CLI uses the Media5 proprietary scripting language as described in the Scripting Language at <http://www.media5corp.com/documentation>.

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 through the console port of the Mediatrix unit (Mediatrix 3000 Series only) or through a Telnet or SSH session.

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

- ▶ [“Accessing the CLI through the Serial Console Port \(Mediatrix 3000 Series only\)” on page 8](#)
- ▶ [“Accessing the CLI via a Telnet Session” on page 9](#)
 - [“Opening a Telnet Session with the Unit Manager Network” on page 9](#)
- ▶ [“Accessing the CLI via a SSH Session” on page 10](#)

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. For more details refer to *Performing a Partial Reset* Technical Bulletin at <http://www.media5corp.com/documentation>.

Accessing the CLI through the Serial Console Port (Mediatrix 3000 Series only)

Serial console access requires a computer, serial terminal software, and null modem cable. Many networking environments have serial terminals available – or a laptop configured to act as a serial terminal – setup for use in configuration of network devices such as routers. In this case, it may be simplest to use the serial console access.

- ▶ **To access the CLI through the console port:**
 1. Connect a null modem cable, or crossover serial cable, to the serial console port on the front panel of the Mediatrix unit and to a serial port on your serial terminal computer.
 2. Using a terminal software, connect by using the following parameters:
 - 9600 baud
 - no parity
 - 8 data bits
 - 1 stop bit
 - no flow control
 3. If the Mediatrix unit is not on, power it up. The startup display should appear on the screen. If the Mediatrix unit is already started, you will see this display:
Login:
 4. Type the following command:
`public`

Do not type a password, just press <Enter>. After you successfully connect to the Mediatrix unit through the console port, you can start using the CLI to configure the Mediatrix unit.

If the connection is unsuccessful, check that the cable is properly connected or that you have the proper cable. Check also the connection parameters of your terminal software.

Accessing the CLI via a Telnet Session

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 Mediatrix unit via its LAN or WAN network interface.

► To access the CLI from a remote host using Telnet:

1. Set up the Mediatrix unit as described in the *Hardware Installation Guide*.
2. Power on your Mediatrix unit. Wait 60 seconds before proceeding to the next step.
3. Open a Telnet session to the Mediatrix unit (Mediatrix 3000 Series only):

- a. You can use the Mediatrix unit WAN IP address if you know it.
- b. You can use the default Mediatrix unit LAN IP address **192.168.0.10** if the LAN interface is enabled.

This procedure also requires some knowledge of how to configure the network settings of your desktop PC. When the unit ships from Media5, it has been assigned a default LAN IP address of 192.168.0.10. In order to log in to the unit across a network connection, you must use a machine located on the 192.168.0.0 subnet, or provide a static route in the routing table of your PC to reach the 192.168.0.0 subnet.

If you are using a Telnet port other than 23, (as configured in [“Configuring the CLI” on page 7](#)) you must also specify it.

4. Open a Telnet session to the Mediatrix unit by using one of the following IP addresses (Mediatrix 4100/4400/C7 Series):
 - 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 Mediatrix unit (see [“Chapter 11 - IPv4 vs. IPv6” on page 49](#) for more details)

If you are using a Telnet port other than 23, (as configured in [“Configuring the CLI” on page 7](#)) you must also specify it.

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

```
public
```

Do not type a password, just press <Enter>. After you successfully connect to the Mediatrix 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 Media5 Unit Manager Network (UMN) product to launch a Telnet client session to configure the parameters of the Mediatrix 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 Mediatrix unit at one of the IP addresses listed in [“Accessing the CLI via a Telnet Session” on page 9](#).
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

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 Mediatrix unit as described in the *Hardware Installation Guide*.
2. Power on your Mediatrix unit. Wait 60 seconds before proceeding to the next step.
3. Open a SSH session to the Mediatrix unit (Mediatrix 3000 Series only):
 - a. You can use the Mediatrix unit WAN IP address if you know it.
 - b. You can use the default Mediatrix unit LAN IP address **192.168.0.10** if the LAN interface is enabled.

This procedure also requires some knowledge of how to configure the network settings of your desktop PC. When the Mediatrix unit ships from Media5, it has been assigned a default LAN IP address of 192.168.0.10. In order to log in to the unit across a network connection, you must use a machine located on the 192.168.0.0 subnet, or provide a static route in the routing table of your PC to reach the 192.168.0.0 subnet.

If you are using a SSH port other than 22, (as configured in [“Configuring the CLI” on page 7](#)) you must also specify it.

4. Open a SSH session to the Mediatrix unit by using one of the following IP addresses (Mediatrix 4100/4400/C7 Series):
 - 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 7](#)) you must also specify it.

5. 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 Mediatrix unit by using Telnet, you can start using the CLI to configure the Mediatrix unit.

Working in the CLI

Refer to the CLI/Conf Scripting Language Syntax on the Documentation Portal.

CHAPTER

3

Web Interface Configuration

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

This chapter describes the following:

- ▶ Introduction to the Mediatrix unit web pages.
- ▶ 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 Mediatrix unit.
- ▶ Set the uplink parameters of the Mediatrix unit.
- ▶ Perform a firmware update, configuration scripts download, or configuration backup/restore.
- ▶ Set numerous parameters of the Mediatrix unit.

All of the parameters in the web interface may also be configured via SNMP. See [“Chapter 50 - SNMP Configuration” on page 509](#) 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 3: 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 Mediatrix unit. See [“Chapter 49 - Certificates Management” on page 501](#) 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"
```

5. Define the allowed cipher suites for the network security settings to which the Web server should listen when using the HTTPS mode in the `httpsCipherSuite` variable.

Any connection attempts to the web server using a cipher that is not allowed by the cipher suite will result in a failure to establish the connection.

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

```
web.httpsCipherSuite="value"
```

where *Value* may be as follows:

Table 4: HTTPS Cipher Suite Values and Parameters

Value	Parameter	Description
100	CS1	<p>The Web server only accepts requests using cipher suites:</p> <ul style="list-style-type: none"> • TLS_DHE_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_DSS_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_DSS_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA • TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA • TLS_RSA_WITH_3DES_EDE_CBC_SHA • TLS_RSA_WITH_RC4_128_SHA • TLS_RSA_WITH_RC4_128_MD5 • TLS_DHE_RSA_WITH_DES_CBC_SHA • TLS_RSA_WITH_DES_CBC_SHA • TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA • TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA • TLS_RSA_EXPORT_WITH_DES40_CBC_SHA • TLS_RSA_EXPORT_WITH_RC4_40_MD5
200	CS2	<p>This represents a secure configuration using SHA-1. Web server only accepts requests using cipher suites:</p> <ul style="list-style-type: none"> • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_3DES_EDE_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

Table 4: HTTPS Cipher Suite Values and Parameters (Continued)

Value	Parameter	Description
300	CS3	<p>This represents the most secure configuration using SHA-2. Only the most secure cipher suites are allowed when using this value.</p> <ul style="list-style-type: none"> • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256

Table 5: Cipher Suites Configuration Values

Value	Meaning
100	CS1
200	CS2
300	CS3

Tls Version Settings

You can define the allowed TLS versions for the network security settings when using the HTTPS. Any connection attempts to the web server using a TLS version that is not allowed will result in a failure to establish the connection.

You can configure this parameter as follows:

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

Table 6: Tls Version Configuration Settings

Parameter	Description
SSLv3	Allow SSL version 3 and all TLS versions.
TLSv1	Allow TLS versions 1 and up.
TLSv1_1	Allow TLS versions 1.1 and up.

Table 6: Tls Version Configuration Settings

Parameter	Description
TLSv1_2	Allow TLS versions 1.2 and up.

The default value is TLS1v.

► **To set the Tls Version configuration parameter:**

1. In the *webMIB*, locate the *ServerGroup* folder.
2. Set the Tls Version configuration in the `tlsversion` parameter.

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

```
web.tlsversion = "value"
```

where value may be:

Table 7: Tls Version Configuration Values

Value	Meaning
100	SSLv3
200	TLSv1
300	TLSv1_1
400	TLSv1_2

HTTP User-Agent Header Format

This section describes configuration that is available only in the MIB parameters of the Mediatrix 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 297](#) 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 8: Macros Supported

Macro	Description
%version%	Application version.
%mac%	MAC address.
%product%	Product name.

Table 8: Macros Supported (Continued)

Macro	Description
%profile%	Profile.
%%	Insert the % character.

For instance, the default value is:

%product%/v%version% %profile%

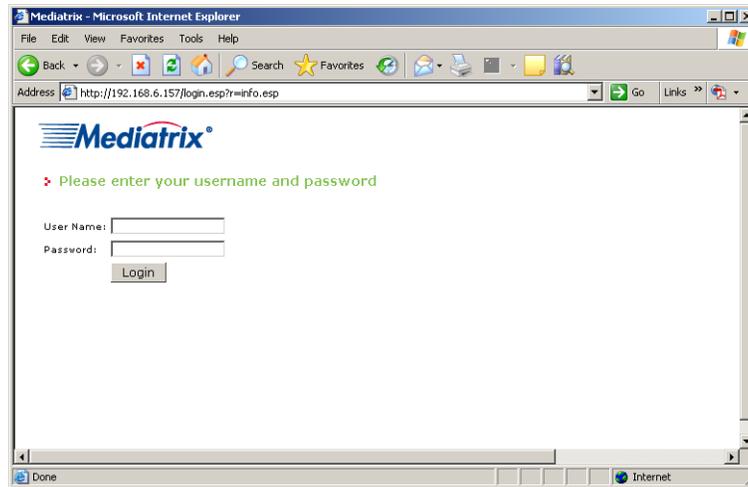
Using the Web Interface

Media5 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 Mediatrix unit LAN interface (if you have performed a partial reset, this is **192.168.0.10**).

Figure 3: 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:

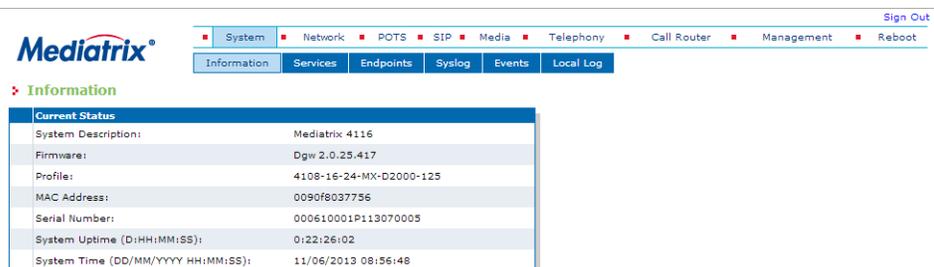
- **User Name:** admin
- **Password:** administrator

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 Mediatrix unit web interface is opened.

Figure 4: Information Web Page



The *Installed Hardware* section (Mediatrix 3000 Series only) lists the cards installed in the Mediatrix unit:

Table 9: Hardware Codes Description

Card Number	Quantity	Description	Products
Mediatrix 3301-010	1	FXS/FXO card	Mediatrix 3308, Mediatrix 3716, Mediatrix 3731, or Mediatrix 3741
	2	FXS/FXO card	Mediatrix 3316
Mediatrix 3301-020	1	E1/T1 card	Mediatrix 3531, Mediatrix 3621, Mediatrix 3631, Mediatrix 3731, or Mediatrix 3734
	2	E1/T1 card	Mediatrix 3532 or Mediatrix 3632
Mediatrix 3301-060	1	BRI card	Mediatrix 3404, Mediatrix 3734, or Mediatrix 3741
	2	BRI card	Mediatrix 3408
Mediatrix 3301-080	1	2 FXS/6 FXO card	Mediatrix 3208, Mediatrix 3716, Mediatrix 3732, or Mediatrix 3742
	2	2 FXS/6 FXO card	Mediatrix 3216

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

The *Login Window* web page displays.

Submitting Changes

When you perform changes in the web interface and click the *Submit* button, the Mediatrix 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 23 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 Mediatrix unit. If the unit is in use when you click *Reboot*, all calls are terminated.

System Parameters

Page Left Intentionally Blank

CHAPTER

4

Services

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

Services Table

The Mediatix 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 Mediatix unit. If the unit is in use when you click *Reboot*, all calls are terminated.

► To manage the Mediatix unit services:

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

Figure 5: System – Services Web Page

The screenshot shows the Mediatix web interface. At the top, there is a navigation bar with links for System, Network, SBC, ISDN, POTS, SIP, Media, Telephony, Call Router, and Ma. Below this is a secondary navigation bar with tabs for Information, Services, Hardware, Endpoints, Syslog, Events, Local Log, and VM. The main content area is titled 'Services' and contains two tables.

System Service	Status
Authentication, Authorization and Accounting (AAA):	Started
Certificate Manager (CERT):	Started
Configuration Manager (CONF):	Started
Device Control Manager (DCM):	Started
Ethernet Manager (ETH):	Started
File Manager (FILE):	Started
Firmware Pack Updater (FPU):	Started
Host Configuration (HOC):	Started
Local Quality Of Service (LQOS):	Started
Process Control Manager (PCM):	Started
Service Controller Manager (SCM):	Started

User Service	Status	Startup Type	Comment
Basic Network Interface (BNI):	Started	Auto	
Call Routing (CROUT):	Started	Auto	
Call Detail Record (CDR):	Stopped	Manual	
Command Line Interface (CLI):	Started	Auto	
CPE WAN Management Protocol (CWMP):	Started	Auto	
DHCP Server (DHCP):	Stopped	Manual	
Endpoint Administration (EPADM):	Started	Auto	
Endpoint Services (EPSERV):	Started	Auto	
IP Routing (IPROUTING):	Started	Auto	
Integrated Services Digital Network (ISDN):	Started	Auto	
Local Firewall (LFW):	Started	Auto	
Link Layer Discovery Protocol (LLDP):	Stopped	Manual	
Media IP Transport (MIPT):	Started	Auto	
Music On Hold (MOH):	Started	Auto	
Network Address Translation (NAT):	Stopped	Manual	
Network Firewall (NFW):	Stopped	Manual	
Notifications and Logging Manager (NLM):	Started	Auto	

The following are the services available. Note that the services available may differ depending on the Mediatrix unit you are using.

Table 10: Mediatrix 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 <i>File</i> transfer protocol.
Firmware Pack Updater (FPU)	Handles firmware upgrade and downgrade operations.
Host Configuration (HOC)	Configures network parameters that apply to the Mediatrix unit (not to a specific interface).
Local Quality Of Service (LQOS)	Configures the packets tagging sent from the Mediatrix unit.
Process Control Manager (PCM)	Responsible to boot and restart the unit.
Service Controller Manager (SCM)	Responsible to: <ul style="list-style-type: none"> • 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 Serial port (Mediatrix 3000 Series only), Telnet or SSH.
CPE WAN Management Protocol (CWMP)	Manages the support of the TR-069 protocol for auto provisioning.
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.

Table 10: Mediatrix unit Services (Continued)

Service	Description
Integrated Services Digital Network (ISDN)	Configures the Integrated Services Digital Network (ISDN) Basic Rate Interfaces (BRI) or Primary Rate Interfaces (PRI) parameters of the Mediatrix unit.
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.

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

Table 11: 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.

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

Table 12: Actions

Action	Description
	Starts the service.
	Stops the service.

Table 12: 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 Download” on page 499](#).

► 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 6: 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.

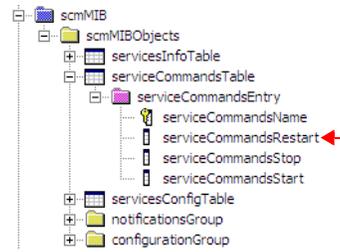
Restarting a Service via MIB

If you are using a MIB browser to access the Mediatrix 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 7: 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 8: 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 Mediatrix unit.

CHAPTER

5

Hardware Parameters

Refer to the **Hardware Configuration User Guide** located on the <http://www.media5corp.com/documentation>.

CHAPTER

6

Endpoints State Configuration

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

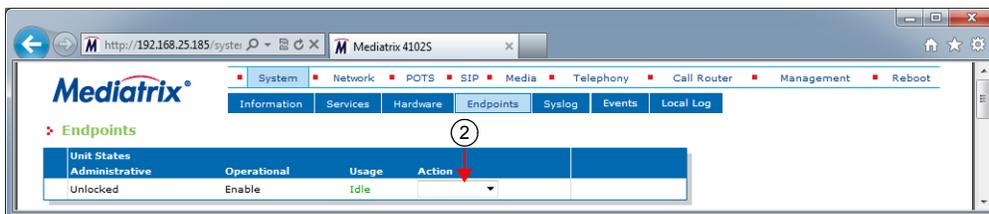
Unit Configuration

The unit configuration section allows you to define the administrative state of all the Mediatix 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 9: 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 Mediatix unit. This state is kept until you modify it or the unit restarts. It offers the following settings:

Table 13: 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 Mediatix 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 Mediatrix unit restarts in the *Initial Administrative* column.

Figure 10: Endpoint States Section

Endpoint States	Administrative	Operational	Usage	Initial Administrative	Action
Phone-Fax1	Unlocked	Enable	Idle	Unlocked	
Phone-Fax2	Unlocked	Enable	Idle	Unlocked	

Table 14: 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 Mediatrix unit. This state is kept until you modify it or the unit restarts. It offers the following settings:

Table 15: 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 11: Administration Section



Table 16: Unit Operational State Parameters

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

Table 16: Unit Operational State Parameters (Continued)

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

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

Table 17: 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 Mediatix LP/4100/C7 series
- Disable** for the Mediatix 3000 and Mediatix 4400 series

- 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 Mediatix 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 18: 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:

- In the *epAdmMIB*, locate the *UnitConfigGroup* folder.
- 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 19: Unit Shutting Down Behaviour Values

Value	Meaning
100	BlockNewCalls
200	AllowNewCalls

CHAPTER

7

Syslog Configuration

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

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

Syslog Daemon Configuration

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 Mediatrix unit. If no Syslog daemon address is provided by a DHCP server or specified by the administrator, no messages are sent.

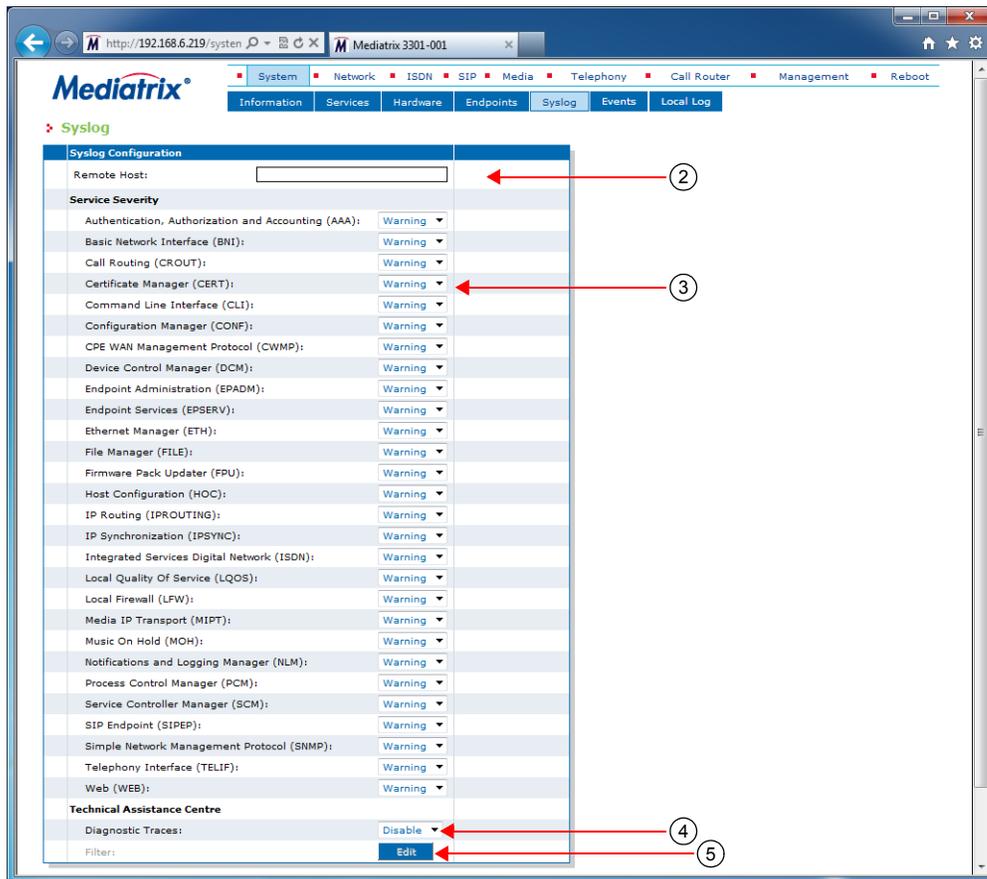
For instance, if you want to download a new firmware into the Mediatrix unit, you can monitor each step of the firmware download phase. Furthermore, if the unit encounters an abnormal behaviour, you may see accurate messages that will help you troubleshoot the problem.

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

► To configure the Mediatrix unit syslog client:

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

Figure 12: 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 20: 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 20: 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**.

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

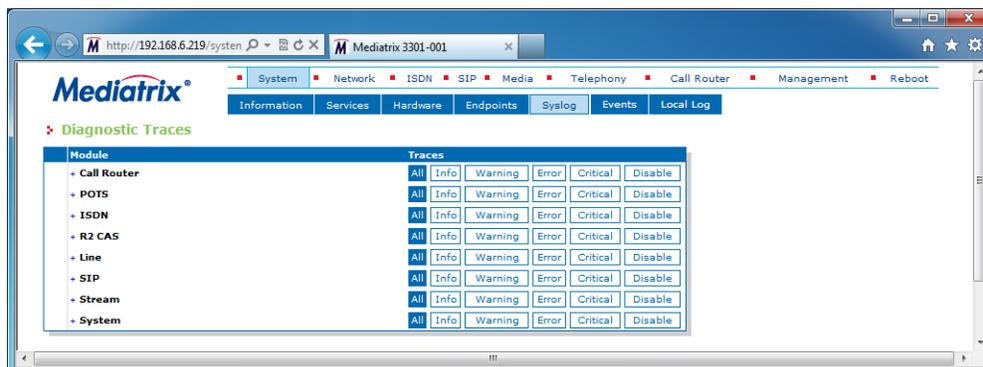
At the request of Media5's Technical Support personnel, enabling these traces will allow Media5 to further assist you in resolving some issues. However, be advised that enabling this feature issues a lot of messages to the syslog host. These messages may be filtered by using the *Diagnostic Traces Filter* field.



Note: Enabling all the traces could affect the performance of the Mediatrix unit.

- If applicable, define the filter applied to diagnostic traces by clicking the **Edit** button in the *Filter* field. The following opens:

Figure 13: Diagnostic Traces Window



You can use the filter to narrow down the number of traces sent at the request of Media5's Technical Support personnel.

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

Configuring PCM Capture

Refer to the *Dgw PCM Traces* technical bulletin on our [Documentation Portal](#).

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 Mediatrix 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 35](#) for more details.
2. In the web interface, click the *System* link, then the *Events* sub-link.

Figure 14: 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 21: 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 Mediatrix 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 22: Action Parameters

Parameter	Description
Send Via Syslog	The event notification is sent using syslog as transport. See “Chapter 7 - Syslog Configuration” on page 35 for more details.
Send Via SIP	The event notification is sent using SIP Notify as transport.
Log Locally	Log is stored in the volatile memory (RAM) and displayed on the Web page/ SNMP/TR-069
Log to File	Log is stored in a file in the persistent storage (flash) and available through file transfers.



Note: The **Log to File** action is only available on units with 1024 KB or more of persistent storage i.e. on Mediatrix Sentinel, Mediatrix 44XX, Mediatrix LP 16/24, Mediatrix 4108/4116/4124, and Mediatrix 3000.

9. Click the **Apply** 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 23: Configuration Status Values

Value	Description
Valid	The current content of the fields <i>Type</i> , <i>Criteria</i> and <i>Action</i> is valid.

Table 23: Configuration Status Values (Continued)

Value	Description
Invalid	The current content of the fields <i>Type</i> , <i>Criteria</i> and <i>Action</i> is not valid.
Not Supported	The current content of the fields <i>Type</i> , <i>Criteria</i> and <i>Action</i> 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 **Apply** button.

Monitoring Parameters

This section describes configuration that is available only in the MIB parameters of the Mediatrix 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 generated by the Notifications and Logging Manager (NLM) for your Mediatrix 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 15: System – Local Log Web Page



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

Table 24: 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 25: 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.

Table 25: *Local Log Entries* Parameters

Parameter	Description
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.

CHAPTER

10

VM

This chapter describes how to use the Virtual Machine (VM) service. The VM service allows the administrator to manage virtual machines.



Note: This web page is available only on the following model:

- Sentinel

For more details, refer to the [VM Service User Guide](#).

Network Parameters

Page Left Intentionally Blank

CHAPTER

11

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 Mediatrix 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 Mediatrix unit with their availability in IPv4 and IPv6.

Table 26: IPv4 vs. IPv6 Availability

Feature	IPv4	IPv6
Backup/Restore transfer	✓	✓
Command Line Interface (CLI)	✓	✓
Configuration file transfer	✓	✓
Embedded DHCP server	✓	
Firmware Transfer	✓	✓
IP Routing	✓	
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)	✓	
TR-069	✓	

Table 26: IPv4 vs. IPv6 Availability (Continued)

Feature	IPv4	IPv6
WEB Configuration	✓	✓

If you configure the Mediatrix 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.

```

C:\WINNT\system32\cmd.exe
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Wan:

    Connection-specific DNS Suffix . : mediatrix.com
    IP Address . . . . . : 10.4.126.223
    Subnet Mask . . . . . : 255.255.0.0
    IP Address . . . . . : 2001:470:8929:4000:7806:1b61:5ef4:bb14
    IP Address . . . . . : 2001:470:8929:4000:219:b9ff:fe65:f59c
    IP Address . . . . . : fe80::219:b9ff:fe65:f59c%4
    Default Gateway . . . . . : 10.4.0.1
    fe80::211:43ff:fe58:18ff%4
  
```

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.

```

[root@PAFillion-Linux paf]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0 <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 1000
    link/ether 00:01:80:3c:64:2f brd ff:ff:ff:ff:ff:ff
    inet 10.4.200.22/16 brd 10.4.255.255 scope global eth0
    inet6 2001:470:8929:4000:201:80ff:fe3c:642f/64 scope global dynamic
        valid_lft 2066644sec preferred_lft 79444sec
    inet6 fe80::201:80ff:fe3c:642f/64 scope link
        valid_lft forever preferred_lft forever
  
```

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 Mediatrix 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 would then become "[fe80::201:80ff:fe3c:642f%wan]".

CHAPTER 12

Host Parameters

This chapter describes how to set the host information of the Mediatrix 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 Mediatrix 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 16: 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 Mediatrix 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 17: Host Name Configuration Section



Table 27: 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 53) 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 <i>Static</i> and <i>PPPoE</i>) 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 <i>Automatic IPv6 config source network</i> drop-down menu.
Static	You manually enter the domain name and it remains the same every time the Mediatrix 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 Mediatrix 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 18: Default Gateway Configuration Section



Table 28: 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 53) 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 <i>Static</i>) 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 Mediatrix 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 29: IPv6 Default Gateway Configuration Sources

Source	Description
Automatic IPv6	The default gateway name is automatically obtained from the IPv6 network defined in the <i>Automatic IPv6 config source network</i> drop-down menu.
Static	You manually enter the IPv6 address of the default gateway and it remains the same every time the Mediatrix 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

You can use up to four Domain Name Servers (DNS) to which the Mediatrix unit can connect. The DNS servers list is the ordered list of DNS servers that the Mediatrix 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 19: DNS Configuration Section

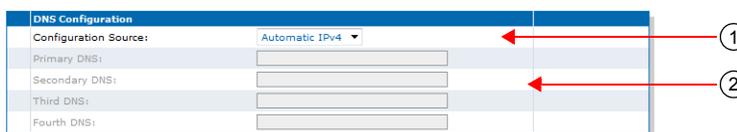


Table 30: DNS Configuration Sources

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 53) 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 <i>Static</i>) 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 <i>Automatic IPv6 config source network</i> drop-down menu.
Static	You manually enter up to four DNS servers IP addresses and they remain the same every time the Mediatrix 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

- 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

The Simple Network Time Protocol (SNTP) enables the notion of time (date, month, time) into the Mediatrix 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 Mediatrix unit implements a SNTP version 3 client.



Note: The Mediatrix 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 Mediatrix unit:

- 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 20: SNTP Configuration Section

Table 31: 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 53) 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 <i>Static</i> and <i>PPPoE</i>) 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 <i>Automatic IPv6 config source network</i> drop-down menu.
Static	You manually enter the values and they remain the same every time the Mediatrix unit restarts. Use the static configuration if you are not using a network server or if you want to bypass it.
Automatic with Fallback	The SNTP parameters are automatically obtained from the IPv4 Network from a fallback to the <i>StaticSntpServers</i> table.

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 32: 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

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 57](#).

► To set the time of the Mediatrix unit:

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

Figure 21: 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.

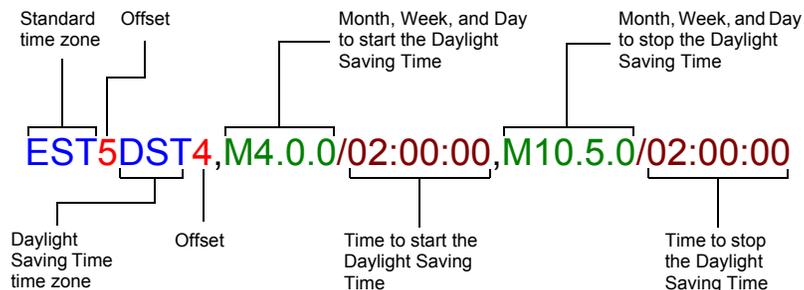
`M10.1.6`

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 33: 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 Mediatrix 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 34: 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 35: 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 36: 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:

- 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:

- 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 Mediatrix 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

13

Interface Parameters

This chapter describes how to set the interfaces of the Mediatrrix 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 Mediatrrix unit to the network, Media5 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 Mediatrrix 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 Mediatrrix unit and dial ****1** on the keypad. The MAC address of the Mediatrrix unit will be stated. This applies to Mediatrrix units with FXS interfaces.

Media5 recommends to reserve an IP address with an infinite lease for each Mediatrrix unit on the network.

Link Connectivity Detection

Each Ethernet port of the Mediatrrix 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

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 Mediatrix unit to properly connect to the WAN. The *Uplink* network interface is the IP interface that encapsulates the following link interface (WAN connection):
 - *eth5* (Mediatrix 3000 Series models)
 - *eth1* (Mediatrix 4400 Series models)
 - *eth1* (Mediatrix LP/4100/C7 Series models), *wan* for the Mediatrix 4102S

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 Mediatrix unit after a partial reset operation. You cannot delete this interface. Refer to *Performing a Partial Reset* at <http://www.media5corp.com/documentation>.
- ▶ 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 63 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, Media5 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 35 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.

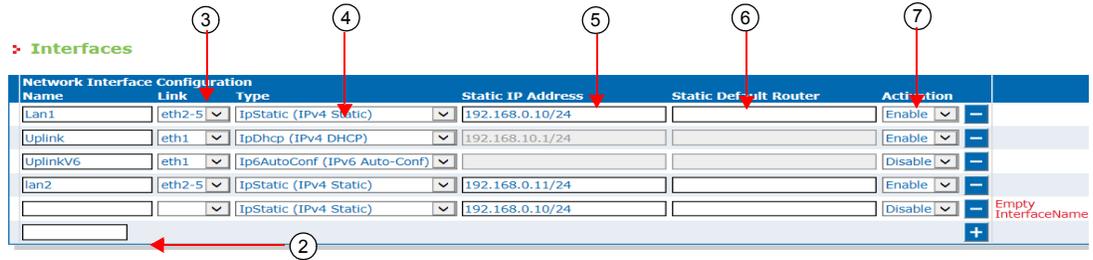


▶ When performing a partial reset (Refer to *Performing a Partial Reset* Technical Bulletin at <http://www.media5corp.com/documentation>), the management interface used for SNMP, CLI and WEB is automatically set to the *Rescue* interface. In that case, you must change the Mediatrix unit system management 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 22: 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 values "All", Loop, LoopV6 and Rescue are 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 Mediatrix 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.
 - Mediatrix 3000 Series: You can select between the *eth1-4* and *eth5* interfaces, as well as any defined VLANs.
 - Mediatrix LP/4100/C7 Series: You can select between the *eth1* and *eth2* interfaces, as well as any defined VLANs.

- Mediatix 4400 Series: You can select between the *eth1* interface and any defined VLANs.

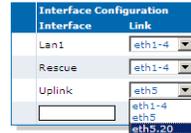
A VLAN is listed with the following syntax:

Link.VLAN ID

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

eth5.20

Figure 23: VLAN Example



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

Table 37: 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 73 for more details.
IPv4 Static	You manually enter the IPv4 address and network mask and they remain the same every time the Mediatix 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 69 for more details.
IPv6 Auto-Conf	IPv6 state-less auto-configuration. See “IPv6 Autoconfiguration Interfaces” on page 67 for more details.
IPv6 Static	You manually enter the IPv6 address and network mask and they remain the same every time the Mediatix 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 Mediatix 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 *Apply* if you do not need to set other parameters.

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

Table 38: 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.
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 Mediatrix 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 before 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, Media5 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 Mediatrix 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 Mediatrix 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 Mediatrix 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 Mediatrix unit should attempt to activate the corresponding network interface in the *Activation* drop-down menu.

Figure 24: Rescue Interface Configuration Section

Rescue interface			
Family	Link	IP Address	Activation
IP version 4	eth5	192.168.0.1/24	Disable
IP version 6	All	fe80::0290:f8ff:fe03:60be	

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 *Apply* if you do not need to set other parameters.

PPPoE Configuration

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 25: PPPoE Configuration Section

The screenshot shows a web form titled "PPPoE configuration". It contains four input fields: "Service Name", "Protocol", "User Name", and "Password". The "Protocol" field is a dropdown menu currently showing "CHAP". Three red arrows originate from numbered circles: circle 1 points to the "Service Name" field, circle 2 points to the "Protocol" dropdown, and circle 3 points to the "User Name" field.

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 Mediatrix 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 537](#) for more details.

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

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

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

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

PPP Negotiation

When the Mediatrix unit restarts, it establishes the connection to the access concentrator in conformance with the RFCs listed in [“PPPoE Configuration” on page 69](#).

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

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

Discovery Phase

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

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

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

Authentication Phase

If the access concentrator requests authentication, the Mediatrix 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 Mediatrix unit negotiates an IP address. The requested IP address is the one from the last successful PPPoE connection. If the Mediatrix 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 Mediatrix 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 39: 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 40: 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 26: 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 41: 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 42: 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 *Apply* if you do not need to set other parameters.

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

Ethernet Link Configuration

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 27: Ethernet Link Configuration Section

Link	MTU	802.1x Authentication	EAP Username	EAP Certificate Validation	
eth1	1500	Disable		Trusted And Valid	
eth2-5	ko	Enable		Trusted And Valid	MTU:Type Mismatch.

The *Maximum Transmission Unit (MTU)* is a parameter that determines the largest packet that 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 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 43: 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 44: 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.

Table 44: 802.1x Certificate Validation Parameters (Continued)

Parameter	Description
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.

- Indicates the configuration status of the row.
- Click *Apply* 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 45: 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).

EAP 802.1x Configuration

The *EAP 802.1x Configuration* section allows you to set the IEEE 802.1x version to be used by the unit.

► **To configure the IEEE 802.1x version parameter:**

- In the *EAP 802.1x Configuration* section, set the IEEE 802.1x version from the *EAP 802.1x Version* drop-down menu.

Figure 28: EAP 802.1x Configuration Section**Table 46:** EAP 802.1x Version Parameters

Parameter	Description
Version 2001	IEEE 802.1X-2001 – Port Based Network Access Control
Version 2004	IEEE 802.1X-2004 – Port Based Network Access Control

- Click *Apply* if you do not need to set other parameters.

DHCP Server Configuration



Note: This section applies only if you are using the DHCP connection type (“[Interfaces Configuration](#)” on [page 64](#)).

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 Mediatrix 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 Mediatrix unit:

*#*1

The Mediatrix unit answers back with its MAC address. This applies to units with FXS interfaces. See [“General POTS Configuration” on page 128](#) for more details.

Media5 recommends to reserve an IP address with an infinite lease for each Mediatrix 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 parameters are set

Table 47: DHCP Parameters

DHCP Parameter	Value
Host Name (option 12)	Set according to the <i>Host Name</i> parameter of the <i>Network > Host</i> page (“Host Configuration” on page 53). This option cannot be empty according to RFC 2132. If the <i>Host Name</i> parameter is empty, the DHCP option 12 is not sent.
Vendor Class Identifier (option 60)	Set according to the <i>System Description</i> parameter of the <i>System > Information</i> page.
Client identifier (option 61)	Set according to <i>MAC Address</i> parameter of the <i>System > Information</i> .

Ethernet Connection Speed

This section describes configuration that is available only in the MIB parameters of the Mediatrix 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 Mediatrix unit. The following values are available:

Table 48: Ethernet Ports Speed and Duplex Supported

Parameter	Description
Auto	Automatic negotiation 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 Mediatrix 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 76](#) 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 49: 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 Mediatrix 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

14

VLAN Parameters

For more details refer to the [Vlan configuration](#) technical bulletin on our documentation portal.

CHAPTER

15

Local QoS (Quality of Service) Configuration

This chapter describes how to configure the local QoS parameters. The local QoS tags packets sent from the Mediatrix 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

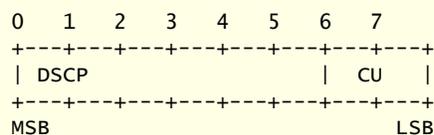
Differentiated Services (DiffServ, or DS) is a protocol for specifying and controlling network traffic by class so that certain types of traffic – for example, voice traffic, which requires a relatively uninterrupted flow of data, might get precedence over other kinds of traffic.

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.

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:



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

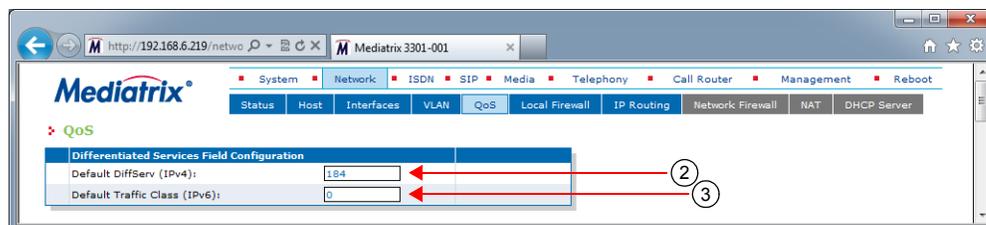
For both signalling and media packets, the DSCP field is configurable independently. The entire DS field (TOS byte) is currently configurable.

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

► **To configure the Mediatrrix unit DiffServ value:**

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

Figure 29: 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 81](#) 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 Mediatrrix 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 81](#) 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 Mediatrix 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 30: Ethernet 802.1Q Tagging Configuration Section

Ethernet 802.1Q Tagging Configuration	Enable	Default User Priority
eth1-4	Disable	0
eth5	Disable	0

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 81](#) 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 Mediatrix unit:

- Signalling
- Voice
- T.38

► 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 31: Service Class Configuration Section

Service Class Configuration	DiffServ (IPv4)	Traffic Class (IPv6)	User Priority
Signaling	184	0	6
Voice	184	0	6
T.38	184	0	6

See [“Differentiated Services \(DS\) Field” on page 79](#) 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 81](#) 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 23](#) 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 50: 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).

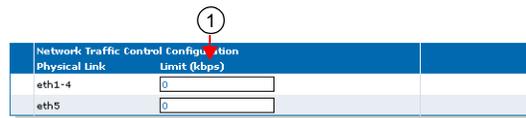
Packets that exceed the defined bandwidth are eventually dropped (when the buffers are exceeded). This implies that data bursts can suffer a slight amount of packet loss. The different codecs configured and the desired number of simultaneous channels should be taken into account when choosing a bandwidth 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 32: Network Traffic Control Configuration Section



Physical Link	Limit (kbps)
eth1-4	0
eth5	0

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

CHAPTER

16

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 Mediatrix unit's local firewall settings do not support IPv6. See ["IPv4 vs. IPv6" on page 49](#) 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 Mediatrix 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 Mediatrix unit's overall performance as the firewall requires additional processing. The more rules are enabled, the more overall performance is affected. Furthermore, Media5 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, especially with the Mediatrix 3632 / 4404 / 4124 / LP24 models.

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.

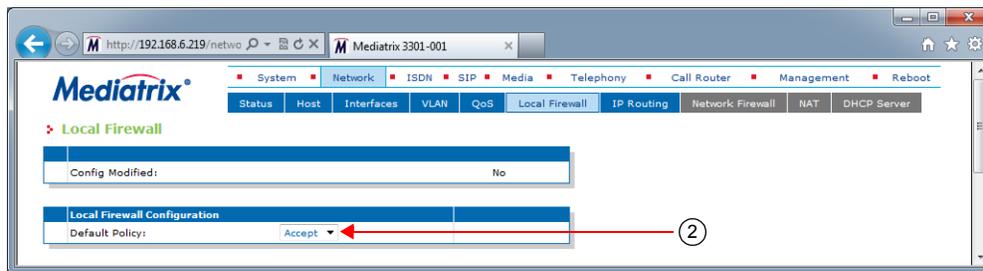
Setting the Default Policy

The default policy defines the action the Mediatrix 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 33: Network – Local Firewall Web Page



2. In the *Local Firewall Configuration* section, define the *Default Policy* drop-down menu.

Table 51: 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.

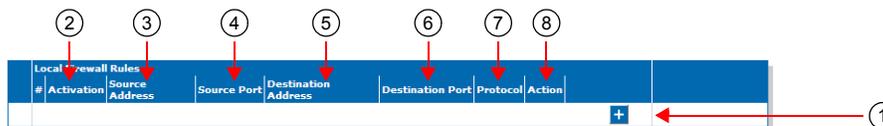
Creating/Editing a Firewall Rule

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 34: 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.

- Set the current activation state for this rule in the corresponding *Activation* drop-down menu.

Table 52: 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.

- Enter the source address of the incoming packet in the corresponding *Source Address* field.

Use one of the following syntax:

Table 53: 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 <i>Interface Configuration</i> table (see “ Interfaces Configuration ” on page 64 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.

- 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).

- Enter the destination address of the incoming packet in the corresponding *Destination Address* field.

Use one of the following syntax:

Table 54: 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 54: Source Address Parameters (Continued)

Parameter	Description
networkInterfaceName	The host address of this interface is used. The value must already exist in the <i>Interface Configuration</i> table (see “ Interfaces Configuration ” on page 64 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.

- 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).
- Select the protocol of the incoming packet to filter in the corresponding *Protocol* drop-down menu.

Table 55: 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.

- Select the action to take in the corresponding *Action* field.

Table 56: 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.

- 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  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 Mediatix 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 Mediatix unit.

CHAPTER

17

IP Routing Configuration

This chapter describes how to configure the IP Routing parameters of the Mediatrix 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 Mediatrix 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 Mediatrix unit's IP Routing settings do not support IPv6. See ["IPv4 vs. IPv6 Availability" on page 49](#) for more details.

Packets matching a list of criteria should¹ 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 18 - Network Firewall Configuration" on page 99](#))
- ▶ NAT (["Chapter 19 - NAT Configuration" on page 105](#))
- ▶ DHCP server (["Chapter 20 - DHCP Server Settings" on page 113](#))
- ▶ Network Traffic Control (["Network Traffic Control Configuration" on page 82](#))

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 Mediatrix 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 23](#) on information on how to start the service.



Caution: Enabling the IP routing service and adding rules has an impact on the Mediatrix unit's overall performance as IP routing requires additional processing. The more rules are enabled, the more overall performance is affected. Furthermore, Media5 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, especially with the Mediatrix 3632 / 4404 / 4104 models.

IPv4 Forwarding

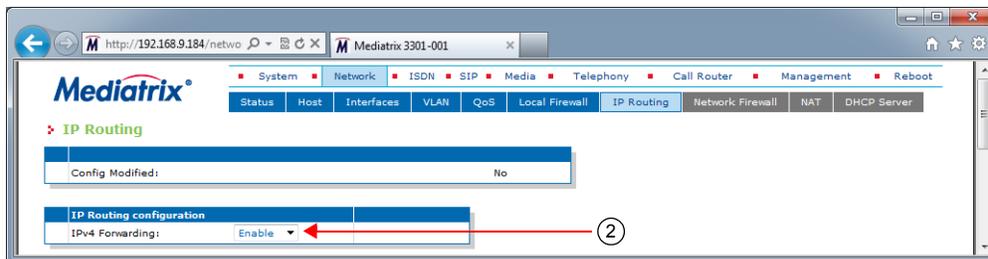
IPv4 forwarding allows you to control the IPv4 forwarding feature and the Advanced IP Routes. When set to Enabled, IPv4 Forwarding is enabled and the Advanced IP Routes are applied. When set to Disabled, IPv4 Forwarding is disabled and the Advanced IP Routes are not applied (the *Advanced IP Routes* 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 35: IPv4 Forwarding Configuration Section



3. Click the **Submit & Apply** button to update the *Network > Status* web page.

Creating/Editing an IP Routing Rule

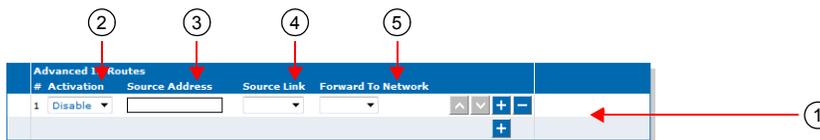
The web interface allows you to create a routing rule or modify the parameters of an existing one.

► **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 36: Advanced IP Routes Section



2. Set the required state for this rule in the corresponding *Activation* drop-down menu.

Table 57: 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 58: 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: <ul style="list-style-type: none"> • 192.168.0.11 • 192.168.1.0/24
networkInterfaceName[/]	The value must already exist in the <i>Interface Configuration</i> table (see “ Interfaces Configuration ” on page 64 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: <ul style="list-style-type: none"> • Lan1/ (Lan1 network address) <p>Note: It is mandatory to use the suffix “/” to indicate that the network address of this interface is used instead of the host address.</p>

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.

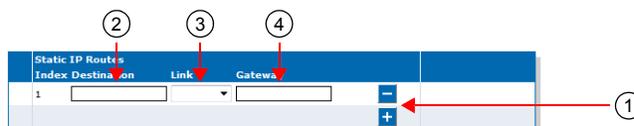
Static IPv4 Routes

You can add or delete static IPv4 routes in the Mediatrix 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 95).

► **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 37: 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 59: 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

This section describes configuration that is available only in the MIB parameters of the Mediatix 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 55](#) for more details), the route received through option 121 has priority.

The following values are available:

Table 60: 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 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 61: DHCPv4 Classless Static Route Option Values

Value	Meaning
100	None
200	Request

DHCPv4 User Class Route Option

Standards Supported	• RFC 3004 -The User Class Option for DHCP
----------------------------	--

This section describes configuration that is available only in the MIB parameters of the Mediatix 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 a list of user classes to enable the User Class Route Option. The list of user classes is sent using option 77. Hexadecimal values are supported using the ‘xXX’ format where XX is the hexadecimal value. When the variable is empty, user class option is not sent.

▶ **To define a list of user classes:**

1. In the *bniMIB*, locate the *DhcpClientGroup* folder.
2. Set the `dhcpClientUserClass` variable with the list of user classes.

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

```
bni.dhcpClientUserClass="value"
```

where *Value* may be one or more user classes.

User Class items are separated by a comma and items must not be empty.

Network Configuration Examples

The following are two examples of advanced IP routing that can be accomplished with the Mediatrix 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 91](#)).
 - Source IP: Lan1/
Remove this criterion if you want to forward all packets received on the *lan* link.
 - Source Link: lan²
 - Destination Network: Uplink
 - Click *Submit & Apply*.
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 105](#)).
 - 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 99](#)).
 - 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 99](#)).
 - 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 109](#)).

This will change the destination of an HTTP packet originally destined to the Mediatrix 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

2. The source link name may vary depending on the unit model you have.

- 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 105).
- 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 99).
- 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 99).
- Destination IP: 192.168.0.11
 - Destination Port: 80
 - Protocol: TCP
 - Action: Accept
 - Click *Submit & Apply*.

CHAPTER

18

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 Mediatrix unit's network firewall settings do not support IPv6. See ["IPv4 vs. IPv6 Availability" on page 49](#) 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 23](#) 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 Mediatrix unit's overall performance as the firewall requires additional processing. The more rules are enabled, the more overall performance is affected. Furthermore, Media5 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, especially with the Mediatrix 3632 / 4404 / 4104 models.

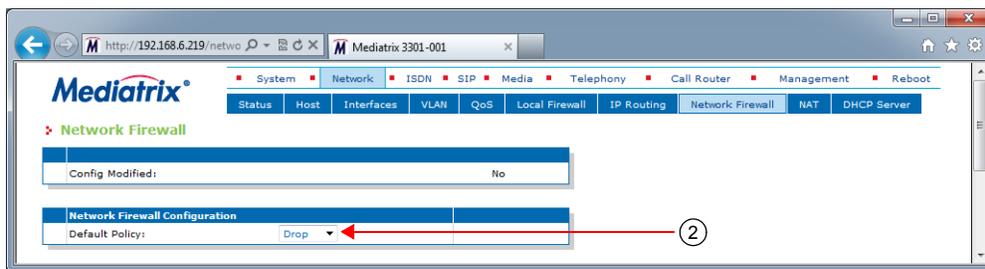
Setting the Default Policy

The default policy defines the action the Mediatrix 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 38: Network – Network Firewall Web Page



2. In the *Network Firewall Configuration* section, define the default policy in the *Default Policy* drop-down menu.

Table 62: 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.

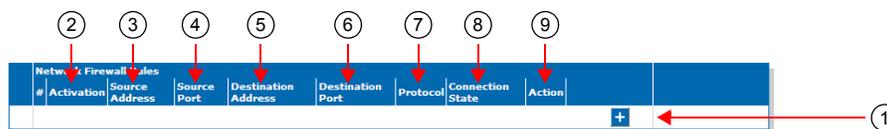
Creating/Editing a Network Firewall Rule

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 39: 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 63: 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 64: 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: <ul style="list-style-type: none"> • 192.168.0.11 • 192.168.1.0/24
networkInterfaceName/	The value must already exist in the <i>Interface Configuration</i> table (see “Interfaces Configuration” on page 64 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: <ul style="list-style-type: none"> • Lan1/ (Lan1 network address) <p>Note: It is mandatory to use the suffix “/” to indicate that the network address of this interface is used instead of the host address.</p>

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 65: 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: <ul style="list-style-type: none"> • 192.168.0.11 • 192.168.1.0/24
networkInterfaceName/	The value must already exist in the <i>Interface Configuration</i> table (see “Interfaces Configuration” on page 64 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: <ul style="list-style-type: none"> • Lan1/ (Lan1 network address) <p>Note: It is mandatory to use the suffix “/” to indicate that the network address of this interface is used instead of the host address.</p>

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 66: 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 67: Connection State Parameters

State	Description
All	Match packets in any state.
New	Match packets that are not part of an existing connection.

Table 67: 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 68: 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  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 Mediatrix 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 23 for more details on how to stop a service. All forwarded traffic is allowed when the network firewall service is stopped.

CHAPTER

19

NAT Configuration

This chapter describes how to configure the NAT parameters of the Mediatrix 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 Mediatrix 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 23 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 Mediatrix unit's overall performance as the NAT requires additional processing. The more rules are enabled, the more overall performance is affected. Furthermore, Media5 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, especially with the Mediatrix 3632 / 4404 /4104 models.

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

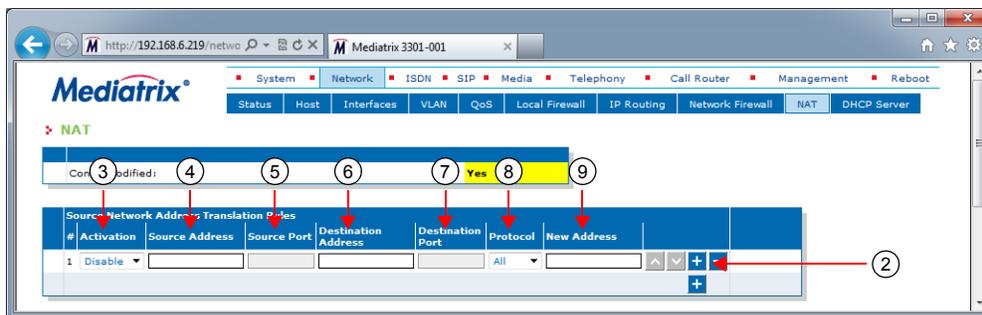
- ▶ Source Port
- ▶ Destination Address
- ▶ Destination Port
- ▶ Protocol

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 40: 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 69: 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 70: 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: <ul style="list-style-type: none"> • 192.168.0.11 • 192.168.1.0/24
networkInterfaceName[/]	The value must already exist in the <i>Interface Configuration</i> table (see “ Interfaces Configuration ” on page 64 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: <ul style="list-style-type: none"> • 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 71: 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: <ul style="list-style-type: none"> • 192.168.0.11 • 192.168.1.0/24

Table 71: Destination Address Syntax (Continued)

Syntax	Description
networkInterfaceName/	<p>The host address of this interface is used. The value must already exist in the <i>Interface Configuration</i> table (see “Interfaces Configuration” on page 64 for more details). The interface name is case sensitive, hence it must be entered properly.</p> <p>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:</p> <ul style="list-style-type: none"> Lan1/ (Lan1 network address) <p>Note: It is mandatory to use the suffix “/” to indicate that the network address of this interface is used instead of the host address.</p>

Leaving the default empty string matches any address.

- 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).
- Select the protocol of the incoming packet to NAT in the corresponding *Protocol* drop-down menu.

Table 72: 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.

- Enter the new address applied to the source of the packet in the *New Address* field.
 Use the following syntax:

Table 73: 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.

- 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 18 - Network Firewall Configuration” on page 99) 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:

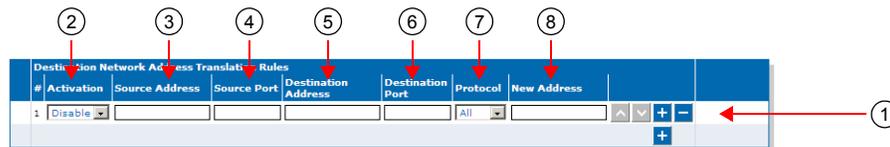
- ▶ Source Address
- ▶ Source Port
- ▶ Destination Address
- ▶ Destination Port
- ▶ Protocol

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 41: 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 74: 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 75: 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: <ul style="list-style-type: none"> 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 <i>Interface Configuration</i> table (see “Interfaces Configuration” on page 64 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: <ul style="list-style-type: none"> Lan1/ (Lan1 network address) <p>Note: It is mandatory to use the suffix “/” to indicate that the network address of this interface is used instead of the host address.</p>

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 76: 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: <ul style="list-style-type: none"> 192.168.0.11 192.168.1.0/24

Table 76: Destination Address Syntax (Continued)

Syntax	Description
networkInterfaceName[/]	<p>The host address of this interface is used. The value must already exist in the <i>Interface Configuration</i> table (see “Interfaces Configuration” on page 64 for more details). The interface name is case sensitive, hence it must be entered properly.</p> <p>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:</p> <ul style="list-style-type: none"> Lan1 (Lan1 IP address) Lan1/ (Lan1 network address)

Leaving the default empty string matches any address.

- 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).

- Select the protocol of the incoming packet to NAT in the corresponding *Protocol* drop-down menu.

Table 77: 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.

- Enter the new address of the packet in the *New Address* field.

Use the following syntax:

Table 78: 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.

- 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 ▼ 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 Mediatix 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 23 for more details on how to stop a service.

CHAPTER

20

DHCP Server Settings

This chapter describes how to configure the embedded DHCP server of the Mediatrix unit.

Introduction

The Mediatrix 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 23](#) on information on how to start the service.



Note: The Mediatrix unit's DHCP server settings do not support IPv6. See [“IPv4 vs. IPv6” on page 49](#) 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 79: 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 <i>Automatic Configuration Interface</i> drop-down menu of this subnet (“DHCP Basic Configuration” on page 115).
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 80: 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 Mediatrix unit.
- ▶ Specific configurations that override the default configurations.

You can define specific configurations for each subnet in your Mediatrix unit. For instance, you could define a lease time for all the subnets of the Mediatrix 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 Mediatrix 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 42: 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 Mediatrix unit. The Mediatrix 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.

Note:

If you created Network Interfaces in the Interface Configuration table (Network > Interfaces) and wish to use them as the *Automatic Configuration Interface*, you must first make the Network interface available to the DHCP service. Refer to ["To have a new network interface available in the DHCP service:"](#) on page 115

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

► **To have a new network interface available in the DHCP service:**

In the CLI or UME, type the `dhcp.AddSubnet` command, where Network =<Interface Name>.

Lease Time (Option 51)

The Mediatrix 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 43: DHCP Server Configuration – Lease Time Option

2. Define the lease time (in seconds) given by the Mediatrix 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 Mediatrix 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 44: 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 81: 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 Mediatrix 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 45: DHCP Server Configuration – Default Gateway Option



2. Select the configuration source of the default gateway information in the *Configuration Source* drop-down menu.

Table 82: 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.

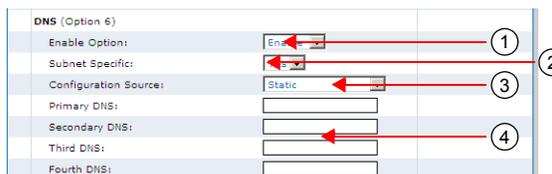
DNS (Option 6)

The Mediatrix 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 46: 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 83: DNS Configuration Sources

Source	Description
Host Configuration	The DNS servers are obtained from the host configuration.

Table 83: DNS Configuration Sources (Continued)

Source	Description
Automatic	The DNS servers are automatically obtained from the network configured in the <i>Automatic Configuration Interface</i> drop-down menu of this subnet (“ DHCP Basic Configuration ” on page 115).
Static	You manually enter the value.

Static Configuration Source Only

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

NTP (Option 42)

The Mediatrix 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:**

- 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 47: DHCP Server Configuration – NTP Option



- 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.
- Select the configuration source of the NTP information in the *Configuration Source* drop-down menu.

Table 84: 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 <i>Automatic Configuration Interface</i> drop-down menu of this subnet (“ DHCP Basic Configuration ” on page 115).

Table 84: NTP Configuration Sources (Continued)

Source	Description
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 Mediatrix 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 48: 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

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 115). The DHCP server can service all subnets on which it is enabled.

► **To define DHCP leases offered by the Mediatrix 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.

SBC Parameters

Page Left Intentionally Blank

CHAPTER

21

SBC Configuration

This chapter describes how to configure the Sbc (Session Border Controller) service, which allows the administrator to perform SIP to SIP normalization, call routing, NAT traversal and survivability.



Note: This web page is available only on the following models:

- Sentinel and Mediatrix 3000

For complete details on the Sbc service, refer to the Sbc User Guide at <http://www.media5corp.com/documentation>

POTS Parameters

Page Left Intentionally Blank

CHAPTER

22

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.



Note: This web page is available only on the following models:

- Mediatrix 3208 / 3216
- Mediatrix 3308 / 3316
- Mediatrix 3716
- Mediatrix 3731
- Mediatrix 3732
- Mediatrix 3741
- Mediatrix 3742
- Mediatrix 4100 Series
- Mediatrix LP Series
- Mediatrix C7 Series

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 49: POTS – Status Web Page

Line Status ID	Type	State
Port1	FXS	Idle
Port2	FXS	Idle
Port3	FXS	Idle
Port4	FXS	Idle

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

FXO Line Status



Note: This web page is available only on the following models:

- Mediatrix 3208 / 3216
- Mediatrix 3308 / 3316
- Mediatrix 3716
- Mediatrix 3731
- Mediatrix 3732
- Mediatrix 3741
- Mediatrix 3742
- Mediatrix C730 / C733 / C731

The *FXO Line Status* table lists the link state updated by the link state verification mechanism.

Figure 50: POTS – FXO Line Status Table

FXO Line Status ID	Link State
Slot3/FXO	Down

You can enable the line state verification in “[FXO Custom Basic Parameters](#)” on page 142.

The unit does not automatically detect when a previously connected port has changed to the disconnected status. The unit only detects the change of status when it attempts to use the port or after a restart.

The unit automatically detects within seconds when a disconnected port becomes connected.

- ▶ **Unknown:** The line fault detection is disabled.
- ▶ **Up:** When last polled, the line was connected.
- ▶ **Down:** When last polled, the line was disconnected.

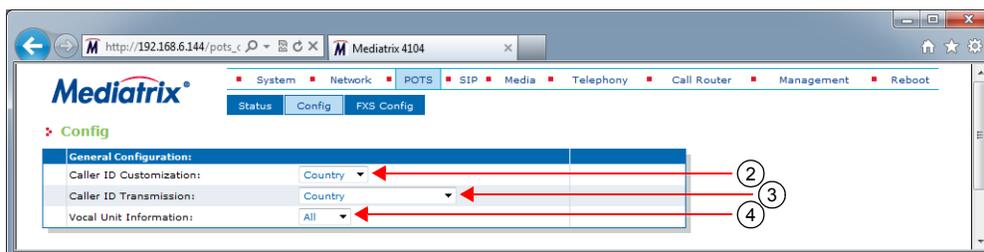
General POTS Configuration

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 51: 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 130 for more details.

Table 85: Caller ID Parameters

Parameter	Description
Country	Uses the default caller ID of the country defined in the <i>Country</i> section of the <i>Telephony > Misc</i> page (“ Country Configuration ” on page 419).

Table 85: Caller ID Parameters (Continued)

Parameter	Description
EtsiDtmf	ETSI 300 659-1 (DTMF string sent between the first and second ring).
EtsiFsk	ETSI 300 659-1 (FSK (V.23) 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 86: Caller ID Transmission Parameters

Parameter	Description
Country	Uses the default caller ID of the country defined in the <i>Country</i> section of the <i>Telephony > Misc</i> page (" Country Configuration " on page 419).
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 Mediatrix unit talks back to you with relevant information.

Table 87: Caller ID Parameters

Parameter	Description
None	The vocal information feature is disabled.
All	Enable all vocal information digit maps.

To access the vocal unit information:

- a. Take one of the telephones connected to the Mediatrix unit.
- b. Dial one of the digits sequence on the keypad.

Table 88: Vocal Unit Information

Digits to Dial	Information Vocally Sent by the Mediatrix unit
*#*0	List of IP addresses of the Mediatrix unit (static or DHCP).
*#*1	MAC address of the Mediatrix unit.
*#*8	Firmware version number of the Mediatrix 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 Mediatrix 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 Mediatrix unit is compatible with the following widely used standards:

- ▶ ETSI 300 659-1



Note: The compatibility of the Mediatrix 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

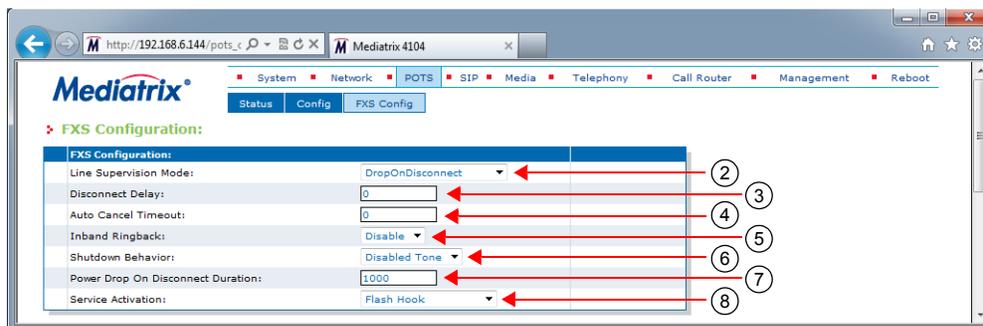
FXS Configuration

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 52: 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 89: 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 <i>FXS Power Drop on Disconnect Duration</i> field (Step 5).
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 90: 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 91: 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 32](#) 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 135](#) 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 92: Service Activation Parameters

Parameter	Description
Flash Hook	Service activation is performed by flash hook or hanging up.

Table 92: Service Activation Parameters (Continued)

Parameter	Description
Flash Hook And Digit	<p>Service activation is performed by flash hook, flash hook followed by a digit or hanging up.</p> <p>The digit dialed has a different behaviour depending on the current call context:</p> <ul style="list-style-type: none"> One call active with one waiting call or one call on hold: <ul style="list-style-type: none"> Flash hook then dial the digit 1 or hang up: Terminate the active call and switch to the call on hold/waiting. Flash hook then dial the digit 2: Hold the active call and switch to the call on hold/waiting. Flash hook then dial the digit 3: Enter in three-party conference mode. Flash hook then dial the digit 4: Transfer the call on hold to the active call (not available on call waiting). In three-party conference mode: <ul style="list-style-type: none"> Flash hook then dial the digit 1: Exit from three-party conference mode. The third party remains active and the second party call is terminated. Flash hook then dial the digit 2: Exit from three-party conference mode. The second party remains active and the third party call is placed on hold. <p>When hanging up in this context, the telephone rings to notify the user there is still a call on hold.</p> <p>When hanging up in this context, all calls are finished.</p>

- 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 651](#) for the pre-defined values for a specific country.

► **To define the FXS country customization parameters:**

- 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 53: FXS Country Customization Section



Table 93: Line Supervision Mode Parameters

Parameter	Description
Disable	The line uses the default country FXS settings.

Table 93: Line Supervision Mode Parameters (Continued)

Parameter	Description
Enable	The line uses the FXS country configuration set in the following steps.

- 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 Mediatix 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 Mediatix 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 131 for more details.

When one of its analog lines goes off-hook, the Mediatix unit controls the endpoint in a fixed loop current mode. When selecting a country (see "[Country Configuration](#)" on page 419 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. **Mediatix LP16/LP24 models:** The values available for these models are between 20 mA and 25 mA. The default value is 22 mA. If you set a value higher than 25 mA, the unit will limit the current to 25 mA.

- 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 419 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.

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

Calling Party Name of the Caller ID

- 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).

FXS Bypass



Note: This web page is available only on the following models:

- Mediatrix 3308 / 3316
- Mediatrix 3716
- Mediatrix 3731
- Mediatrix 3741
- Mediatrix 4100 Series (except Mediatrix 4102S)

The *FXS Bypass* section allows you to define whether or not the bypass feature is enabled. This feature allows its users to maintain telephone services in the event of a power outage or network failure.

During normal operation, the SCN line connected to the *Bypass* connector is switched out of the circuit through commuting relays. The *Bypass* connector can be activated by three different conditions:

- ▶ When power is removed from the Mediatrix unit.
- ▶ When the FXS endpoint's operational state is disabled and the endpoint is not in use.
- ▶ When the user signals the configured DTMF map.

If one of these conditions is met, a phone/fax used on a FXS connector that supports the bypass feature is directly connected to the SCN Bypass line. The FXS connector stays in Bypass connection until:

- ▶ The error conditions have been cleared.
- ▶ The device connected to it is on-hook and a delay has elapsed.



Note: For the Mediatrix 3308, Mediatrix 3316, Mediatrix 3731 and Mediatrix 3741 models: If an event that activates the FXS bypass occurs and the FXO port is in use, the bypass activation waits until the FXO port is no longer in use. See [“FXO Configuration” on page 139](#) for more details.

For more information on your model's bypass feature and which FXS connectors are available for bypass, please refer to your model's *Hardware Configuration Guide*.

▶ **To define the FXS bypass parameters:**

1. In the *FXS Bypass* section, specify when the bypass needs to be activated in the corresponding *Activation* column's drop-down menu.

Figure 54: FXS Bypass Section

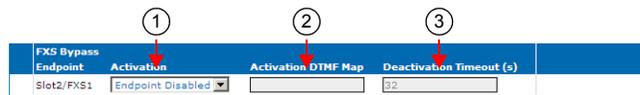


Table 94: Activation Parameters

Parameter	Description
Power Off	The bypass is activated only when the unit power is off or the POTS service is not started.
Endpoint Disabled	The bypass is activated when: <ul style="list-style-type: none"> • the operational state of the endpoint is <i>Disable</i>, and • the <i>Shutdown Endpoint When Operational State is 'Disable' And Its Usage State Is 'idle-unusable'</i> parameter of the <i>SIP > Endpoints</i> page is set to Enable. See “Administration” on page 32 for more details. The bypass is also activated for the same conditions as the ones defined in <i>Power Off</i> .

Table 94: Activation Parameters (Continued)

Parameter	Description
On Demand	<p>The bypass is activated when the user enters the DTMF map configured in the corresponding <i>Activation DTMF Map</i> field (Step 2).</p> <p>The bypass is deactivated when the user on hooks the phone for at least the number of time configured in the corresponding <i>Deactivation Timeout</i> field (Step 3).</p> <p>The bypass is also activated for the same conditions as the ones defined in <i>Power Off</i>.</p>

2. Set the corresponding *Activation DTMF Map* field with the DTMFs to signal to enable the bypass.
This field is only used when the corresponding *Activation* drop-down menu is set to **On Demand**.
3. Set the corresponding *Deactivation Timeout* field with the delay, in seconds, to wait before deactivating the bypass after an on hook if the bypass is activated on demand.

The delay is restarted after each on hook. The bypass is not deactivated if the delay expires while the FXS is off hook.
This field is only used when the corresponding *Activation* drop-down menu is set to **On Demand**.



Note: For the Mediatrix 3308, Mediatrix 3316, Mediatrix 3731 and Mediatrix 3741 models, the bypass is automatically disabled after the timeout, whether or not the bypass is in use. Furthermore, if the conditions that activate the bypass are no longer present, the bypass is disabled.

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

FXS Emergency Call Override



Note: This feature is available for FXS units only.

This FXS Emergency Call Override feature allows you to override a set of services that are activated during an emergency call.

Two variables are available:

- ▶ *FxsEmergencyCallOverride* : to override or not the services.
- ▶ *FxsEmergencyRingTimeout*: to set the period before the phone starts to ring in the event where the originator of an emergency call hangs-up before the emergency call center disconnects the call.

The configuration of the Emergency Call Override is only available in the MIB parameters of the Mediatrix unit.

You can configure the parameters as follows:

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

▶ **To set the Emergency Call Override:**

1. In the *potsMIB*, set the *FxsEmergencyCallOverride* variable to the proper value, or
2. In the CLI or a configuration script use:

Pots.FxsEmergencyCallOverride="Value"
 where *Value* may be one of the following:

Table 95: Fxs Emergency Call Override Parameters

Value	Parameter	Description
100	NoOverride	The set of services for emergency calls remains the same as configured. This is the default value.
200	NoServices	Ignores any service requiring a flash-hook. Call waiting and all other related services are deactivated.
300	NoDisconnect	Ignores any service requiring a flash-hook. Call waiting and all other related services are deactivated AND automatically re-establishes a call that was disconnected by the originator.

► **To set the Emergency Ring Timeout Override:**

1. Make sure the *FxsEmergencyCallOverride* variable is set to *NoDisconnect*.
2. In the *PotsMIB*, set the *FxsEmergencyRingTimeout* variable to the proper value, or
3. In the CLI or a configuration script use:

Pots.FxsEmergencyRingTimeout="Value"

where *Value* is in milliseconds. The default value is 2000 ms.

FXS Distinctive Ring

This *FxsDistinctiveRingId* parameter allows you to create a custom distinctive ring. Configuring the custom distinctive ring allows the administrator to modify the ring pattern. When a *pots.fxsDistinctiveRing.RingId* is defined, the corresponding ring pattern is used.

To use the distinctive ringing with the unit, the received SIP INVITE message must contain the *Alert-Info* header field with the proper *Call Property* value.

Example

Alert-Info: <http://127.0.0.1/Bellcore-dr2>

Two variables are used to configure a distinctive ring:

- *RingId*: Identifies the distinctive ring. When the incoming call property 'distinctive-ring' matches the defined *RingId*, the corresponding ring pattern is used. Otherwise, the country ring pattern is used.
- *Pattern*: Describes a tone pattern.

The format of the pattern is as follows:

```
ring-pattern = [ states-section ]
states-section = on-state-description "," off-state-description [ "," on-state-description
"," off-state-description [ "," on-state-description "," off-state-description ] ]
on-state-description = time
off-state-description = time
time = 2*5DIGIT
```

Table 96: Tag description

Tag	Description
ring-pattern	String describing the pattern to use for the ring. An empty string means no ring.

Table 96: Tag description

Tag	Description
states-section	Description of the state of the ring. Up to 3 pairs of states can be defined. They must be at least one state described if the ring-pattern is not empty.
on-state-description	Description of a state playing a ring.
off-state-description	Description of a state not playing a ring.
time	The number of time in ms to perform the action of the state. Range is from 0 to 32767 ms.

Examples:

- No ring: ""
- Bellcore-dr2: "800,400,800,4000"
- Bellcore-dr4: "300,200,1000,200,300,4000"

Table 97: Default mapping between call property and ring cadence

Call Property Value	Ring cadence in milliseconds (bold are on, not bold are off).
//127.0.0.1/Bellcore-dr2	800 , 400, 800 , 400
//127.0.0.1/Bellcore-dr3	400 , 200, 400 , 200, 800 , 4000
//127.0.0.1/Bellcore-dr3	300 , 200, 1000 , 200, 300 , 4000
All other value or call properties not present	Country's normal ring.

The parameters can be set:

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

▶ **To customise a distinctive ring:**

1. In the *potsMIB* set:
 - *Pots.FxsDistinctiveRingId* variable in the *FxsDistinctiveRing* table
 - *Pots.FxsDistinctivePattern* variable in the *FxsDistinctiveRing* table.
 - or
 2. Use the CLI or a configuration script:
 - `Pots.FxsDistinctivering[index=value].RingId="value"`
 - `Pots.FxsDistinctivering[index=value].Pattern="value"`
- ▶ Index value can vary from 1 to 4.

FXO Configuration

The *FXO Config* page allows you to configure gateways-specific parameters.



Note: This web page is available only on the following models:

- Mediatrix 3208 / 3216
- Mediatrix 3308 / 3316
- Mediatrix 3716
- Mediatrix 3731
- Mediatrix 3732
- Mediatrix 3741
- Mediatrix 3742
- Mediatrix C730 / C733 / C731

The FXO port's use depends on the FXS bypass state (as defined in the *FXS Bypass* section of the *FXS Configuration* page – "[FXS Bypass](#)" on page 135):

- ▶ The FXO port becomes disabled as IP-FXO gateway when the FXS bypass is active. In this case:
 - calls from the IP side to the FXO port are discarded
 - calls coming from the SCN side on the FXO port are routed to FXS port #1.
- ▶ The FXO port becomes enabled and available for calls when the FXS bypass is disabled.

If an event that activates the FXS bypass occurs and the FXO port is in use, the bypass activation waits until the FXO port is no longer in use.

FXO Dialing Configuration

The *FXO Dialing Configuration* section allows you to set dialing parameters.

▶ **To set FXO dialing parameters:**

1. In the web interface, click the *POTS* link, then the *FXO Config* sub-link.

Figure 55: POTS FXO Config Web Page



2. Set the *Pre Dial Delay* field with the delay, in milliseconds, between the time the line is successfully seized, or dial tone detected, and the moment the destination phone number is dialed.

Some country specifications include a mandatory pre-dial delay. In that case, the highest value between that and the value set in this field is used.

A value of '0' indicates to use a value that is specific to the country specification as set in the *Tellf.CountrySelection* parameter.
3. Set the *Dial Tone Detection Mode* drop-down menu with the proper behaviour.

When dial tone detection is enabled, the unit waits for a dial tone on the FXO line before initiating the dialling sequence. If no dial tone is detected, the line is considered as busy with an incoming call. This mechanism helps avoid collisions between incoming and outgoing calls.

Table 98: Dial Tone Detection Modes

Parameter	Description
Disable	Dial tone detection is disabled.
Country Tone	The unit tries to detect the tone specified for this purpose in the current country's tone specification. Some country specifications omit this information. In that case, the unit behaves as if the parameter is set to Disable .

The following table lists the default dial tone detection frequency and cadence for each supported country.

Table 99: Default Dial Tone Detection

Country	Frequency	Cadence	
		ON (s)	OFF (s)
Austria	450 Hz	0.5	0.0
Czech Republic	425 Hz	0.3	0.0
France	440 Hz	0.5	0.0
Germany1/2	425 Hz	0.15	0.0
Italy	425 Hz	0.15	0.0
NorthAmerica1	440 Hz	0.5	0.0
Spain	425 Hz	0.15	0.0
Switzerland	425 Hz	0.5	0.0

4. Set the *Dial Tone Detection Timeout* field with the value, in milliseconds, indicating how long the unit waits for a dial tone before considering the line is busy with an incoming FXO call.
5. Click *Submit* if you do not need to set other parameters.

FXO Answering Configuration

The *FXO Answering Configuration* section allows you to define how the FXO line must behave when answering calls.

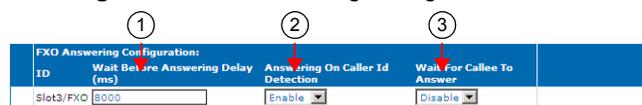
► **To set FXO answering parameters:**

1. In the *FXO Answering Configuration* section, set the corresponding *Wait Before Answering Delay* column's FXO interface field with the waiting period, in milliseconds, before answering an incoming FXO call.

If this delay expires before the caller ID signal is decoded, the call proceeds without caller ID information.

If a minimal waiting period is required for the selected country, the highest of both values is used.

Figure 56: FXO Answering Configuration Section



2. Set the corresponding *Answering On Caller ID Detection* column's drop-down menu with the proper behaviour.

This parameter enables answering upon caller ID detection instead of the waiting delay configured in Step 1.

When enabled, an incoming FXO call is answered on the first occurrence of either:

- The reception of the caller ID signal.
- The expiration of the delay configured by the *Wait Before Answering Delay* field and the country wait before answering delay.

3. Set the corresponding *Wait For Callee To Answer* column's drop-down menu with the proper behaviour.

When the endpoint is set up for automatic call (see [“Automatic Call” on page 387](#)), enabling this variable makes the endpoint wait until the called the party connection is established before answering the incoming call.

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

FXO Incoming Call Configuration

This section allows you to define how each line behaves when there is an incoming call.

► **To set FXO incoming call parameters:**

- In the *FXO Incoming Call Behavior* section, set the corresponding *Not Allowed Behavior* column's drop-down menu with the proper behaviour.
Under certain circumstances (locked port, configuration, etc.), incoming FXO calls are not allowed. When that is the case, the FXO endpoint behaves in one of the manners below.

Table 100: Not Allowed Behavior Parameters

Parameter	Description
Do Not Answer	The incoming call is left unanswered.
Play Congestion Tone	The incoming call is answered, a congestion tone is played for 10 seconds, and then the call is terminated.

Figure 57: FXO Incoming Call Behavior Section



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

FXO Custom Basic Parameters

Overrides the default country basic parameters for this FXO line.

The parameters can be set:

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

► **To override the FXO Custom Basic Parameters:**

- In the *potsMIB* set:
 - *OverrideDefaultCountryParameters* parameter in the *FxoCustomBasicParameters* table
 - *Impedance* parameter in the *FxoCustomBasicParameters* table
- Use the CLI or a configuration script:
 - `Pots.FxoCustomBasicParameters[index=value].OverrideDefaultCountryParameters="value"`

Where value can be:

enable: The FXO line uses the custom values as defined in the current row. To reset the parameter values to the default country values, use the Reset row command.

disable: The FXO line uses the default country values. The values set in the current row are not applied.

- `Pots.FxoCustomBasicParameters[index=value].Impedance="value"`

Where value equals:

Table 101: Impedance Values

Value	Meaning	Description
100	I600	Impedance of 600 ohms. (Used in North America)
200	I600LongLoop	ANSI/EIA/TIA 464 compromise impedance for trunks.

Table 101: Impedance Values

Value	Meaning	Description
300	I900	Impedance of 900 ohms.
400	Australia	Impedance used in Australia
500	Austria	Impedance used in Austria
600	Belgium	Impedance used in Belgium
700	Brazil	Impedance used in Brazil
800	China	Impedance used in China
900	Czech Republic	Impedance used in Czech Republic
1000	Denmark	Impedance used in Denmark
1100	Finland	Impedance used in Finland
1200	France	Impedance used in France
1300	Germany	Impedance used in Germany
1400	Greece	Impedance used in Greece
1500	Italy	Impedance used in Italy
1600	Japan	Impedance used in Japan
1700	Netherlands	Impedance used in Netherlands
1800	New Zealand	Impedance used in New Zealand
1900	Norway	Impedance used in Norway
2000	Russia	Impedance used in Russia
2100	Slovakia	Impedance used in Slovakia
2200	Spain	Impedance used in Spain
2300	Sweden	Impedance used in Sweden
2400	UK	Impedance used in UK

FXO Line Verification

The line state verification mechanism allows the detection of defective or down lines based on the absence of current when closing the loop. You can view the line state in the *FXO Line State* table ([“FXO Line Status” on page 128](#)).

► **To set FXO line verification parameters:**

1. In the *FXO Line Verification* section, set the *Link State Verification* drop-down menu with the proper behaviour.

Figure 58: FXO Answering Configuration Section



2. Set the *Link State Verification Timeout* field with the value, in milliseconds, indicating how long the unit waits to successfully take the line before considering the line is defective or down.
3. Click *Submit* if you do not need to set other parameters.

FXO Force End of Call

FXO Force end of call, also known as Far End Disconnect, refers to methods for detecting that a remote party has hung up. If the Far End Disconnect signal is not sent to or properly detected by the Mediatrix unit, the connection will not be released by the unit, thus freezing the FXO line in the off hook state.

The *FXO Force End of Call* section allows you to define various methods to detect a far end disconnect.

► **To set FXO force end of call parameters:**

1. In the *FXO Force End of Call* section, set the *Force End Of Call On Call Failure* drop-down menu with the proper behaviour.

This parameter enables or disables forced-end-of-call on call failure.

The forced end of call on call failure occurs when a SCN caller tries to reach someone on the IP network and the SCN caller hangs up before reaching the IP callee.

If the connection is not established, the Mediatrix unit cannot detect that the caller has hung up. You can configure the Mediatrix unit to disconnect an unsuccessful communication after a specific number of seconds. This number of seconds is defined in a timeout that starts to count when the SCN caller contacts the Mediatrix unit. If the connection is not successful, the line is closed when the call time reaches the defined timeout value.

This feature forcefully terminates a call that stayed in an error state for some time. When the line falls in an error state where a SIT, a ROH, a BUSY or any error tone is played outbound to the FXO line, the unit waits for the timeout specified in the *Call Failure Timeout* field and then hangs up.

Figure 59: FXO Force End of Call Section



2. Set the *Call Failure Timeout* field with the waiting period, in seconds, before terminating a call in an error state.
3. Set the *Forced End Of Call On Silence Detection Mode* drop-down menu with the proper behaviour.

This parameter enables or disables forced-end-of-call on silence detection.

The silence detection feature applies when two parties are in communication and one of them hangs up. It allows the Mediatrix unit to close a line when no voice activity or silence is detected for a specified amount of time.

When silence is detected on the IP and/or SCN side for an amount of time specified in a timeout, the call is terminated. This feature is useful to free resources in the event of an IP network failure that prevents the end of call to be detected or when the SCN end of call tone was not detected.



Note: The silence detection feature could inadvertently disconnect a communication when one party puts the other on hold. Using the hold tone can prevent detection of silence when the call is put on hold by the IP peer. See [“Tone Override” on page 412](#) for more details.

The current implementation of silence detection relies on the power of the media signal. A silence is detected if the power level of the media signal is lower than -60 dBm.

This feature forcefully terminates a call that stayed silent for some time. When silence is detected on the inbound and/or outbound media for an amount of time specified in the *Silence Detection Timeout* field, the call is terminated.

Table 102: Forced End of Call on Silence Detection Mode Parameters

Parameter	Description
Disable	Forced-end-of-call on silence detection is disabled.
Inbound And Outbound Silent	The call is terminated if both inbound and outbound media are silent at the same time.

This feature is useful to free resources in the event of a network failure preventing the end-of-call to be detected or when the FXO end-of-call tone was not detected.

4. Set the *Silence Detection Timeout* field with the maximum amount of time, in seconds, that a call can remain silent, before it is terminated and the line is released.
5. Set the *Forced End Of Call On Tone Detection Mode* drop-down menu with the proper behaviour.

This parameter enables or disables forced-end-of-call upon tone detection. It terminates a call upon detection of an end-of-call tone on the inbound from the FXO line.

Table 103:

Parameter	Description
Disable	Force-end-of-call upon tone detection is disabled.
Country Tone	The unit tries to detect the tone specified for this purpose in the current country's tone specification. Some country specifications omit this information. In that case, the unit behaves as if the parameter is Disable .
Custom Tone	Terminates a call upon detection of a custom tone. See Steps 6-8.

The Mediatrix unit can monitor special tones that indicate the remote SCN user has hung up. You can use the default value for a selected country or customize a tone. [Table 104](#) lists the default frequency and cadence detected by supported country.

Table 104: Default Frequency and Cadence Supported

Country	Frequency	Cadence				
		ON1 (s)	OFF1 (s)	ON2 (s)	OFF2 (s)	Repetition
Austria	450 Hz	8.0	0.0	0.0	0.0	1
Czech Republic	425 Hz	8.0	0.0	0.0	0.0	1
France	440 Hz	8.0	0.0	0.0	0.0	1
Germany	425 Hz	8.0	0.0	0.0	0.0	1
Italy	425 Hz	0.2	0.2	0.6	1.0	4
North America	440 Hz	8.0	0.0	0.0	0.0	1
Spain	425 Hz	8.0	0.0	0.0	0.0	1
Switzerland	425 Hz	8.0	0.0	0.0	0.0	1

When customizing a tone, Media5 suggests to ask your Central Office about the tone it generates to indicate a call has been disconnected. You will thus be able to customize your tone according to this information.

Custom Tone Settings

6. If you have selected **Custom Tone** in Step 5, set the *Tone Detection Custom Frequency* field with the Frequency, in Hertz (Hz), to detect in the custom cadence.

You can set any value between 350 Hz and 620 Hz.

A customized tone detection can only detect a single frequency. To detect tones made of multiple frequencies, create the cadence for only one of the frequencies found in the tone.

7. Set the *Tone Detection Custom Cadence* field with the cadence to detect.

A cadence is a series of frequencies that are played for a specified time, making up a tone. The format for a cadence is:

on1,off1,on2,off2,on3,off3

In this string, “on” and “off” are numerical values representing the time, in milliseconds, that the frequency can and cannot be detected, respectively. For instance, “2000, 1000, 2000, 0” is a cadence in which the frequency plays for 2 seconds, stops for 1 second, and plays for 2 more seconds. This example is also equivalent to setting the string “2000, 1000, 2000”.

You can specify up to three “on,off” pairs. If you specify less than those six values, “0” values will be added as necessary. Specifying more than six will only use the six first values.

A cadence starting with a value of zero (0) is invalid. The first zero (0) found in the string signals the end of the cadence (i.e. “200, 0, 300” is the same as “200”).

- To detect a continuous tone, use a single “on” value, e.g., “200, 0” or “200” (the off time is 0 ms.). A continuous tone of 200 ms is used if the field is empty.
- To detect a tone in which two or more frequencies are used, for instance with a cadence of “200 ms, 500 ms, 300 ms, 400 ms”, in which the respective frequencies would be “400 Hz, 300 Hz, 400 Hz, 500 Hz”, detect a frequency that comes twice or more in the tone. In the above example, detect the 400 Hz frequency by using the cadence “200 ms, 400 ms, 300 ms, 500 ms”. In this example, the 400 ms and 500 ms off times represent the times that the 400 Hz frequency cannot be heard, even though another frequency may be playing.

The “on” and “off” values can be from 0 to 32767 ms.

8. Set the *Detection Custom Repetition* field with the number of times the custom cadence must be detected to consider the custom end-of-call tone has been detected.
9. Click *Submit* if you do not need to set other parameters.

ISDN Parameters

Page Left Intentionally Blank

CHAPTER

23

ISDN Configuration

This chapter describes how to configure the Integrated Services Digital Network (ISDN) Basic Rate Interfaces (BRI) and/or Primary Rate Interfaces (PRI) parameters of the Mediatrix unit.



Note: This web page is not available on the Mediatrix LP/4100/C7 Series models.

Introduction

ISDN is a set of digital transmission protocols defined by a few international standards body for telecommunications, such as the ITU-T. One or another of these protocols are accepted as standards by virtually every telecommunications carrier all over the world.

ISDN replaces the traditional telephone system so that one or two pairs of telephone wires can carry voice and data simultaneously. It is a fully digital network where all devices and applications present themselves in a digital form.

ISDN is a User-Network Interface (UNI) signalling protocol with a user and a network side. The user side is implemented in ISDN terminals (phones, terminal adapters, etc.) while the network side is implemented in the exchange switches of the network operator. Both sides have different signaling states and messages. The Mediatrix unit ISDN interfaces can be configured to work as user (TE) or network (NT) interfaces.

Depending on your product, you can configure two types of ISDN interfaces:

- ▶ The ISDN Basic Rate Interface (BRI) – Mediatrix 3404, 3408, 3734, 3741, 3742, and 4400 Series models.
- ▶ The ISDN Primary Rate Interface (PRI) – Mediatrix 3531, 3532, 3621, 3631, 3632, 3731, 3732, and 3734 models.

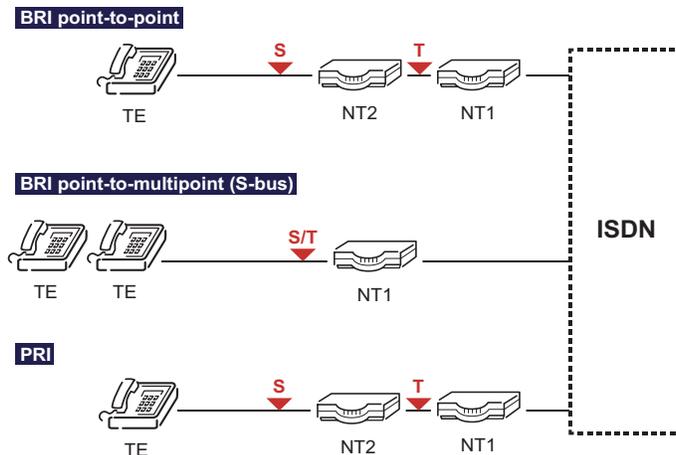
ISDN Reference Points

ISDN specifies a number of reference points that define logical interfaces between the various equipment types on an ISDN access line. The Mediatrix unit supports the following ISDN reference points:

- ▶ **S:** The reference point between user terminals and the NT2. This is used in point-to-multipoint BRI connections.
- ▶ **T:** The reference point between NT1 (Modem) and NT2 (PBX) devices. This is used in point-to-point PRI/BRI connections.

All other ISDN reference points are not supported.

Figure 60: ISDN Reference Points



Inband Tones Generation

In an ISDN network, most of the call setup tones are played locally by the TE equipment (i.e., telephone handset), although some require that the tones be played inband by the NT.

When interworking with other networks occurs, the need for the tones to be played inband is more likely to arise.

The Mediatrix unit may enable inband tones to be played locally, on a per-interface basis. This option is present when the unit is acting as both the NT and the TE UNI-side. However, in TE mode, only the ringback tone is played.

The Call Setup tones (dial tone, ringback tone, etc.) are played in the direction where the call has been initiated. The call disconnection tones are played in both directions, but of course will not arrive to the peer who disconnected the call.

When an inband tone is played, a Progress Indicator information element (IE) #8 “*Inband information or appropriate pattern available*” is added to the ISDN message corresponding to the call state change, and in a PROGRESS ISDN message if no state change is occurring.

When an interface is acting as the TE, as soon as the NT advertises that it plays inband tones through a Progress Indicator IE #8 or #1, the local inband tones generation is disabled for the rest of the call.

Whenever a tone is played inband locally or the ISDN peer advertises that inband informations are available, the Mediatrix unit is notified. The IP media path can then be opened earlier in the call, and can be closed with some delay after the call disconnection initiation.

The following table summarizes the inband tones generation behaviour for the NT mode.

Table 105: Inband Tones Generation Behaviour - NT

Signal IE Handling Enabled	Inband Tones Generation Enabled	Inband Tone Played
No	No	No
No	Yes	Yes
Yes	Don't care	No

The following table summarizes the inband tones generation behaviour for the TE mode.

Table 106: Inband Tones Generation Behaviour - TE

Signal IE Handling Enabled	Signal IE Received	Inband Tones Generation Enabled	NT Peer Advertised Inband Tones	Inband Tone Played
No	Don't care	No	Don't care	No

Table 106: Inband Tones Generation Behaviour - TE (Continued)

Signal IE Handling Enabled	Signal IE Received	Inband Tones Generation Enabled	NT Peer Advertised Inband Tones	Inband Tone Played
Yes	Yes	No	Don't care	Yes
Yes	No	Don't care	Don't care	No
No	Don't care	Yes	Yes	No

Note that when the PRI/BRI interface *Signalling Protocol* drop-down is set to **QSIG**, the Signal IE does not exist so it has no effect on the inband tones generation. In QSIG, inband tones are played when the inband tones generation is activated on the incoming side of the call. See [“PRI Configuration” on page 155](#) or [“BRI Configuration” on page 167](#) for more details.

Signal Handling

The Signal IE is used by the NT ISDN side to tell its TE peers that they must generate an inband tone locally. Thus, the Signal IEs are sent by the NT only.

When the Signal IE handling is enabled on a given ISDN interface acting as a TE, inband tones are played towards the IP side when a Signal IE is received. On a NT interface, a Signal IE is inserted in the ISDN messages sent to the TE when appropriate.

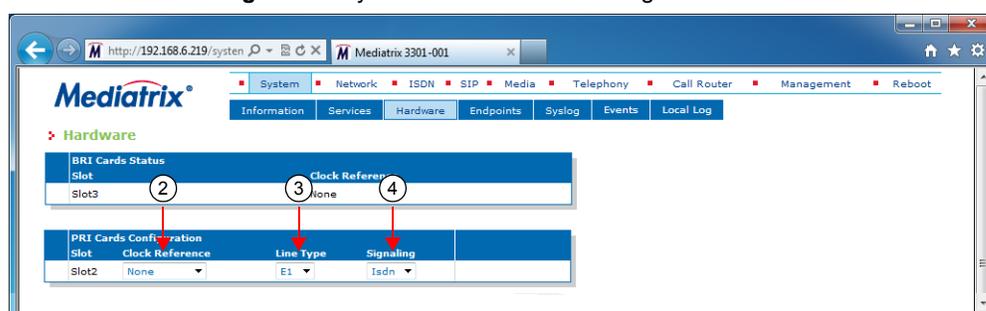
Note that when the Mediatrix 3500 Series signaling protocol is set to “NI-2” (National ISDN-2) on that interface, the Signal IE handling is forced to be enabled for a NT.

Setting PRI Hardware Parameters

You must set hardware-related parameters. You can do so in the *System / Hardware* page. The *Hardware* page differs depending on the product and model you have.

► To configure the Mediatrix unit hardware:

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

Figure 61: System – Hardware Web Page

2. In the *PRI Cards Configuration* section, select the reference of the clock source in the *Clock Reference* drop-down menu.

If you want to configure the clock reference of a specific interface, you must set the *Endpoint Type* drop-down menu to **NT**. See [“PRI Configuration” on page 155](#) for more details.

Table 107: Clock Reference

Reference	Description
None	The internal clock does not synchronize with any other source.

Table 107: Clock Reference (Continued)

Reference	Description
Other Card	The internal clock synchronizes with the other PRI interface of the Mediatrrix unit. This interface must be configured in TE mode (<i>Endpoint</i> drop-down menu of the <i>Interface Configuration</i> section) to provide the clock reference to the other interfaces. Note: This choice is not available on the Mediatrrix 3531, 3621 and 3631 models.

- Select whether the line uses *T1* or *E1* in the *Line Type* drop-down menu.
You must restart the unit if you change this setting.
- Select the **ISDN** signaling in the *Signaling* drop down menu.
When changing from R2 to ISDN or ISDN to R2, you must change your routes accordingly. For instance, if you are in R2 with a route *r2-Slot2/E1T1*, then change to ISDN, you must change the route to *isdn-Slot2/E1T1*.
This parameter is available only for the Mediatrrix 3621/3631/3632 models. Other models support only the ISDN protocol.
- Click *Submit* if you do not need to set other parameters.

ISDN Auto-Configuration

The ISDN Auto-configuration feature allows you to detect and to configure all ISDN interfaces so that the ISDN link goes up and becomes usable with a minimal user interaction. When launching an auto-configuration process, it stops automatically when all interfaces have been tested. For each interface, the auto-configuration process is considered successful when the link becomes up or a failure when all combinations have been tried without having a link up.



Caution: Launching the auto-configuration may terminate abruptly all ongoing ISDN calls.



Note: Auto-configuration on all ISDN interfaces may take some time to complete. Some of the current ISDN settings might be replaced by new values.

Please note that some parameters cannot be auto configured. For instance, the clock mode is configured according to the endpoint type, master for NT and slave for TE.

► To launch the auto-configuration process:

- In the web interface, click the *ISDN* link, then the *Status* sub-link.

Figure 62: ISDN – Status Configuration Section



- Click the **Start Sensing** button.
The process starts.

Preset

The *ISDN Preset Configuration* section allows you to load a set of preset configuration for your ISDN connections. These preset files are located in the file system's persistent memory. They differ depending on the Mediatrix unit you are using. Depending on your unit's profile, it may be possible that no preset files are available.

Using preset files is especially useful for units that do not use the default values provided by Media5 (for instance, T1 instead of E1 for Mediatrix 3000 units). Please note that only script files work. Any other type of file present in the file system cannot be run here.

You can also export your current ISDN configuration in a preset. Please note that these user-defined presets are not kept in the event of a partial or factory reset.

To see the content of the unit's file system persistent memory, go to File Manager (["Chapter 53 - File Manager" on page 543](#)). All installed configuration scripts/images are listed.

► To load and execute a preset file:

1. In the *ISDN Status* tab, *ISDN Preset Configuration* section, select one of the available preset files in the *Local Preset* drop-down menu.

Figure 63: ISDN – Status Configuration Section



2. Click **Apply**.
The configuration is applied.

► To export the current ISDN configuration as a preset:

1. In the *ISDN Preset Configuration* section, type a name for the preset in the *Preset Name* field.

Figure 64: ISDN – Status Configuration Section



2. Click **Save**.
The current ISDN configuration is exported. Please note that these user-defined presets are not kept in the event of a partial or factory reset.
When the clock device is not synchronized, the description value of the file is "Automatically Generated". When synchronized, the description is "Automatically Generated on Date/Time". See the File Manager (["Chapter 53 - File Manager" on page 543](#)) for more details on how to see and manage the files in the unit's file system.

Partial Reset

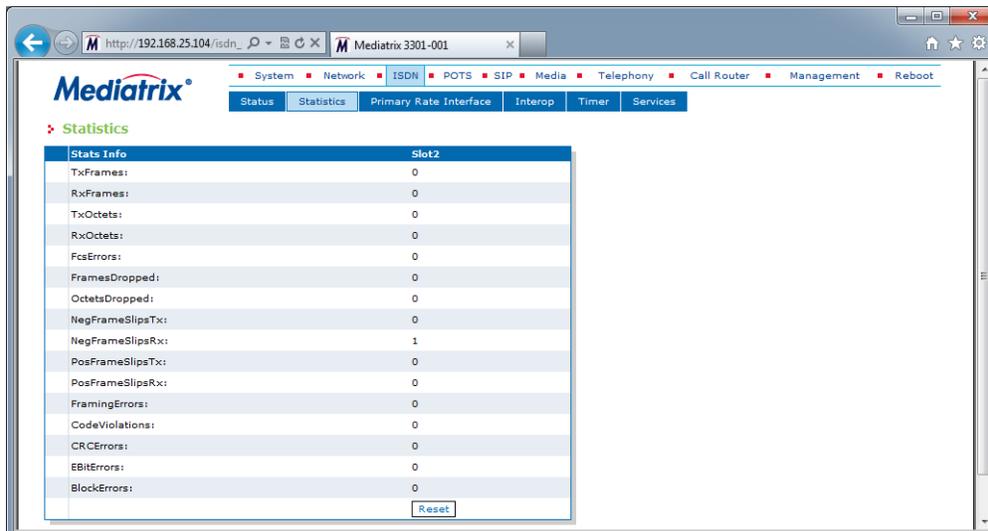
When a partial reset is triggered, the user-defined presets are deleted.

PRI ISDN Statistics

The Mediatrix unit collects meaningful statistics for each PRI digital card that can be read via the web interface. These statistics are also available via SNMP and CLI.

The Mediatrix unit collects statistics for each of its two cards, if available. Slot 2 and Slot 3 indicate the physical location of the cards in the unit, Slot 2 being on the left when looking at the rear of the unit. You can click the **Reset Stats** button at any time to reset all statistics for the specified interface.

Figure 65: ISDN – Statistics Web Page



The following table describes the statistics available.

Table 108: ISDN Statistics Displayed

Statistic	Description
TxFrames	Number of HDLC frames transmitted. Note: The term frames does not refer to the structure defined in I.431.
RxFrames	Number of HDLC frames received. Note: The term frames does not refer to the structure defined in I.431.
TxOctets	Number of octets transmitted. This value is obtained by cumulating the octets transmitted in the HDLC frames. Note: The term frames does not refer to the structure defined in I.431.
RxOctets	Number of octets received. This value is obtained by cumulating the octets received in the HDLC frames. Note: The term frames does not refer to the structure defined in I.431.
FcsErrors	Frame check sequence (FCS) errors indicate that frames of data are being corrupted during transmission. FCS error count is the number of frames that were received with a bad checksum (CRC value) in the HDLC frame. These frames are dropped and not propagated in the upper layers. This value is available on E1 and T1.
FramesDropped	Number of frames dropped. This value is obtained by cumulating the number of frames dropped when transferring the data from the framer chip to the device internal buffer. This value is available on E1 and T1.
OctetsDropped	Number of octets dropped. This value is obtained by cumulating the number of octets dropped when transferring the data from the framer chip to the device internal buffer. This value is available on E1 and T1.

Table 108: ISDN Statistics Displayed (Continued)

Statistic	Description
NegFrameSlipsTx	A frame is skipped when the frequency of the transmit clock is greater than the frequency of the transmit system interface working clock based on 2.048 MHz (on E1) or 1.544 MHz (on T1). This value is available on E1 and T1.
NegFrameSlipsRx	A frame is skipped when the frequency of the received route clock is greater than the frequency of the receive system interface working clock based on 2.048 MHz (on E1) or 1.544 MHz (on T1). This value is available on E1 and T1.
PosFrameSlipsTx	A frame is repeated when the frequency of the transmit clock is less than the frequency of the transmit system interface working clock based on 2.048 MHz (on E1) or 1.544 MHz (on T1). This value is available on E1 and T1.
PosFrameSlipsRx	A frame is repeated when the frequency of the receive route clock is less than the frequency of the receive system interface working clock based on 2.048 MHz (on E1) or 1.544 MHz (on T1). This value is available on E1 and T1.
FramingErrors	The framing error count indicates that a FAS (Frame Alignment Signal) word has been received with an error. The FAS-bits are present in every even frame of timeslot 0 on E1. The FAS-bits are present in ESF format on T1. This value is available on E1 and T1.
CodeViolations	The code violations count indicates that an encoding error on the PCM line has been detected. This value is available on E1 and T1.
CRCErrors	The CRC errors count is incremented when a multiframe has been received with a CRC error. The CRC error count is available in CRC multiframe mode only on E1. The CRC error count is in ESF format on T1.
EBitErrors	The E-Bit error count gives information about the outgoing transmit PCM line if the E-bits are used by the remote end for submultiframe error indication. Incrementing is only possible in the multiframe synchronous state. Due to signaling requirements, the E-bits of frame 13 and frame 15 of the CRC multiframe can be used to indicate an error in a received submultiframes: <pre> Submultiframe I status E-bit located in frame 13 Submultiframe II status E-bit located in frame 15 no CRC error : E = 1 CRC error : E = 0 </pre> This value is only available in E1.
BlockErrors	The Block Error count is incremented once per multiframe if a multiframe has been received with a CRC error or a bad frame alignment has been detected. This value is only available for ESF format on T1 only.

PRI Configuration

This section applies to the following models:

- ▶ Mediatrix 3531
- ▶ Mediatrix 3532
- ▶ Mediatrix 3621
- ▶ Mediatrix 3631
- ▶ Mediatrix 3632
- ▶ Mediatrix 3731
- ▶ Mediatrix 3732
- ▶ Mediatrix 3734

The Primary Rate Interface (PRI) port supports 30 x 64 kbit/s B-channels, 1 x 64 kbit/s D-channel and 1 x synchronization timeslot on a standard E1 (G.704) physical layer. In its T1 version, a PRI interface supports 23 x B-channels and 1 x D-channel, all at a 64 kbit/s rate. E1 is mostly deployed in Europe, while T1 is more present in North America.



Caution: You can configure ISDN ports while they are active. However they are internally disabled to modify the configuration and then re-enabled. All active calls on the port are dropped during this process. Configuration changes should only be performed during planned down times. Most of the ISDN parameters change require a restart of the ISDN service to be applied.

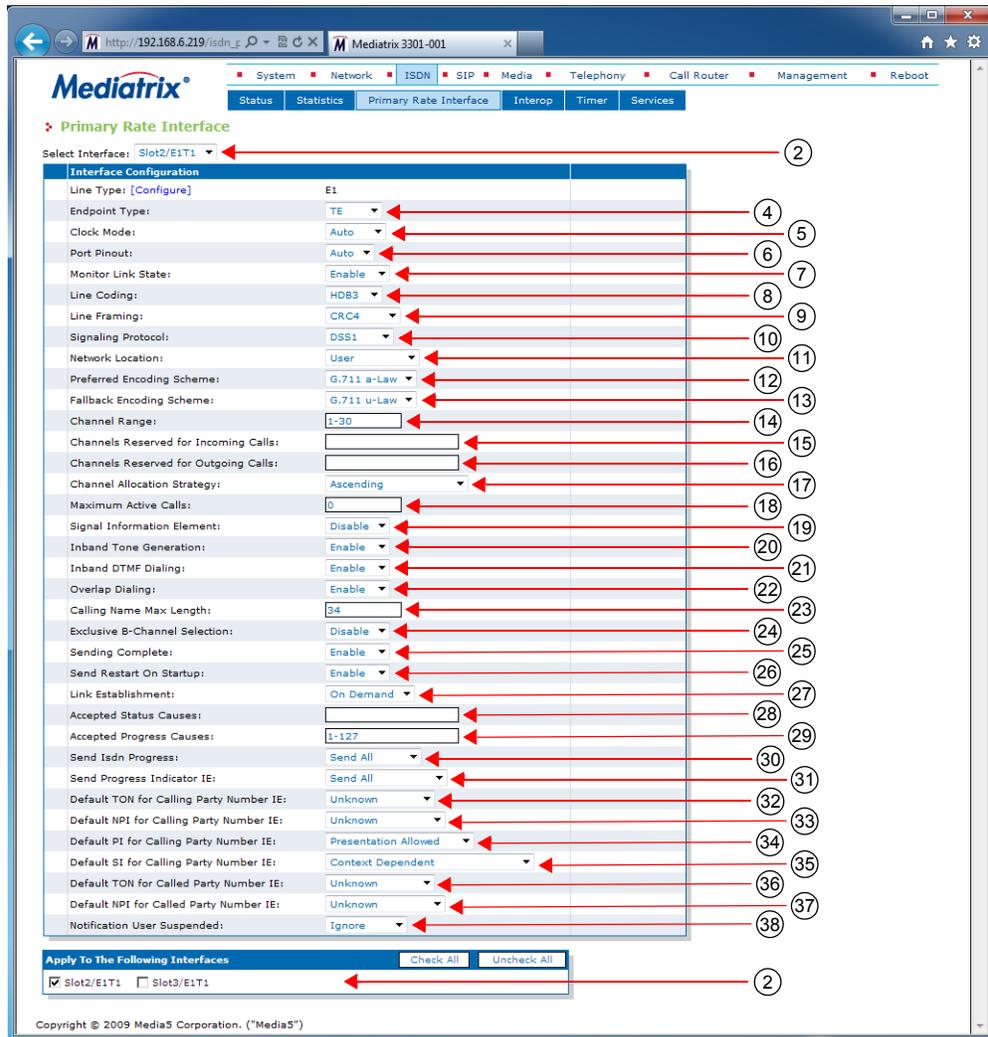


Caution: The Mediatrix unit PRI ports can be used as a T reference point, but not as U reference points (2-wire). Never connect a U SCN line or a U TE into the Mediatrix unit PRI ports.

► To configure the PRI parameters:

1. In the web interface, click the *ISDN* link, then the *Primary Rate Interface* sub-link.

Figure 66: ISDN – Interface Configuration Section



2. Select to which interface you want to apply the changes in the *Select Interface* drop-down menu at the top of the window.

You can copy the configuration of the selected interface to one or more interfaces of the Mediatrix unit in the *Apply to the Following Interfaces* section at the bottom of the page. You can select specific interfaces by checking them, as well as use the *Check All* or *Uncheck All* buttons.

The Mediatrix 3532 and 3632 models have two interfaces.

3. If applicable, use the *Line Type Configure* link to set the line type, as described in “[Setting PRI Hardware Parameters](#)” on page 151.
4. Select the endpoint type in the *Endpoint Type* drop-down menu.

Table 109: Endpoint Type

Type	Description
TE	Terminal Equipment. The endpoint emulates the subscriber (terminal) side of the digital connection. You can connect the SCN to the endpoint.

Table 109: Endpoint Type (Continued)

Type	Description
NT	Network Termination. The endpoint emulates the central office (network) side of the digital connection. You can connect a PBX to the endpoint.

The setting used for the Mediatrix unit must be opposite to the setting used in the PBX. For instance, if the PBX is set to *TE*, then the Mediatrix unit must be set to *NT*.



Note: If you want to use a specific interface as the reference clock, you must set it to **TE**.

When the PRI interface *Signalling Protocol* drop-down is set to **QSIG** (see Step 9), the endpoint type is only used in the second layer (LAPD) since it is a concept that does not exist in QSIG.

5. Select the clock mode of the interface in the *Clock Mode* drop-down menu.

The interface can either generate the clocking for the line or accept the clock from the line.

Table 110: Clock Mode

Mode	Description
auto	The setting is derived from the endpoint type. <ul style="list-style-type: none"> • NT: clock master • TE: clock slave
Master	The interface generates the clock.
Slave	The interface accepts the clock from the line.

The clock mode is used to give the user the possibility to set an endpoint in TE mode and still generate the clock by specifying the clock mode to master. The clock source can then be selected from the *Clock Reference* drop-down menu (see [“Setting PRI Hardware Parameters” on page 151](#) for more details). The clock mode could be used, for instance, to synchronize several units in NT mode via a T1 or E1 line.

6. Select the port pinout in the *Port Pinout* drop-down menu.

Table 111: Port Pinout

Mode	Description
Auto	The pinout is set according to the Endpoint Type parameter setting (Step 4).
Te	Forces the pinout to TE regardless of the Endpoint Type value.
Nt	Forces the pinout to NT regardless of the Endpoint Type value.

7. Set the *Monitor Link State* drop-down menu with the physical link state of the ISDN interface.

Table 112: Interface Link State

Parameter	Description
Enable	The ISDN endpoint's operational state is affected by its interface physical link state. When the link state of the ISDN interface is down, the operational state of its matching endpoint becomes “disable”.
Disable	The ISDN endpoint's operational state is not affected by its interface physical link state.

Note that if the *Monitor Link State* parameter is enabled and the *Ignore SIP OPTIONS on no usable endpoints* parameter is also enabled in the *SIP / Interop* page, this will influence how the SIP options are answered. See [“SIP Interop” on page 279](#) for more details.

8. Select the transmission encoding of bits in the *Line Coding* drop-down menu.

Table 113: Transmission Encoding

Coding	Description
B8ZS	Bipolar with 8-Zeros Substitution (T1 lines).
HDB3	High-Density Bipolar with 3-zeros (E1 lines).
AMI	Alternate Mark Inversion (E1 and T1 lines).

Make sure that the transmission encoding matches with the remote system. For further information, see ITU-T Recommendation G.703.

9. Select the frame format in the *Line Framing* drop-down menu.

Line Framing is used to synchronize the channels on the frame relay circuit (when a frame starts and finishes). Without it, the sending and receiving equipment would not be able to synchronize their frames.

Table 114: Line Framing

Format	Description
SF	Super frame. Sometimes known as D4 (T1 lines).
ESF	Extended super frame (T1 lines).
CRC4	Cyclic redundancy check 4 (E1 lines).
NO-CRC4	No Cyclic redundancy check 4 (E1 lines).

For further information, see ITU-T Recommendation G.704.

10. Select the protocol to use for the signalling channel in the *Signalling Protocol* drop-down menu.

This signalling must match the connected ISDN equipment or network.

Table 115: Signalling Protocols

Protocol	Description
DSS1	Digital Subscriber Signaling System No.1
DMS100	Digital Multiplex System 100
NI2	National ISDN No.2
5ESS	5 Electronic Switching System
QSIG	ECMA's protocol for Private Integrated Services Networks

The 5ESS and DMS100 protocols support basic call only and the model is derived directly from the DSS1 protocol.

If you select the NI2 protocol, see [“Information Following Operation” on page 166](#) for the behaviour if this parameter is present.

11. Select the value of the network location in the progress indicator messages that the unit sends in the *Network Location* drop-down menu.

This defines the location code to be inserted in ISDN causes code information elements, i.e., the type of network to which the system belongs. The following values are available:

- User
- Private
- Public
- Transit

- International

12. Set the *Preferred Encoding Scheme* drop-down menu with the data encoding scheme in the bearer capabilities (user information layer 1 protocol).

This encoding scheme is used when initiating a call on the ISDN side. The supported encoding schemes are *G.711 u-Law* and *G.711 a-Law*.

G.711 u-Law may not be supported by DSS1 NT and TE endpoints. It is recommended to use *G.711 a-Law* as preferred encoding protocol.

13. Set the *Fallback Encoding Scheme* drop-down menu with the fallback data encoding scheme in case the preferred encoding scheme is not available.

The supported encoding schemes are *G.711 u-Law* and *G.711 a-Law*.



Note: The fallback encoding scheme is valid only when receiving a SETUP message. The user sending the SETUP message does not indicate alternative bearer capability.

If the proposed encoding scheme in the bearer capability received in the SETUP message is different than the preferred encoding scheme, then the fallback encoding scheme is used.

14. Define the range of active bearer channels in the *Channel Range* field.
15. Define the range to reserve channels for incoming calls in the *Channels Reserved for Incoming Calls* field.

Bearer channels are by default usable for both incoming and outgoing calls. Use this range to reserve channels for incoming calls.



Note:

- Channels outside of the range defined by the *Channel Range* field are ignored.
- Channels reserved in both the *Channels Reserved for Incoming Calls* and *Channels Reserved for Outgoing Calls* fields are considered usable for both incoming and outgoing calls.

The string has the following syntax:

- ',': Separator between non-consecutive lists of channels or single channels.
- 'n': A single channel, where n is the channel number.
- 'm-n': List of channels where m is the start channel number and n is the end channel number.



Note: The space character is ignored and duplication is not allowed. Channels must be specified in low to high order.

Example: '1,12-15': The accepted channels are 1, 12, 13, 14 and 15.

16. Define the range to reserve channels for outgoing calls in the *Channels Reserved for Outgoing Calls* field.

Bearer channels are by default usable for both incoming and outgoing calls. Use this range to reserve channels for outgoing calls.



Note:

- Channels outside of the range defined by the *Channel Range* field are ignored.
- Channels reserved in both the *Channels Reserved for Incoming Calls* and *Channels Reserved for Outgoing Calls* fields are considered usable for both incoming and outgoing calls.

The string has the following syntax:

- ',': Separator between non-consecutive lists of channels or single channels.
- 'n': A single channel, where n is the channel number.

- 'm-n': List of channels where m is the start channel number and n is the end channel number.



Note: The space character is ignored and duplication is not allowed. Channels must be specified in low to high order.

Example: '1,12-15': The accepted channels are 1, 12, 13, 14 and 15.

17. Select the strategy for selecting bearer channels in the *Channel Allocation Strategy* drop-down menu.

Table 116: Channel Allocation Strategy

Allocation	Description
Ascending	Starting from the lowest-numbered non-busy bearer channel and going toward the highest-numbered non-busy bearer channel, the Mediatrix unit selects the first bearer channel available.
Descending	Starting from the highest-numbered non-busy bearer channel and going toward the lowest-numbered non-busy bearer channel, the Mediatrix unit selects the first bearer channel available.
RoundRobinAscending	The Mediatrix unit starts from the bearer channel that follows the bearer channel used for the last call. For instance, if channel #1 was used in the last call, the unit starts with channel #2. Going toward the highest-numbered non-busy bearer channel, the unit selects the first channel available. If the highest channel is unavailable, the search continues from the lowest-numbered non-busy bearer channel.
RoundRobinDescending	The Mediatrix unit starts from the bearer channel that precedes the bearer channel used for the last call. For instance, if channel #3 was used in the last call, the unit starts with channel #2. Going toward the lowest-numbered non-busy bearer channel, the unit selects the first channel available. If the lowest channel is unavailable, the search continues from the highest-numbered non-busy bearer channel.

18. Define the maximum number of active calls on the interface in the *Maximum Active Calls* field.
This limits the total number of concurrent calls on the interface. Entering **0** indicates no maximum number of active calls.
19. Select whether or not the signal information element is enabled in the *Signal Information Element* drop-down menu.
 - When activated at the Network UNI-side (*Endpoint Type* drop-down menu set to **NT**), the signal information element is sent to the User UNI-side.
 - When activated at the User UNI-side (*Endpoint Type* drop-down menu set to **TE**), the tone indicated in the signal information element is played in the IP direction.
20. Select whether or not inband tone generation is enabled in the *Inband Tone Generation* drop-down menu.
When activated at the User UNI-side (*Endpoint Type* drop-down menu is set to **TE**), only the ringback tone is generated.
When the *Signalling Protocol* drop-down menu is set to QSIG (Step 9) and this variable is activated, the incoming side of the call plays the tones inband.
21. Select whether or not inband DTMF dialing is enabled in the *Inband DTMF Dialing* drop-down menu.
If you select **Enable**, the Mediatrix unit accepts inband DTMF digits when Overlap Dialing occurs.

22. Select whether or not overlap dialing is enabled in the *Overlap Dialing* drop-down menu.

Table 117: Overlap Dialing Parameters

Parameter	Description
Enable	The Mediatix unit transports the called-party number digit by digit, after the first SETUP message, which contains no called party information at all.
Disable	The Mediatix unit transports the full called party information in the first SETUP message from the terminal. This means that the user must dial the number before going off-hook.

23. Define the maximum length of the calling party name for calls from SIP to ISDN in the *Calling Name Max Length* field.

Available values range from 0 to 82.

24. Select whether or not exclusive B-Channel selection is enabled for calls from SIP to ISDN in the *Exclusive B-Channel Selection* drop-down menu.

If you select **Enable** and initiate a call, only the requested B channel is accepted; if the requested B channel is not available, the call is cleared.

25. Select whether or not to enable the Sending Complete information element into SETUP messages for calls from SIP to ISDN in the *Sending Complete* drop-down menu.

Some ISDN switches may require that the Sending Complete information element be included in the outgoing SETUP message to indicate that the entire number is included and there are no further destination digits to be sent.

26. Select whether or not to enable sending the RESTART message upon a signalling channel "UP" event in the *Send Restart On Startup* drop-down menu.

The RESTART message requests a restart for the interface specified.

27. Set the link establishment strategy in the *Link Establishment* drop-down menu.

Table 118: Link Establishment Parameters

Parameter	Description
OnDemand	When the data link is shut down, the unit establishes a new link only when required.
Permanent	When the data link is shut down, the unit immediately attempts to establish a new link.

28. Set the STATUS causes that can be received without automatically clearing the call in the *Accepted Status Causes* field.

The default action is to clear the call upon receiving a STATUS message. If a STATUS message is received indicating a compatible call state and containing the supplied STATUS causes, the clearing of the call is prevented.

The string has the following syntax:

- ',': Separator between non-consecutive lists of causes or single cause.
- 'n': A single cause, where n is the cause number.
- 'm-n': List of causes where m is the start cause number and n is the end cause number.



Note: The space character is ignored and cause duplication is not allowed.

Causes must be specified in low to high order.

Example: '1,124-127': The accepted causes are 1, 124, 125, 126 and 127.

- 29. Set the range of PROGRESS causes accepted by the unit in the *Accepted Progress Causes* field. Causes excluded from this range trigger call disconnections.

The string has the following syntax:

- ',': Separator between non-consecutive lists of causes or single cause.
- 'n': A single cause, where n is the cause number.
- 'm-n': List of causes where m is the start cause number and n is the end cause number.

 **Note:** You must consider the following:

- The space character is not allowed.
- Causes must be specified in low to high order.
- Cause duplication is not allowed.

Example: '1,124-127': The accepted causes are 1, 124, 125, 126 and 127.

- 30. Select the strategy for sending ISDN Progress messages in the *Send Isdn Progress* drop-down menu.

Table 119: Send ISDN Progress Parameters

Parameter	Description
Send All	Send an ISDN Progress message in all situations where call progression is signaled.
Send Inband	Send an ISDN Progress message only when call progression contains an indication of in-band information.
Send Alerting	Send an ISDN Alerting message instead of ISDN Progress message when call progression contains an indication of in-band information. If call progression does not contain in-band information, no message is sent at this step.

The strategy for sending Progress messages should be adapted to the configuration of the peer ISDN switch. Some switches may terminate calls when receiving one or many ISDN progress messages.

- 31. Select the strategy for sending the Progress Indicator Information Element in the *Send Progress Indicator IE* drop-down menu.

Table 120: Send Progress Indicator IE Parameters

Parameter	Description
Send All	Send the Progress Indicator IE in all situations.
Send Inband Only	Send the Progress Indicator only when the Progress Description contains an indication of in-band information.

The strategy for the Progress Indicator IE should be adapted to the configuration of the peer ISDN switch.

This parameter controls sending of a Progress Indicator IE in ISDN messages where Progress Indicators are allowed. See the parameters in [“Interop Parameters Configuration” on page 178](#) for a control over which ISDN message allows Progress Indicators.

- 32. Select the default value to insert in the "Type of Number" parameter of the "Calling Party Number" IE when "Type of Number" is not already defined in the call properties in the *Default TON for Calling Party Number IE* drop-down menu.

 **Note:** A call property set by the "Properties Manipulation" feature of the Call Router has precedence over this default value. See [“Chapter 44 - Call Router Configuration” on page 431](#) for more details.

This parameter applies to the outgoing ISDN calls. Possible values are:

Table 121: Default TON for Calling Party Number IE Parameters

Parameter	Description
Unknown	Default value of Type of Number is set to Unknown.
International	Default value of Type of Number is set to International.
National	Default value of Type of Number is set to National.
Network Specific	Default value of Type of Number is set to Network-Specific.
Subscriber	Default value of Type of Number is set to Subscriber.
Abbreviated	Default value of Type of Number is set to Abbreviated.

33. Select the default value to insert in the "Numbering Plan Identification" parameter of the "Calling Party Number" IE when "Numbering Plan Identification" is not already defined in the call properties in the *Default NPI for Calling Party Number IE* drop-down menu.



Note: A call property set by the "Properties Manipulation" feature of the Call Router has precedence over this default value. See ["Chapter 44 - Call Router Configuration" on page 431](#) for more details.

This parameter applies to the outgoing ISDN calls. Possible values are:

Table 122: Default NPI for Calling Party Number IE Parameters

Parameter	Description
Unknown	Default value of Numbering Plan Identification is set to Unknown.
ISDN Telephony	Default value of Numbering Plan Identification is set to ISDN Telephony.
Data	Default value of Numbering Plan Identification is set to Data.
Telex	Default value of Numbering Plan Identification is set to Telex.
National Standard	Default value of Numbering Plan Identification is set to National Standard.
Private	Default value of Numbering Plan Identification is set to Private.

34. Select the default value to insert in the "Presentation Indicator" parameter of the "Calling Party Number" IE when "Presentation Indicator" is not already defined in the call properties in the *Default PI for Calling Party Number IE* drop-down menu.



Note: A call property set by the "Properties Manipulation" feature of the Call Router has precedence over this default value. See ["Chapter 44 - Call Router Configuration" on page 431](#) for more details.

If "Presentation Indicator" is not provided by the call properties, its value is determined by the following two steps.

- a. First, it is set to the default value defined by "DefaultCallingPi".
- b. Second, the "Presentation Indicator" can be overridden by the CLIP and CLIR services: the value can be set to "Restricted" by the CLIR service and the value can be set to "NotAvailable" if there is no number to forward. This variable applies to the outgoing ISDN calls.

Possible values are:

Table 123: Default PI for Calling Party Number IE Parameters

Parameter	Description
Presentation Allowed	Default value of Presentation Indicator is set to Presentation Allowed.
Presentation Restricted	Default value of Presentation Indicator is set to Presentation Restricted.
Not Available	Default value of Presentation Indicator is set to Not Available.

- 35. Select the default value to insert in the "Screening Indicator" parameter of the "Calling Party Number" IE when "Screening Indicator" is not already defined in the call properties in the *Default SI for Calling Party Number IE* drop-down menu.



Note: A call property set by the "Properties Manipulation" feature of the Call Router has precedence over this default value. See ["Chapter 44 - Call Router Configuration" on page 431](#) for more details.

This parameter applies to the outgoing ISDN calls. Possible values are:

Table 124: Default SI for Calling Party Number IE Parameters

Parameter	Description
User Provided Not Screened	Default value of Screening Indicator is set to User Provided Not Screened.
User Provided Verified And Passed	Default value of Screening Indicator is set to User Provided Verified And Passed.
User Provided Verified And Failed	Default value of Screening Indicator is set to User Provided Verified And Failed.
Network Provided	Default value of Screening Indicator is set to Network Provided.
Context Dependent	Screening Indicator is set to the value that makes the most sense according to run-time context.

- 36. Select the default value to insert in the "Type of Number" parameter of the "Called Party Number" IE when "Type of Number" is not already defined in the call properties in the *Default TON for Called Party Number IE* drop-down menu.



Note: A call property set by the "Properties Manipulation" feature of the Call Router has precedence over this default value. See ["Chapter 44 - Call Router Configuration" on page 431](#) for more details.

This parameter applies to the outgoing ISDN calls. Possible values are:

Table 125: Default TON for Called Party Number IE Parameters

Parameter	Description
Unknown	Default value of Type of Number is set to Unknown.
International	Default value of Type of Number is set to International.
National	Default value of Type of Number is set to National.

Table 125: Default TON for Called Party Number IE Parameters (Continued)

Parameter	Description
Network Specific	Default value of Type of Number is set to Network-Specific.
Subscriber	Default value of Type of Number is set to Subscriber.
Abbreviated	Default value of Type of Number is set to Abbreviated.

37. Select the default value to insert in the "Numbering Plan Identification" parameter of the "Called Party Number" IE when "Numbering Plan Identification" is not already defined in the call properties in the *Default NPI for Called Party Number IE* drop-down menu.



Note: A call property set by the "Properties Manipulation" feature of the Call Router has precedence over this default value. See "[Chapter 44 - Call Router Configuration](#)" on page 431 for more details.

This parameter applies to the outgoing ISDN calls. Possible values are:

Table 126: Default NPI for Called Party Number IE Parameters

Parameter	Description
Unknown	Default value of Numbering Plan Identification is set to Unknown.
ISDN Telephony	Default value of Numbering Plan Identification is set to ISDN Telephony.
Data	Default value of Numbering Plan Identification is set to Data.
Telex	Default value of Numbering Plan Identification is set to Telex.
National Standard	Default value of Numbering Plan Identification is set to National Standard.
Private	Default value of Numbering Plan Identification is set to Private.

38. Select the unit's behaviour when it receives a Notification Indicator IE with the description set to User suspended in the *Notification User Suspended* drop-down menu.

Possible values are:

Table 127: Notification User Suspended Parameters

Parameter	Description
Ignore	The Mediatrix unit ignores the Notification Indicator IE with description set to User suspended.
Disconnect	The Mediatrix unit disconnects the call on Notification Indicator IE with description set to User suspended.

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

InformationFollowing Operation

The "informationFollowing" operation is supported for NI2 signaling only (see "[PRI Configuration](#)" on page 155 for more details).

When a SETUP message is received containing an "informationFollowing" operation, the unit immediately sends a PROCEEDING message. The unit then waits normally for a FACILITY message containing the calling party name, for a maximum time configured with the *Maximum Facility Waiting Delay* parameter (see "[Interop Parameters Configuration](#)" on page 178 for more details).

The only difference between this behaviour and the usual behaviour (i.e. without the "informationFollowing" operation), is the immediate sending of the PROCEEDING message before waiting for the calling party name.

Note that the "informationFollowing" operation is mutually exclusive with the *Call Proceeding Delay* parameter (see "Interop Parameters Configuration" on page 178 for more details), which configures a delay before sending the PROCEEDING message. If the PROCEEDING message is sent due to the "informationFollowing" operation, *Call Proceeding Delay* parameter is ignored.

BRI Configuration

This section applies to the following models:

- ▶ Mediatrix 3404
- ▶ Mediatrix 3408
- ▶ Mediatrix 3734
- ▶ Mediatrix 3741
- ▶ Mediatrix 3742
- ▶ Mediatrix 4400 Series

A Basic Rate Interface (BRI) port supports 2 x 64 kbit/s B-channels for switched voice or data connections and 1 x 16 kbit/s D-channel for signalling.



Caution: The Mediatrix unit ISDN BRI ports are configurable to operate as network or terminal ports. The pin-out of the sockets is switched according to this configuration. Wrong port configurations, wrong cabling or wrong connections to neighbouring equipment can lead to short circuits in the BRI line powering. Refer to the *Hardware Installation Guide* to avoid misconfigurations.



Caution: The Mediatrix unit BRI ports can be used as a S or T reference point, but not as U reference points (2-wire). Never connect a U SCN line or a U TE into the Mediatrix unit BRI ports.

The Mediatrix 3404 / 3734 / 3741 / 3742 has 5 ISDN BRI ports. It supports up to 8 simultaneous ISDN voice/data channels over any IP connection.

The Mediatrix 3408 has 10 ISDN BRI ports. It supports up to 16 simultaneous ISDN voice/data channels over any IP connection.

The Mediatrix 4400 Series has up to 4 ISDN BRI ports depending on the model. It supports up to 8 simultaneous ISDN voice/data channels over any IP connection.

► To configure the BRI parameters:

1. In the web interface, click the *ISDN* link, then the *Basic Rate Interface* sub-link.

Figure 67: ISDN – Basic Rate Interface Web Page



2. In the *Interface Configuration* section of the *Basic Rate Interface* page, select to which interface you want to apply the changes in the *Select Interface* drop-down menu at the top of the window.

You can copy the configuration of the selected interface to one or more interfaces of the Mediatrix unit in the *Apply to the Following Interfaces* section at the bottom of the page. You can select specific interfaces by checking them, as well as use the *Check All* or *Uncheck All* buttons.

The Mediatrix 3404 model has 5 interfaces in Slot 1, while the Mediatrix 3408 model has 10 interfaces in Slots 1 and 2 (5 in each).

3. Select the endpoint type in the *Endpoint Type* drop-down menu.

Table 128: Endpoint Type

Type	Description
TE	Terminal Equipment. The endpoint emulates the subscriber (terminal) side of the digital connection. You can connect the SCN to the endpoint.
NT	Network Termination. The endpoint emulates the central office (network) side of the digital connection. You can connect a PBX or ISDN telephones to the endpoint.

The setting used for the Mediatix unit must be opposite to the setting used in the PBX. For instance, if the PBX is set to *TE*, then the Mediatix unit must be set to *NT*.



Note: If you want to use a specific interface as the reference clock, you must set it to **TE**.

When the BRI interface *Signalling Protocol* drop-down is set to **QSIG** (see Step 7), the endpoint type is only used in the second layer (LAPD) since it is a concept that does not exist in QSIG.

4. Select the clock mode of the interface in the *Clock Mode* drop-down menu.

The interface can either generate the clocking for the line or accept the clock from the line.

Table 129: Clock Mode

Mode	Description
auto	The setting is derived from the endpoint type. <ul style="list-style-type: none"> • NT: clock master • TE: clock slave
Master	The interface generates the clock.
Slave	The interface accepts the clock from the line.

The clock mode is used to give the user the possibility to set an endpoint in TE mode and still generate the clock by specifying the clock mode to master. The clock source can then be selected from the *Clock Reference* drop-down menu (see “[Chapter 5 - Hardware Parameters](#)” on page 29 for more details). The clock mode could be used, for instance, to synchronize several units in NT mode via a BRI line.



Note: In a BRI configuration, setting the clock mode to master for a TE endpoint is invalid. Slave mode is automatically applied in this case.

5. Set the *Monitor Link State* drop-down menu with the physical link state of the ISDN interface.

Table 130: Interface Link State

Parameter	Description
Enable	The ISDN endpoint's operational state is affected by its interface physical link state. When the link state of the ISDN interface is down, the operational state of its matching endpoint becomes “disable”.
Disable	The ISDN endpoint's operational state is not affected by its interface physical link state.

Note that if the *Monitor Link State* parameter is enabled and the *Ignore SIP OPTIONS on no usable endpoints* parameter is also enabled in the *SIP / Interop* page, this will influence how the SIP options are answered. See “[SIP Interop](#)” on page 279 for more details.

6. Select the connection type of the endpoint in the *Connection Type* drop-down menu.

The type of connection depends on the equipment to which the Mediatix unit port is connected and it must be the same for all interconnected pieces of equipment.

Table 131: Connection Type

Type	Description
Point to Point	Can only attach one device (for instance a PBX or SCN) and acts as a T reference point.
Point to MultiPoint	Can attach more than one ISDN device and acts as a S reference point. Up to 8 TEs and one NT can be connected to a S-bus.



Note: If you are using a Mediatix unit connected to a S-Bus in point-to-multipoint TE mode, you cannot currently connect any additional ISDN devices to the S-Bus.

The Point to MultiPoint configuration is not available in QSIG.

7. Select the protocol to use for the signalling channel in the *Signalling Protocol* drop-down menu. This signalling must match the connected ISDN equipment or network.

Table 132: Signalling Protocols

Protocol	Description
DSS1	Digital Subscriber Signaling System No.1
DMS100	Digital Multiplex System 100
NI2	National ISDN No.2
5ESS	5 Electronic Switching System
QSIG	ECMA's protocol for Private Integrated Services Networks



Note: The Dgw v2.0 Application currently supports only the DSS1 and QSIG signalling protocols.

8. Select the value of the network location in the progress indicator messages that the unit sends in the *Network Location* drop-down menu.
This defines the location code to be inserted in ISDN causes code information elements, i.e., the type of network to which the system belongs. The following values are available:
 - User
 - Private
 - Public
 - Transit
 - International
9. Set the *Preferred Encoding Scheme* drop-down menu with the data encoding scheme in the bearer capabilities (user information layer 1 protocol).
This encoding scheme is used when initiating a call on the ISDN side. The supported encoding schemes are *G.711 u-Law* and *G.711 a-Law*.
G.711 u-Law may not be supported by DSS1 NT and TE endpoints. It is recommended to use *G.711 a-Law* as preferred encoding protocol.
10. Set the *Fallback Encoding Scheme* drop-down menu with the fallback data encoding scheme in case the preferred encoding scheme is not available.

The supported encoding schemes are *G.711 u-Law* and *G.711 a-Law*.



Note: The fallback encoding scheme is valid only when receiving a SETUP message. The user sending the SETUP message does not indicate alternative bearer capability.

If the proposed encoding scheme in the bearer capability received in the SETUP message is different than the preferred encoding scheme, then the fallback encoding scheme is used.

11. Select the strategy for selecting bearer channels in the *Channel Allocation Strategy* drop-down menu.

Table 133: Channel Allocation Strategy

Allocation	Description
Ascending	Starting from the lowest-numbered non-busy bearer channel and going toward the highest-numbered non-busy bearer channel, the Mediatrix unit selects the first bearer channel available.
Descending	Starting from the highest-numbered non-busy bearer channel and going toward the lowest-numbered non-busy bearer channel, the Mediatrix unit selects the first bearer channel available.
RoundRobinAscending	The Mediatrix unit starts from the bearer channel that follows the bearer channel used for the last call. For instance, if channel #1 was used in the last call, the unit starts with channel #2. Going toward the highest-numbered non-busy bearer channel, the unit selects the first channel available. If the highest channel is unavailable, the search continues from the lowest-numbered non-busy bearer channel.
RoundRobinDescending	The Mediatrix unit starts from the bearer channel that precedes the bearer channel used for the last call. For instance, if channel #3 was used in the last call, the unit starts with channel #2. Going toward the lowest-numbered non-busy bearer channel, the unit selects the first channel available. If the lowest channel is unavailable, the search continues from the highest-numbered non-busy bearer channel.

12. Define the maximum number of active calls on the interface in the *Maximum Active Calls* field.
 This limits the total number of concurrent calls on the interface. Entering **0** indicates no maximum number of active calls.
 For a Mediatrix 3404 / 3408, the maximum number of simultaneous calls is limited to 8, even if 5 BRI ports can physically support 10 calls.
13. Select whether or not the signal information element is enabled in the *Signal Information Element* drop-down menu.
 - When activated at the Network UNI-side (*Endpoint Type* drop-down menu set to **NT**), the signal information element is sent to the User UNI-side.
 - When activated at the User UNI-side (*Endpoint Type* drop-down menu set to **TE**), the tone indicated in the signal information element is played in the IP direction.
14. Select whether or not inband tone generation is enabled in the *Inband Tone Generation* drop-down menu.
 When activated at the User UNI-side (*Endpoint Type* drop-down menu is set to **TE**), only the ringback tone is generated.
 When the BRI interface *Signalling Protocol* drop-down is set to **QSIG** (see Step 7) and this parameter is activated, the incoming side of the call plays the tones inband.
15. Select whether or not inband DTMF dialing is enabled in the *Inband DTMF Dialing* drop-down menu.
 If you select **Enable**, the Mediatrix unit accepts inband DTMF digits when Overlap Dialing occurs.

16. Select whether or not overlap dialing is enabled in the *Overlap Dialing* drop-down menu.

Table 134: Overlap Dialing Parameters

Parameter	Description
Enable	The Mediatix unit transports the called-party number digit by digit, after the first SETUP message, which contains no called party information at all.
Disable	The Mediatix unit transports the full called party information in the first SETUP message from the terminal. This means that the user must dial the number before going off-hook.

17. Define the maximum length of the calling party name for calls from SIP to ISDN in the *Calling Name Max Length* field.

Available values range from 0 to 82.

18. Select whether or not exclusive B-Channel selection is enabled for calls from SIP to ISDN in the *Exclusive B-Channel Selection* drop-down menu.

If you select **Enable** and initiate a call, only the requested B channel is accepted; if the requested B channel is not available, the call is cleared.

19. Select whether or not to enable the Sending Complete information element into SETUP messages for calls from SIP to ISDN in the *Sending Complete* drop-down menu.

Some ISDN switches may require that the Sending Complete information element be included in the outgoing SETUP message to indicate that the entire number is included and there are no further destination digits to be sent.

20. Select whether or not to enable sending the RESTART message upon a signalling channel "UP" event in the *Send Restart On Startup* drop-down menu.

The RESTART message requests a restart for the interface specified.

21. Set the link establishment strategy in the *Link Establishment* drop-down menu.

Table 135: Link Establishment Parameters

Parameter	Description
OnDemand	When the data link is shut down, the unit establishes a new link only when required.
Permanent	When the data link is shut down, the unit immediately attempts to establish a new link.

22. Set the actual keypad string that is to be considered as a hook-flash in the *Hook-Flash Keypad* field.

An ISDN telephone may send INFORMATION messages that contain a "Keypad Facility". You can thus trigger a supplementary service (Hold, Conference, etc.) by sending a keypad facility.

Since the keypads can be received via several INFORMATION messages, they are accumulated until they match or reset if the keypad reception timeout (second) has elapsed since the last keypad has been received. The keypad reception timeout can only be modified via SNMP. If the keypad reception timeout is set to 0, it disables the timeout, thus assuming that all keypads will be received in a single INFORMATION message.

Setting this variable to an empty string disables the hook-flash detection.

The permitted keypad must be made up of IA5 characters. See ITU-T Recommendation T.50.

23. Set the STATUS causes that can be received without automatically clearing the call in the *Accepted Status Causes* field.

The default action is to clear the call upon receiving a STATUS message. If a STATUS message is received indicating a compatible call state and containing the supplied STATUS causes, the clearing of the call is prevented.

The string has the following syntax:

- ',': Separator between non-consecutive lists of causes or single cause.
- 'n': A single cause, where n is the cause number.

'm-n': List of causes where m is the start cause number and n is the end cause number.



Note: The space character is ignored and cause duplication is not allowed.

Causes must be specified in low to high order.

Example: '1,124-127': The accepted causes are 1, 124, 125, 126 and 127.

24. Set the range of PROGRESS causes accepted by the unit in the *Accepted Progress Causes* field.

Causes excluded from this range trigger call disconnections.

The string has the following syntax:

- ',': Separator between non-consecutive lists of causes or single cause.
- 'n': A single cause, where n is the cause number.
- 'm-n': List of causes where m is the start cause number and n is the end cause number.



Note: You must consider the following:

- The space character is not allowed.
- Causes must be specified in low to high order.
- Cause duplication is not allowed.

Example: '1,124-127': The accepted causes are 1, 124, 125, 126 and 127.

25. Select the strategy for sending ISDN Progress messages in the *Send Isdn Progress* drop-down menu.

Table 136: Send ISDN Progress Parameters

Parameter	Description
Send All	Send an ISDN Progress message in all situations where call progression is signaled.
Send Inband	Send an ISDN Progress message only when call progression contains an indication of in-band information.
Send Alerting	Send an ISDN Alerting message instead of ISDN Progress message when call progression contains an indication of in-band information. If call progression does not contain in-band information, no message is sent at this step.

The strategy for sending Progress messages should be adapted to the configuration of the peer ISDN switch. Some switches may terminate calls when receiving one or many ISDN progress messages.

26. Select the strategy for sending the Progress Indicator Information Element in the *Send Progress Indicator IE* drop-down menu.

Table 137: Send Progress Indicator IE Parameters

Parameter	Description
Send All	Send the Progress Indicator IE in all situations.
Send Inband Only	Send the Progress Indicator only when the Progress Description contains an indication of in-band information.

The strategy for the Progress Indicator IE should be adapted to the configuration of the peer ISDN switch.

This parameter controls sending of a Progress Indicator IE in ISDN messages where Progress Indicators are allowed. See the parameters in [“Interop Parameters Configuration” on page 178](#) for a control over which ISDN message allows Progress Indicators.

27. Set the *TEI Negotiation* drop-down menu with the proper Terminal Endpoint Identifier (TEI) negotiation strategy.

Table 138: TEI Negotiation Parameters

Parameter	Description
Link Up	Each time the physical link comes up, the unit renegotiates the TEI value.
Power Up	When the physical link comes up, the unit does not renegotiate the TEI value. The value obtained at power-up is reused.
Signaling up	Each time the signaling link comes up, the unit renegotiates the TEI value.



Note: This parameter only applies on Point To Multipoint connections.

28. Select the default value to insert in the "Type of Number" parameter of the "Calling Party Number" IE when "Type of Number" is not already defined in the call properties in the *Default TON for Calling Party Number IE* drop-down menu.



Note: A call property set by the "Properties Manipulation" feature of the Call Router has precedence over this default value. See [“Chapter 44 - Call Router Configuration” on page 431](#) for more details.

This parameter applies to the outgoing ISDN calls. Possible values are:

Table 139: Default TON for Calling Party Number IE Parameters

Parameter	Description
Unknown	Default value of Type of Number is set to Unknown.
International	Default value of Type of Number is set to International.
National	Default value of Type of Number is set to National.
Network Specific	Default value of Type of Number is set to Network-Specific.
Subscriber	Default value of Type of Number is set to Subscriber.
Abbreviated	Default value of Type of Number is set to Abbreviated.

29. Select the default value to insert in the "Numbering Plan Identification" parameter of the "Calling Party Number" IE when "Numbering Plan Identification" is not already defined in the call properties in the *Default NPI for Calling Party Number IE* drop-down menu.



Note: A call property set by the "Properties Manipulation" feature of the Call Router has precedence over this default value. See [“Chapter 44 - Call Router Configuration” on page 431](#) for more details.

This parameter applies to the outgoing ISDN calls. Possible values are:

Table 140: Default NPI for Calling Party Number IE Parameters

Parameter	Description
Unknown	Default value of Numbering Plan Identification is set to Unknown.
ISDN Telephony	Default value of Numbering Plan Identification is set to ISDN Telephony.

Table 140: Default NPI for Calling Party Number IE Parameters (Continued)

Parameter	Description
Data	Default value of Numbering Plan Identification is set to Data.
Telex	Default value of Numbering Plan Identification is set to Telex.
National Standard	Default value of Numbering Plan Identification is set to National Standard.
Private	Default value of Numbering Plan Identification is set to Private.

30. Select the default value to insert in the "Presentation Indicator" parameter of the "Calling Party Number" IE when "Presentation Indicator" is not already defined in the call properties in the *Default PI for Calling Party Number IE* drop-down menu.



Note: A call property set by the "Properties Manipulation" feature of the Call Router has precedence over this default value. See ["Chapter 44 - Call Router Configuration" on page 431](#) for more details.

If "Presentation Indicator" is not provided by the call properties, its value is determined by the following two steps.

- a. First, it is set to the default value defined by "DefaultCallingPi".
- b. Second, the "Presentation Indicator" can be overridden by the CLIP and CLIR services: the value can be set to "Restricted" by the CLIR service and the value can be set to "NotAvailable" if there is no number to forward. This variable applies to the outgoing ISDN calls.

Possible values are:

Table 141: Default PI for Calling Party Number IE Parameters

Parameter	Description
Presentation Allowed	Default value of Presentation Indicator is set to Presentation Allowed.
Presentation Restricted	Default value of Presentation Indicator is set to Presentation Restricted.
Not Available	Default value of Presentation Indicator is set to Not Available.

31. Select the default value to insert in the "Screening Indicator" parameter of the "Calling Party Number" IE when "Screening Indicator" is not already defined in the call properties in the *Default SI for Calling Party Number IE* drop-down menu.



Note: A call property set by the "Properties Manipulation" feature of the Call Router has precedence over this default value. See ["Chapter 44 - Call Router Configuration" on page 431](#) for more details.

This parameter applies to the outgoing ISDN calls. Possible values are:

Table 142: Default SI for Calling Party Number IE Parameters

Parameter	Description
User Provided Not Screened	Default value of Screening Indicator is set to User Provided Not Screened.
User Provided Verified And Passed	Default value of Screening Indicator is set to User Provided Verified And Passed.
User Provided Verified And Failed	Default value of Screening Indicator is set to User Provided Verified And Failed.
Network Provided	Default value of Screening Indicator is set to Network Provided.

Table 142: Default SI for Calling Party Number IE Parameters (Continued)

Parameter	Description
Context Dependent	Screening Indicator is set to the value that makes the most sense according to run-time context.

32. Select the default value to insert in the "Type of Number" parameter of the "Called Party Number" IE when "Type of Number" is not already defined in the call properties in the *Default TON for Called Party Number IE* drop-down menu.



Note: A call property set by the "Properties Manipulation" feature of the Call Router has precedence over this default value. See "[Chapter 44 - Call Router Configuration](#)" on page 431 for more details.

This parameter applies to the outgoing ISDN calls. Possible values are:

Table 143: Default TON for Called Party Number IE Parameters

Parameter	Description
Unknown	Default value of Type of Number is set to Unknown.
International	Default value of Type of Number is set to International.
National	Default value of Type of Number is set to National.
Network Specific	Default value of Type of Number is set to Network-Specific.
Subscriber	Default value of Type of Number is set to Subscriber.
Abbreviated	Default value of Type of Number is set to Abbreviated.

33. Select the default value to insert in the "Numbering Plan Identification" parameter of the "Called Party Number" IE when "Numbering Plan Identification" is not already defined in the call properties in the *Default NPI for Called Party Number IE* drop-down menu.



Note: A call property set by the "Properties Manipulation" feature of the Call Router has precedence over this default value. See "[Chapter 44 - Call Router Configuration](#)" on page 431 for more details.

This parameter applies to the outgoing ISDN calls. Possible values are:

Table 144: Default NPI for Called Party Number IE Parameters

Parameter	Description
Unknown	Default value of Numbering Plan Identification is set to Unknown.
ISDN Telephony	Default value of Numbering Plan Identification is set to ISDN Telephony.
Data	Default value of Numbering Plan Identification is set to Data.
Telex	Default value of Numbering Plan Identification is set to Telex.
National Standard	Default value of Numbering Plan Identification is set to National Standard.
Private	Default value of Numbering Plan Identification is set to Private.

34. Select the unit's behaviour when it receives a Notification Indicator IE with the description set to User suspended in the *Notification User Suspended* drop-down menu.

Possible values are:

Table 145: Notification User Suspended Parameters

Parameter	Description
Ignore	The Mediatrix unit ignores the Notification Indicator IE with description set to User suspended.
Disconnect	The Mediatrix unit disconnects the call on Notification Indicator IE with description set to User suspended.

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

Bypass Feature (Mediatrix 3404/3408/3734/3741/3742 Models)

In the event of a power or network failure, the bypass feature permits users to make and receive calls even when the Mediatrix unit is not operating. The Mediatrix unit **BRI 3** and **BRI 4** ports may either act as a SCN bypass. For instance, if you decide to connect a SCN line into the *BRI 4* port, you can use a BRI telephone connected into the *BRI 3* port to make calls.

Furthermore:

- ▶ The port on which the SCN line is connected must be configured as a TE.
- ▶ The other port must be configured as a NT.

Refer to [“BRI Configuration” on page 167](#) for more details on how to configure the line type.

During normal operation, the direct connection between the *BRI 3* and *BRI 4* ports is switched out through commuting relays and both ports resume normal functions. When power is removed from the Mediatrix unit, the relay setting is restored to a connected state and the SCN line can be used as an emergency line.

Consequently, a BRI telephone used on the other port is directly connected to this SCN line. When the power is restored, this automatically removes the Bypass connection; this means that any ongoing call on the Bypass connection is terminated.



Note: If you are using a crossover Ethernet cable to connect the SCN line to the Mediatrix unit and there is a power failure, the bypass feature does not work properly.

Bypass Feature (Mediatrix 4402plus / 4404plus Models)

In the event of a power or network failure, the optional bypass feature permits users to make and receive calls even when the Mediatrix unit is not operating. The Mediatrix unit **BRI 1** and **BRI 2** ports may either act as a SCN bypass. For instance, if you decide to connect a SCN line into the *BRI 2* port, you can use a BRI telephone connected into the *BRI 1* port to make calls.

Furthermore:

- ▶ The port on which the SCN line is connected must be configured as a TE.
- ▶ The other port must be configured as a NT.

Refer to [“BRI Configuration” on page 167](#) for more details on how to configure the line type.

During normal operation, the direct connection between the *BRI 1* and *BRI 2* ports is switched out through commuting relays and both ports resume normal functions. When power is removed from the Mediatrix unit, the relay setting is restored to a connected state and the SCN line can be used as an emergency line.

Consequently, a BRI telephone used on the other port is directly connected to this SCN line. When the power is restored, this automatically removes the Bypass connection; this means that any ongoing call on the Bypass connection is terminated.

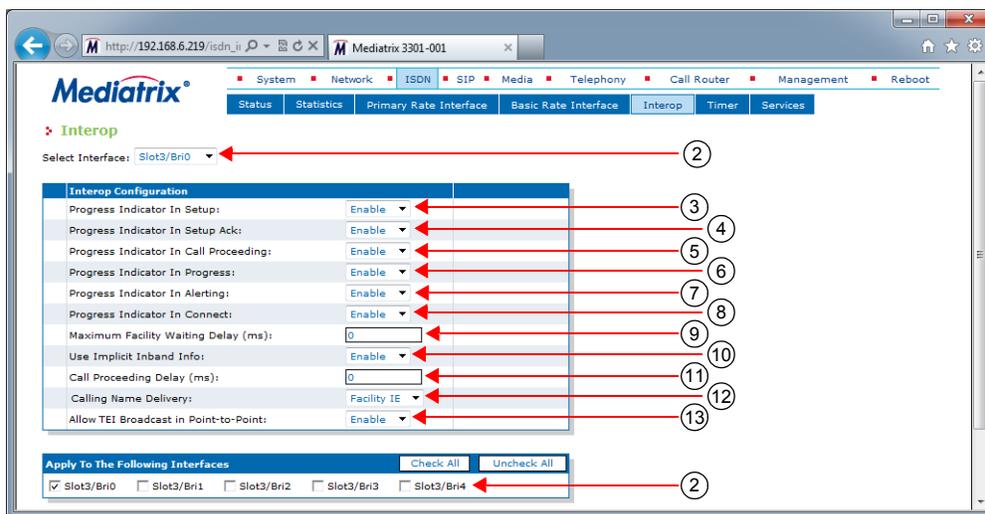
Interop Parameters Configuration

The interop parameters allow the Mediatrix unit to properly work, communicate, or connect with specific ISDN devices.

► **To set the interop parameters:**

1. In the web interface, click the *ISDN* link, then the *Interop* sub-link.

Figure 68: ISDN – Interop Web Page



2. Select to which interface you want to apply the changes in the *Select Interface* drop-down menu at the top of the window.

You can copy the configuration of the selected interface to one or more interfaces of the Mediatrix unit in the *Apply to the Following Interfaces* section at the bottom of the page. You can select specific interfaces by checking them, as well as use the *Check All* or *Uncheck All* buttons.

The Mediatrix 3404 model has 5 interfaces in Slot 2, while the Mediatrix 3408 model has 10 interfaces in Slots 2 and 3 (5 in each).

The Mediatrix 3532 and 3632 models have two interfaces.

The Mediatrix 3734/3741/3742 models have 5 interfaces.

The number of interfaces available vary depending on the Mediatrix 4400 model you have.

3. Define the behaviour of the *Progress Indicator In Setup* drop-down menu.

This menu defines whether or not the Progress Indicator Information Element (IE) is allowed in the SETUP message when acting as the originating side.

See the *Send Progress Indicator IE* parameter for other conditions for sending Progress Indicator IE ([“PRI Configuration” on page 155](#) and [“BRI Configuration” on page 167](#)).

4. Define the behaviour of the *Progress Indicator In Setup Ack* drop-down menu.

This menu defines whether or not the Progress Indicator Information Element (IE) is allowed in the SETUP ACK when acting as the terminating side.

See the *Send Progress Indicator IE* parameter for other conditions for sending Progress Indicator IE ([“PRI Configuration” on page 155](#) and [“BRI Configuration” on page 167](#)).

5. Define the behaviour of the *Progress Indicator In Call Proceeding* drop-down menu.

This menu defines whether or not the Progress Indicator Information Element (IE) is allowed in the CALL PROCEEDING message in response to a SETUP message when acting as the terminating side.

See the *Send Progress Indicator IE* parameter for other conditions for sending Progress Indicator IE (“[PRI Configuration](#)” on page 155 and “[BRI Configuration](#)” on page 167).

6. Define the behaviour of the *Progress Indicator In Progress* drop-down menu.
This menu defines whether or not the Progress Indicator Information Element (IE) is allowed in the PROGRESS message in response to a SETUP message when acting as the terminating side.
See the *Send Progress Indicator IE* parameter for other conditions for sending Progress Indicator IE (“[PRI Configuration](#)” on page 155 and “[BRI Configuration](#)” on page 167).
7. Define the behaviour of the *Progress Indicator In Alerting* drop-down menu.
This menu defines whether or not the Progress Indicator Information Element (IE) is allowed in the ALERTING message.
See the *Send Progress Indicator IE* parameter for other conditions for sending Progress Indicator IE (“[PRI Configuration](#)” on page 155 and “[BRI Configuration](#)” on page 167).
8. Define the behaviour of the *Progress Indicator In Connect* drop-down menu.
This menu defines whether or not the Progress Indicator Information Element (IE) is allowed in the CONNECT message.
See the *Send Progress Indicator IE* parameter for other conditions for sending Progress Indicator IE (“[PRI Configuration](#)” on page 155 and “[BRI Configuration](#)” on page 167).
9. Define a value, in milliseconds (ms), in the *Maximum Facility Waiting Delay (ms)* field.
This value defines the maximum amount of time to wait for a FACILITY message, after receiving a SETUP message, before going on with normal call processing.
After receiving a SETUP message, the system waits for this amount of time for a FACILITY message. As soon as it receives a FACILITY message or the delay expires, it goes on with normal call processing.
A FACILITY message can contain useful information for the call. For example, it can contain a Calling Name.
You must enable the Supplementary Services to use the delay. See “[PRI Configuration](#)” on page 155 or “[BRI Configuration](#)” on page 167 for more details.
Setting the value to 0 deactivates this waiting delay.
10. Define whether or not a message with progress indicator No. 1 MUST be considered as offering inband information available in the *Use Implicit Inband Info* drop-down menu.
If so, the network must activate the B-channel connection.
The progress indicator No. 1 means that the call is not end-to-end ISDN; further call progress information may be available inband.
11. Defines the maximum time, in milliseconds, to wait after receiving a SETUP message before sending a CALL PROCEEDING message and going on with normal call processing in the *Call Proceeding Delay* field.
After receiving a SETUP message, the system waits for a message from the called party. If the message maps to a User Busy cause, a DISCONNECT message is sent instead of the CALL PROCEEDING otherwise it goes on with normal call processing.
The value 0 deactivates this feature.
12. Define how the Calling Name is delivered in the *Calling Name Delivery* field.
The Calling Party Name can be received and sent through three different methods: Facility information element, Display information element or User-User information element.

Table 146: Calling Name Delivery Parameters

Parameter	Description
Displayle	Use a Display Information Element for delivering the Calling Name.
Facilityle	Use a Facility Information Element for delivering the Calling Name.

Table 146: Calling Name Delivery Parameters (Continued)

Parameter	Description
UserUserIe	Use a User-User Information Element for delivering the Calling Name.
SignalingProtocol	Use the delivery method defined by the signaling protocol.

When receiving an incoming call, the three possible sources of Calling Party Name are checked in the following order: User-User, Display and Facility. The last found is used.

The Calling Party Name is accepted in a Display information element only when explicitly identified as a Calling Party Name (i.e. only when "Display Type" = "Calling Party Name" in the information element).

When initiating a call, the Calling Party Name is sent according to the method selected above. If the method selected is not supported for the protocol in use, the default method for this protocol is used. The following table shows which method is used vs. the configuration of CallingNameDelivery:

Table 147: Calling Name Delivery Method vs. Configuration

Protocol	Calling Name Delivery			
	eFacility	eDisplay	eUserUser	eSignalingProtocol
DSS1	IE User-User	IE User-User	IE User-User	IE User-User
Dms100	IE Facility	IE Display	IE Display	IE Display
NI-2	IE Facility	IE Facility	IE Facility	IE Facility
5ESS	IE Facility	IE Facility	IE User-User	IE Facility
QSIG	IE Facility	IE Facility	IE Facility	IE Facility

See [“PRI Configuration” on page 155](#) and [“BRI Configuration” on page 167](#) for more details on signaling protocols.

13. Define whether or not an ISDN message with a TEI broadcast needs to be interpreted as a TEI 0 when the connection type is 'PointToPoint' in the *Allow TEI Broadcast in PTP* drop-down menu.

See [“BRI Configuration” on page 167](#) for more details on the connection type.

This parameter is available for the following BRI models:

- Mediatrix 3404
- Mediatrix 3408
- Mediatrix 3734
- Mediatrix 3741
- Mediatrix 3742
- Mediatrix 4400 Series

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

Play Local Ringback when no Media Stream

This section describes configuration that is available only in the MIB parameters of the Mediatrix 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 force the local ringback generation when early-media is enabled but no media stream has been received yet. This variable only affects incoming calls on the ISDN interface.

Note that this variable only applies to 180 SIP responses when early-media is enabled.
The following configurations are supported:

Table 148: Play Local Ringback Configuration

Configuration	Description
disable	Do not play local ringback when doing early-media.
enable	The local ringback is played after sending an ALERTING and no media stream has been received yet from the outgoing interface.

► **To set how to play the local ringback when there is no media stream:**

1. In the *isdnMIB*, set the Play Local Ringback configuration in the `InteropPlayLocalRingbackWhenNoMediaStream` variable.
You can also use the following line in the CLI or a configuration script:
`isdn.InteropPlayLocalRingbackWhenNoMediaStream="value"`
where *Value* may be as follows:

Table 149: Play Local Ringback Values

Value	Meaning
0	disable
1	enable

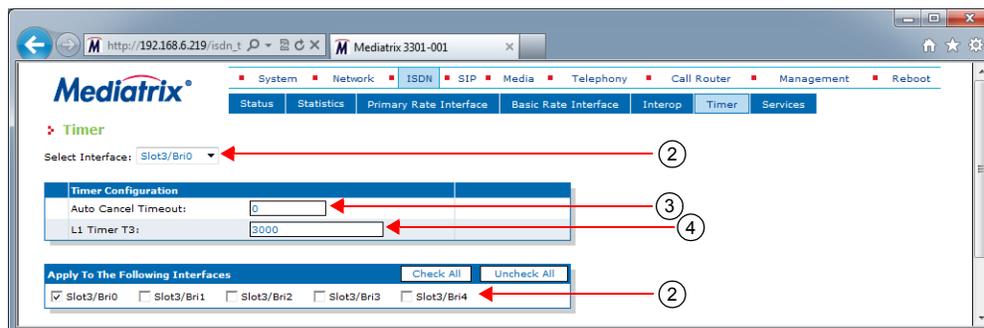
ISDN Timers Configuration

This section allows you to set timer parameters.

► **To set the ISDN timers:**

1. In the web interface, click the *ISDN* link, then the *Timer* sub-link.

Figure 69: ISDN – Timer Web Page



2. Select to which interface you want to apply the changes in the *Select Interface* drop-down menu at the top of the window.

You can copy the configuration of the selected interface to one or more interfaces of the Mediatrix unit in the *Apply to the Following Interfaces* section at the bottom of the page. You can select specific interfaces by checking them, as well as use the *Check All* or *Uncheck All* buttons.

The Mediatrix 3404 model has 5 interfaces in Slot 2, while the Mediatrix 3408 model has 10 interfaces in Slots 2 and 3 (5 in each).

The Mediatrix 3532 and 3632 models have two interfaces.

The Mediatrix 3734/3741/3742 models have 5 interfaces.

The number of interfaces available vary depending on the Mediatrix 4400 model you have.

3. 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.
4. Set the value, in milliseconds (ms), of the Layer 1 Timer T3 in the *L1 Timer T3* field.

Timer 3 (T3) is a supervisory timer that has to take into account the overall time to activate. This time includes the time it takes to activate both the TE-NT and the NT-TE portion of the customer access.

The expiry of Timer T3 is intended to provide an indication that the network side cannot complete the activation procedure, probably due to a failure condition or the terminal cannot detect INFO 4.
5. Click *Submit* if you do not need to set other parameters.

Services Configuration

This section allows you to set the ISDN optional services.

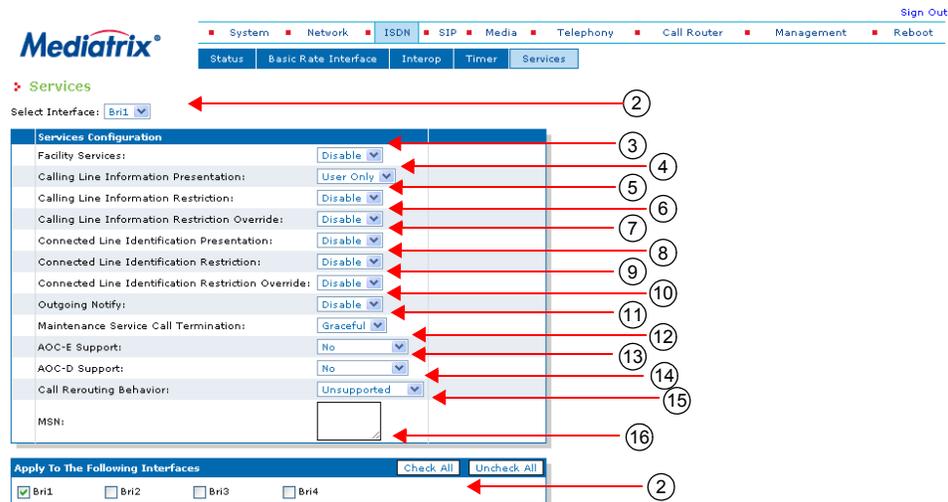
Standards Supported

- ETS 300 207: Call Diversion and Call Rerouting

► **To set the ISDN optional services:**

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

Figure 70: ISDN – Services Web Page



2. Select to which interface you want to apply the changes in the *Select Interface* drop-down menu at the top of the window.

You can copy the configuration of the selected interface to one or more interfaces of the Mediatrix unit in the *Apply to the Following Interfaces* section at the bottom of the page. You can select specific interfaces by checking them, as well as use the *Check All* or *Uncheck All* buttons.

The Mediatrix 3404 model has 5 interfaces in Slot 2, while the Mediatrix 3408 model has 10 interfaces in Slots 2 and 3 (5 in each).

The Mediatrix 3532 and 3632 models have two interfaces.

The Mediatrix 3734/3741/3742 models have 5 interfaces.

The number of interfaces available vary depending on the Mediatrix 4400 model you have.

3. Select whether or not supplementary services FACILITY messages and FACILITY information elements should be enabled on the ISDN interface in the *Facility Services* drop-down menu.

This controls how to use the FACILITY information element.

Table 150: Facility Services

Parameter	Description
Disable	Facility information elements are disabled in both directions (send and receive). No Facility information element can be inserted in sent messages. When receiving a FACILITY message containing supplementary services information, the Mediatrix unit replies with a STATUS message saying the FACILITY is not supported.

Table 150: Facility Services (Continued)

Parameter	Description
Enable	Facility information elements are enabled in both directions (send and receive). Facility information elements can be inserted in sent messages. When receiving a FACILITY message containing supplementary services information, the Mediatix unit accepts and interprets the message, processing supported supplementary service messages and silently discarding unsupported supplementary service messages.

Generic procedures for the control of ISDN supplementary services are defined in the recommendation ITU-T Q.932.

You can define a waiting delay as described in the section [“Interop Parameters Configuration” on page 178](#).



Note: To activate the ISDN hold feature, you must also set the *Default Hook Flash Processing* feature to **Use Signaling Protocol** in [“General Configuration” on page 385](#).

4. Select whether or not to enable the CLIP service in the *Calling Line Information Presentation* drop-down menu.

The Calling Line Information Presentation (CLIP) is an optional service that can be offered by the ISDN provider. CLIP is offered to the called party to see the calling party's ISDN number. CLIP is complemented by privacy rules controlled by the *Calling Line Information Restriction* and *Calling Line Information Restriction Override* parameters.

The *Calling Line Information Presentation* parameter has the following effect:

Parameter	Description
UserOnly	Sends a Calling Number IE that contains the calling number digits when acting as the User UNI-side (<i>Endpoint Type</i> drop-down menu set to TE) otherwise the Calling Number IE is not sent.
Enable	Sends a Calling Number IE that contains the calling number digits.
Disable	The Calling Number IE is never sent.

5. Select whether or not to enable the CLIR service in the *Calling Line Information Restriction* drop-down menu.

The Calling Line Information Restriction (CLIR) service is offered to the calling party to restrict presentation of the calling party's ISDN number to the called party.

Setting this parameter to **Disable** disables the CLIR service.

Setting this parameter to **Enable** enables the CLIR service. This has the following effects:

For all ISDN signaling protocols except QSIG:

- On a TE interface (*Endpoint Type* drop-down menu set to **TE**) at the originating network side, when sending a SETUP message with a Calling Party Number (CPN) IE, the Presentation Indicator (PI) is set to "Restricted". The calling party number itself is included in the CPN IE if available.
- On a NT interface (*Endpoint Type* drop-down menu set to **NT**) at the originating network side, when receiving a SETUP message with a CPN IE, the PI is set to "Restricted". The calling party number itself is forwarded.

For the QSIG signaling protocol (PRI/BRI interface *Signalling Protocol* drop-down is set to **QSIG**):

- Sending a SETUP message: The PI is set to "Restricted" in the CPN IE inserted in the SETUP message sent to the ISDN, unless the CLIR override option is set. However, even if PI is set to "Restricted", the calling number is included in the CPN IE.

- Receiving a SETUP message: If PI is set in the received message, the calling party number is removed, unless the CLIR override option is set.

See “PRI Configuration” on page 155 or “BRI Configuration” on page 167 for more details.

See “PRI Configuration” on page 155 or “BRI Configuration” on page 167 for more details.

- Select whether or not to enable the CLIR override option in the *Calling Line Information Restriction Override* drop-down menu.

This option allows the calling party number to be presented to the destination party even when the Calling Party Number (CPN) IE's Presentation Indicator (PI) is set to "Restricted". This option is typically used for police or emergency services.

Setting this variable to **Disable** disables the CLIR Override option.

Setting this variable to **Enable** enables the CLIR Override option. This has the following effects:

For all ISDN signaling protocols except QSIG:

- The override option acts on the NT interface of the destination network side. It prevents the number to be removed from the CPN IE inserted in the SETUP message sent to the destination TE.

For the QSIG signaling protocol (PRI/BRI interface *Signalling Protocol* drop-down is set to **QSIG**):

- The override option prevents the calling name to be removed from the CPN IE in a received SETUP message.

See “PRI Configuration” on page 155 or “BRI Configuration” on page 167 for more details.

- Select whether or not to send a Connected Number IE within the CONNECT message at the originating ISDN side in the *Connected Line Identification Presentation* drop-down menu.

The Connected Line Identification Presentation (COLP) is an optional service offered at the originating interface by the NT to the TE.

Table 151: COLP Parameters

Parameter	Description
Enable	Sends a Connected Number IE within the CONNECT message, which contains the connected number digits once the transformation of the routing table has been applied.
Disable	The Connected Number IE is never sent.

- Select whether or not to set the Connected Number Information Element restriction at the destination ISDN side in the *Connected Line Identification Restriction* drop-down menu.

The Connected Line Identification Restriction (COLR) is a service offered to the TE at the destination interface.

Table 152: COLR Parameters

Parameter	Description
Enable	When activated at the User UNI-side (<i>Endpoint Type</i> drop-down menu set to TE), marks the Connected Number IE with a 'restricted' Presentation Indicator, which keeps privacy over the connected number digits. This option has no effect when activated at the Network UNI-side (<i>Endpoint Type</i> drop-down menu set to NT).
Disable	No restriction is applied.

9. Select whether or not to set the Connected Number Information Element restriction override at the originating ISDN side in the *Connected Line Identification Restriction Override* drop-down menu.

Table 153: COLR Override Parameters

Parameter	Description
Enable	When activated at the Network UNI-side (<i>Endpoint Type</i> drop-down menu set to NT), the connected number digits are delivered even if the Presentation Indicator is set to 'restricted'. This option has no effect when activated at the User UNI-side (<i>Endpoint Type</i> drop-down menu set to TE). This is a national option designed for emergency services.
Disable	No restriction override is applied.

10. Define whether or not NOTIFY messages can be sent in the *Outgoing Notify* drop-down menu.

Table 154: Outgoing Notify Parameters

Parameter	Description
Enable	NOTIFY messages can be sent.
Disable	NOTIFY messages are never sent.

The following NOTIFY messages are supported:

- REMOTE HOLD: Sent when the remote peer holds the call.
- REMOTE RETRIEVAL: Sent when the remote peer retrieves the call.

11. Set the *Maintenance Service Call Termination* drop-down menu with the call termination strategy after reception of a service message requesting a maintenance on the associated bearer channel.

Table 155: Maintenance Service Parameters

Parameter	Description
Graceful	The call proceeds normally until the user clears the call. The associated bearer is then set to maintenance. This is the default value.
Abrupt	The call is terminated immediately and set to maintenance.

12. Define whether or not the optional *Date/Time Information* Element (IE) can be included in the CONNECT and SETUP messages in the BRI and PRI.

Table 156: Date/Time IE Support Parameters

Parameter	Description
Disable	Date/Time is not sent
Local Time	Date/Time IE is sent, containing the local time according to the configured time zone in the Network Host Time Configuration.
UTC	Date/Time IE is sent, containing the Coordinated Universal Time (UTC)



Note: Without a SNTP Synchronized connection, the Date/Time IE is not sent. See [“SNTP Configuration” on page 57](#) for more details on how to configure the SNTP.

13. Define the *AOC-E Support* drop-down menu how to send the total charge at the (E)nd of the call in AOC-E messages.

Table 157: AOC-E Support Parameters

Parameter	Description
no	The AOC-E support is disabled. No information is forwarded to the peer interface.
transparent	On an NT interface, the information is sent as received from the network. No information is sent if the network does not provide information. On a TE interface, the information is forwarded to the peer interface if AOC messages are received from the network.
automatic	On an NT interface, always send the information. If the network does not provide information, 'noChargeAvailable' is sent. On a TE interface, the information is forwarded to the peer interface if AOC messages are received from the network.
explicit	On an NT interface, always send the information if the phone requests AOC on a per-call basis. 'noChargeAvailable' is sent if the network does not provide information. If the phone does not request AOC on a per-call basis, no information is sent. On a TE interface, send an AOC request to the network. If the network rejects the request, no information is forwarded to the peer interface. Otherwise, the information is forwarded to the peer interface if AOC messages are received from the network.

14. Define the *AOC-D Support* drop-down menu how to send the current charge (D)uring the call in AOC-D messages.

Table 158: AOC-D Support Parameters

Parameter	Description
no	The AOC-D support is disabled. No information is forwarded to the peer interface.
transparent	On an NT interface, the information is sent as received from the network. No information is sent if the network does not provide information. On a TE interface, the information is forwarded to the peer interface if AOC messages are received from the network.
automatic	On an NT interface, always send the information. If the network does not provide information, 'noChargeAvailable' is sent. On a TE interface, the information is forwarded to the peer interface if AOC messages are received from the network.
explicit	On an NT interface, always send the information if the phone requests AOC on a per-call basis. 'noChargeAvailable' is sent if the network does not provide information. If the phone does not request AOC on a per-call basis, no information is sent. On a TE interface, send an AOC request to the network. If the network rejects the request, no information is forwarded to the peer interface. Otherwise, the information is forwarded to the peer interface if AOC messages are received from the network.



Note: The AOC features are not available in the NI2 and QSIG signalling protocols. See [“PRI Configuration” on page 155](#) for more details on how to configure the signalling protocol.



Note: To enable AOC support on the ISDN interface, you must enable the FACILITY services and at least one of the following AOC support: AOC-E (End of Call) or AOC-D (During the Call).

Since the AOC from ISDN interface to SIP is currently not supported, enabling the AOC on an ISDN interface configured as TE (user side) is only meaningful when using hairpinning.

15. Set the *Call Rerouting Behavior* drop-down menu with how the call rerouting request received from the private network side is supported.

The Call Rerouting supplementary service allows to reroute an incoming public ISDN call (originated from the PSTN) within or beyond the private ISDN network (such a PBX) as specified in the ETS 300 207 01, section 10.5. The Rerouting data are received and relayed through a Facility message containing a Facility Information Element.

Rerouting requests are received in a Facility IE.

Table 159: Forward Call Rerouting Parameters

Parameter	Description
Unsupported	Rerouting requests received are rejected. A reject answer is sent to the private network.
Relay Reroute	Rerouting requests are relayed as received to the public network side. If the peer rejects or does not support the reroute request, the ISDN service may initiate a new call to process the rerouting request locally.
Process Locally	Received Rerouting requests are not relayed to the public network side. The ISDN service attempts to connect to the rerouted address by initiating a new call.



Note: The Call Rerouting feature is not available in the NI2 and QSIG signalling protocols. See [“PRI Configuration” on page 155](#) for more details on how to configure the signalling protocol.

16. Enter one or more numbers in the *MSN* field.

You can enter a comma-separated list of numbers. The comma-separated list must use the following syntax:

777, 888, 999, 555, 444.

This enables the Multiple Subscriber Numbers (MSN) supplementary service with these numbers. A MSN is a telephone number associated with a line.

The MSN supplementary service enables each individual terminal on one access to have one or more identities.

If the Called E.164 received from a call does not match any MSN numbers, the call is silently discarded.

This supplementary service applies only on a BRI Interface configured in TE Point to Multi-Point. See [“BRI Configuration” on page 167](#) for more details.

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

R2 CAS Parameters

Page Left Intentionally Blank

CHAPTER

24

R2 CAS Configuration

This chapter describes how to configure the R2 CAS parameters of the Mediatrix unit.



Note: This chapter applies only to the Mediatrix 3621, Mediatrix 3631, and Mediatrix 3632 models.

Introduction

CAS stands for Channel Associated Signaling. With this method of signalling, each traffic channel has a dedicated signaling 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.

The Mediatrix unit uses the MFC/R2 CAS protocol. This is a compelled sequence multi-frequency code signaling. MFC/R2 can be used on international as well as national connections.

In MFC/R2 signaling, the equipment units at the exchanges that send and receive digits, and the signaling between these units, are usually referred to as register and interregister signalling.

The terms forwards and backwards are heavily used in descriptions of MFC/R2. Forwards is the direction from the calling party to the called party. Backwards is the direction from the called party to the calling party.

You can configure Mediatrix unit parameters for the E1 R2 CAS.

Line Signals for the Digital Version of MFC/R2

The MFC/R2 digital line signals (defined in ITU-T Q.421) are the ABCD bits of CAS in timeslot 16 of an E1. They represent the states of the line, and are similar to the states of an analog line. In general, only bits A and B are used. In most systems, bits C and D are set to fixed values and never change. There are some national variants where bit C or D may be used for metering pulses.

Interregister Signals

The interregister, or interswitch, signals in MFC/R2 signaling (defined in ITU-T Q.441) are encoded as the presence of 2, and only 2, out of 6 specific tones, spaced at 120 Hz intervals. Two sets of tones are defined – one for forward signals, and one for backward signals. There are 15 combinations of 2 out of 6 tones, so there are 10 signals for the digits 0 to 9, and 5 additional signals available for supervisory purposes.

MFC/R2 uses a separate set of frequencies for the forward and backwards directions.

The interregister signals are sent in-band. They may pass transparently through several nodes in the network between the two terminating switches. The signals are arranged in groups. When a call begins, the calling end uses group I signals, and the called end uses group A. The called end may tell the calling end to switch to using group II and group B signals, or to switch back to group A. In some countries, there are also groups III and C, used for caller number transfer. Groups III and C do not exist in the ITU specifications.

MFC/R2 uses a system called compelled signaling. To ensure the sending end never sends signals too fast, each signal from the sending end results in an acknowledgement from the receiving end. The sending end is instructed signal by signal what it should send next – a dialed digit, a digit of caller ID, etc.

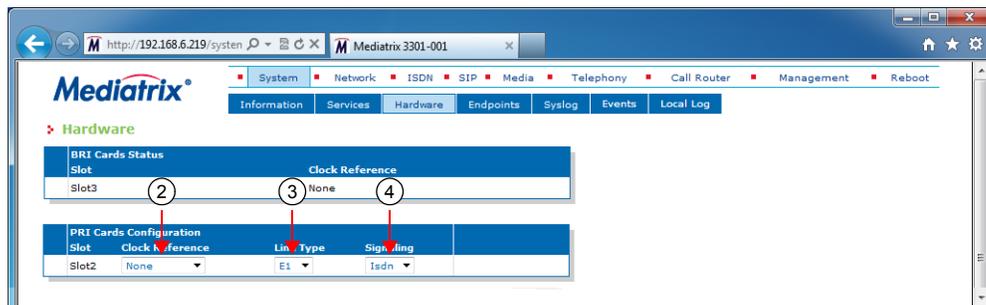
Selecting the R2 Signaling Protocol

You must set the unit to use the R2 signaling protocol. You can do so in the *System / Hardware* page. The *Hardware* page differs depending on the product and model you have.

► **To configure the Mediatrix unit hardware:**

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

Figure 71: System – Hardware Web Page



2. In the *PRI Cards Configuration* section, select the reference of the clock source in the *Clock Reference* drop-down menu.

If you want to configure the clock reference of a specific interface, you must set the *Clock Mode* drop-down menu to **Master**. See [“R2 Channel Associated Signaling” on page 194](#) for more details.

Table 160: Clock Reference

Reference	Description
None	The internal clock does not synchronize with any other source.
Other Card	The internal clock synchronizes with the other R2 interface of the Mediatrix unit. This interface must be configured in Slave mode (<i>Clock Mode</i> drop-down menu of the <i>R2 Channel Associated Signaling</i> section) to provide the clock reference to the other interfaces. Note: This choice is not available on the Mediatrix 3621 and 3631 models.

3. Select whether the line uses *T1* or *E1* in the *Line Type* drop-down menu.
Currently, R2 works only on the E1 line type.



Note: Before version 1.1r8.76, the Isdn service needed to be restarted when modifying the Line Type. Since version 1.1r8.76, the Line Type variable has been moved to the Ex1Pri_1 service and now you rather need to restart the unit instead of restarting the service when the Line Type is modified.

4. Select the **R2** signaling in the *Signaling* drop down menu.
When changing from R2 to ISDN or ISDN to R2, you must change your routes accordingly. For instance, if you are in ISDN with a route *isdn-Slot2/E1T1*, then change to R2, you must change the route to *r2-Slot2/E1T1*.
5. Click *Submit* if you do not need to set other parameters.

R2 Auto-Configuration

The R2 Auto-configuration feature allows you to detect and to configure all R2 interfaces so that the R2 link goes up and becomes usable with a minimal user interaction. When launching an auto-configuration process, it stops automatically when all interfaces have been tested. For each interface, the auto-configuration process is considered successful when the link becomes up or a failure when all combinations have been tried without having a link up.



Caution: Launching the auto-configuration may terminate abruptly all ongoing R2 calls.



Note: Auto-configuration on all R2 interfaces may take some time to complete. Some of the current R2 settings might be replaced by new values.

Please note that some parameters cannot be auto configured. For instance, the clock mode is configured according to the endpoint type, master for NT and slave for TE.

► To launch the auto-configuration process:

1. In the web interface, click the *R2* link, then the *Status* sub-link.

Figure 72: R2 – Status Configuration Section



2. Click the **Start Sensing** button.
The process starts.

Preset

The *R2 Preset Configuration* section allows you to load a set of preset configuration for your R2 connections. These preset files are located in the file system's persistent memory. They differ depending on the Mediatrix unit you are using. Depending on your unit's profile, it may be possible that no preset files are available.

Using preset files is especially useful for units that do not use the default values provided by Media5 (for instance, T1 instead of E1 for Mediatrix 3000 units). Please note that only script files work. Any other type of file present in the file system cannot be run here.

You can also export your current R2 configuration in a preset. Please note that these user-defined presets are not kept in the event of a partial or factory reset.

To see the content of the unit's file system persistent memory, go to File Manager (["Chapter 53 - File Manager" on page 543](#)). All installed configuration scripts/images are listed.

► **To load and execute a preset file:**

1. In the *R2 Status* tab, *R2 Preset Configuration* section, select one of the available preset files in the *Local Preset* drop-down menu.

Figure 73: R2 – Status Configuration Section



2. Click **Apply**.
The configuration is applied.

► **To export the current R2 configuration as a preset:**

1. In the *R2 Preset Configuration* section, type a name for the preset in the *Preset Name* field.

Figure 74: R2 – Status Configuration Section



2. Click **Save**.
The current R2 configuration is exported. Please note that these user-defined presets are not kept in the event of a partial or factory reset.
When the clock device is not synchronized, the description value of the file is "Automatically Generated". When synchronized, the description is "Automatically Generated on Date/Time". See the File Manager (["Chapter 53 - File Manager" on page 543](#)) for more details on how to see and manage the files in the unit's file system.

Partial Reset

When a partial reset is triggered, the user-defined presets are deleted.

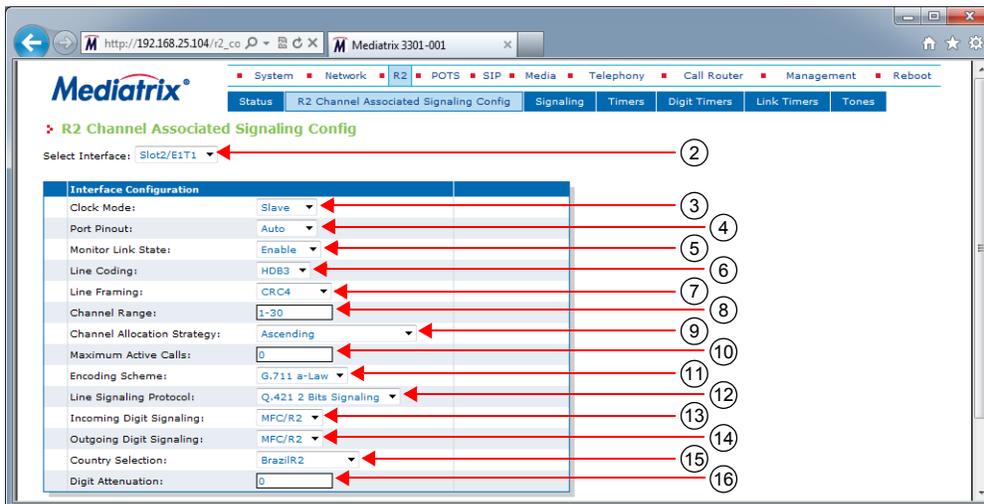
R2 Channel Associated Signaling

The *R2 Channel Associated Signaling* section allows you to define the general parameters related to R2.

► To configure the R2 CAS parameters:

1. In the web interface, click the R2 link, then the R2 Channel Associated Signaling Config sub-link.

Figure 75: R2 Channel Associated Signaling Web Page



2. Select to which interface you want to apply the changes in the *Select Interface* drop-down menu at the top of the window.

The number of interfaces available vary depending on the Mediatrix unit model you have.

3. Select the clock mode of the interface in the *Clock Mode* drop-down menu.

The interface can either generate the clocking for the line or accept the clock from the line.

Table 161: R2 Interface Clock Mode

Mode	Description
Master	The interface generates the clock.
Slave	The interface accepts the clock from the line.

The clock source can be selected from the *Clock Reference* drop-down menu (see [“Selecting the R2 Signaling Protocol” on page 192](#) for more details). The clock mode could be used, for instance, to synchronize several units in master clock mode via an E1 line.

4. Select the port pinout in the *Port Pinout* drop-down menu.

Table 162: Port Pinout

Mode	Description
Auto	The pinout is set according to the Clock Mode parameter setting (Step 3).
Te	Forces the pinout to TE regardless of the Clock Mode value.
Nt	Forces the pinout to NT regardless of the Clock Mode value.

5. Set the *Monitor Link State* drop-down menu with the physical link state of the R2 interface.

Table 163: Interface Link State

Parameter	Description
Enable	The R2 endpoint's operational state is affected by its interface physical link state. When the link state of the R2 interface is down, the operational state of its matching endpoint becomes "disable".

Table 163: Interface Link State (Continued)

Parameter	Description
Disable	The R2 endpoint's operational state is not affected by its interface physical link state.

Note that if the *Monitor Link State* parameter is enabled and the *Ignore SIP OPTIONS on no usable endpoints* parameter is also enabled in the *SIP / Interop* page, this will influence how the SIP options are answered. See “[SIP Interop](#)” on page 279 for more details.

6. Select the transmission encoding of bits in the *Line Coding* drop-down menu.

Table 164: Transmission Encoding

Coding	Description
B8ZS	Bipolar with 8-Zeros Substitution (T1 lines). Currently not available.
HDB3	High-Density Bipolar with 3-zeros (E1 lines).
AMI	Alternate Mark Inversion (E1 and T1 lines).

Make sure that the transmission encoding matches with the remote system. For further information, see ITU-T Recommendation G.703.

7. Select the frame format in the *Line Framing* drop-down menu.

Line Framing is used to synchronize the channels on the frame relay circuit (when a frame starts and finishes). Without it, the sending and receiving equipment would not be able to synchronize their frames.

Table 165: Line Framing

Format	Description
SF(D4)	Super frame. Sometimes known as D4 (T1 lines). Currently not available.
ESF	Extended super frame (T1 lines). Currently not available.
CRC4	Cyclic redundancy check 4 (E1 lines).
NO-CRC4	No Cyclic redundancy check 4 (E1 lines).

For further information, see ITU-T Recommendation G.704.

8. Define the range of active bearer channels in the *Channel Range* field.
9. Select the strategy for selecting bearer channels in the *Channel Allocation Strategy* drop-down menu.

Table 166: Channel Allocation Strategy

Allocation	Description
Ascending	Starting from the lowest-numbered non-busy bearer channel and going toward the highest-numbered non-busy bearer channel, the Mediatrix unit selects the first bearer channel available.
Descending	Starting from the highest-numbered non-busy bearer channel and going toward the lowest-numbered non-busy bearer channel, the Mediatrix unit selects the first bearer channel available.

Table 166: Channel Allocation Strategy (Continued)

Allocation	Description
RoundRobinAscending	The Mediatix unit starts from the bearer channel that follows the bearer channel used for the last call. For instance, if channel #1 was used in the last call, the unit starts with channel #2. Going toward the highest-numbered non-busy bearer channel, the unit selects the first channel available. If the highest channel is unavailable, the search continues from the lowest-numbered non-busy bearer channel.
RoundRobinDescending	The Mediatix unit starts from the bearer channel that precedes the bearer channel used for the last call. For instance, if channel #3 was used in the last call, the unit starts with channel #2. Going toward the lowest-numbered non-busy bearer channel, the unit selects the first channel available. If the lowest channel is unavailable, the search continues from the highest-numbered non-busy bearer channel.

10. Define the maximum number of active calls on the interface in the *Maximum Active Calls* field.
This limits the total number of concurrent calls on the interface. Entering **0** indicates no maximum number of active calls.
11. Set the *Encoding Scheme* drop-down menu with the voice encoding scheme in the bearer capabilities.
This encoding scheme is used when initiating a call on the R2 side. The supported encoding schemes are *G.711 u-Law* and *G.711 a-Law*.
12. Select the protocol to use for the line signaling in the *Line Signaling Protocol* drop-down menu.
This signaling must match the connected equipment or network. The Mediatix unit currently supports only the *Q421-2BitsSignaling* signaling, which is the R2 line signaling type ITU-U Q.421. It is typically used for PCM systems.
13. Select the R2 incoming digit signaling method in the *Incoming Digit Signaling* drop-down menu.
Digit signaling is also known as Address Signaling, selection signals and register signaling. The digits are used primarily to indicate the called number, but can also have other meanings.

Table 167: Incoming Digit Signaling Parameters

Allocation	Description
MfcR2	Multi Frequency Compelled - R2.
DtmfR2	Dual Tone Multi Frequency - R2.

14. Select the R2 outgoing digit signaling method in the *Outgoing Digit Signaling* drop-down menu.
Digit signaling is also known as Address Signaling, selection signals and register signaling. The digits are used primarily to indicate the called number, but can also have other meanings.

Table 168: Outgoing Digit Signaling Parameters

Allocation	Description
MfcR2	Multi Frequency Compelled - R2.
DtmfR2	Dual Tone Multi Frequency - R2.

15. Select the country in the *Country Selection* drop-down menu.
You have the following choices:
 - BrazilR2
 - MexicoR2

- ArgentinaR2
- SaudiArabiaR2
- VenezuelaR2
- PhilipinesR2
- ITU-TR2

16. Set the *Digit Attenuation* field with the additional attenuation, in dB, for MFR2/DTMF digits generation.

By default, MFR2/DTMF digits generation power is determined by country selection. This parameter provides a mean to reduce this power.

R2 Signaling Variants

This section allows you to decide whether or not you want to override the default R2 signaling parameters. The Mediatrix unit uses the following default values:

Table 169: R2 Signaling Parameters Default Values

Parameter	Default Value (ms)						
	Bra.	Mex.	Arg.	Sau.	Ven.	Phi.	ITU-T
Bits CD	1	1	1	1	1	1	1
ANI Length	0 (Variable ANI length)	0 (Variable ANI length)	0 (Variable ANI length)	0 (Variable ANI length)	0 (Variable ANI length)	0 (Variable ANI length)	0 (Variable ANI length)
DNIS Length	0 (Variable DNIS length)	0 (Variable DNIS length)	0 (Variable DNIS length)	0 (Variable DNIS length)	0 (Variable DNIS length)	0 (Variable DNIS length)	0 (Variable DNIS length)
ANI Request	Enable	Disable	Enable	Enable	Enable	Enable	Enable
Send ANI request after nth DNIS Digits	0 (Variable number of DNIS digits)	0 (Variable number of DNIS digits)	0 (Variable number of DNIS digits)	1	0 (Variable number of DNIS digits)	0 (Variable number of DNIS digits)	0 (Variable number of DNIS digits)
Collect Call Blocked Enabled	Enable	Disable	Disable	Disable	Disable	Disable	Disable
ANI Category	NatSubscriberNoPrio	NatSubscriberNoPrio	NatSubscriberNoPrio	NatSubscriberNoPrio	NatSubscriberNoPrio	NatSubscriberNoPrio	NatSubscriberNoPrio
Line Free Category	LineFreeNoCharge	LineFreeNoCharge	LineFreeCharge	LineFreeCharge	LineFreeCharge	LineFreeCharge	LineFreeCharge
ANI Restricted	Enable	Disable	Disable	Disable	Disable	Disable	Disable
Incoming Decline Method	Release	Release	Release	Release	Release	Release	Release

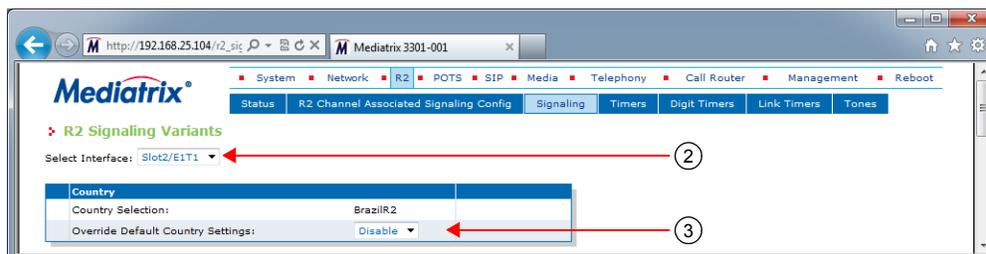
Override Default Country Settings

You can override the default R2 signaling parameters. In that case, you will have access to the *R2 Signaling Variants* section to define the signaling you want.

► **To override the R2 signaling default settings:**

1. In the web interface, click the *R2* link, then the *Signaling* sub-link.

Figure 76: R2 Signaling Variants Web Page



2. Select to which interface you want to apply the changes in the *Select Interface* drop-down menu at the top of the window.
The number of interfaces available vary depending on the Mediatrix unit model you have.
3. Select whether or not you want to override the default setting of R2 signaling parameters in the *Override Default Country Settings* drop-down menu.

Table 170: R2 Signaling Override

Allocation	Description
Disable	The interface uses the default country configuration.
Enable	The interface uses the specific country configuration as defined in the <i>R2 Signaling Variants</i> section. To retrieve the default configuration associated with the current country, click the <i>Reset to Default</i> button. Proceed to “ R2 Signaling Variants ” on page 199.

Overriding the default settings is considered as advanced configuration. Media5 recommends not to modify the country variants unless you know exactly what you are doing.

R2 Signaling Variants

This section allows you to define R2 signaling parameters. You can click the *Reset to Default* button at any time to revert back to the default R2 signaling.

► **To set R2 signaling parameters:**

1. In the *R2 Signaling Variants* section, set the C and D bits when the device transmits line signals in the *Bits CD* field.
The device ignores the C and D bits of received line signals.

Figure 77: R2 Signaling Variants Section

R2 Signaling Variants Parameters	Value	
Bits CD:	<input type="text" value="1"/>	1
ANI Length:	<input type="text" value="0"/>	2
DNIS Length:	<input type="text" value="0"/>	3
ANI Request:	<input type="text" value="Enable"/>	4
Send ANI request after nth DNIS Digits:	<input type="text" value="0"/>	5
Collect Call Blocked:	<input type="text" value="Enable"/>	6
ANI Category:	<input type="text" value="Nat Subscriber NoPri"/>	7
Line Free Category:	<input type="text" value="Line Free Charge"/>	8
ANI Restricted:	<input type="text" value="Enable"/>	9
Incoming Decline Method:	<input type="text" value="Release"/>	10

11 →

- Set the *ANI Length* field with the length of Automatic Number Identification (ANI) to be requested or sent.

If a variable-length ANI is used, the End of ANI tone set in “R2 Tones Forward Groups” on page 213 is sent to indicate the end of the ANI digits. When fixed-length ANI is used and the available ANI digits are longer than the requested length, the last n digits are sent. If available ANI digits are shorter, then the End of ANI tone set in “R2 Tones Forward Groups” on page 213 is sent.

- 0: Variable ANI length.
- 1..20: Specific ANI length.

- Set the *DNIS Length* field with the length of the Dialed Number Identification Service (DNIS) expected.

DNIS is the called party or the destination number. If a variable length is defined, then the I-15 digit is used to indicate the end of DNIS.

- 0: Variable DNIS length used.
- 1..20: Specific DNIS length expected.

- Define whether or not ANI should be requested in the *ANI Request* field.

ANI is the calling party number. When ANI is requested, the calling party category followed by the actual ANI is sent. If this parameter is enabled, the ANI request is sent after the nth DNIS digit (defined in Step 5) is received.

- Set the *Send ANI Request after nth DNIS Digits* field with the number of DNIS digits to be received before sending the ANI request (if the *ANI Request* field is set to **Enable**).

If a variable number is used, the ANI request is sent after all DNIS digits have been received.

- 0: Variable number of DNIS digits.
- 1..10: Specific number of DNIS digits.

- Define whether or not the Collect Call Blocked Option is used in the *Collect Call Blocked Enabled* drop-down menu.

Two methods actually exist to do Collect Call Blockage. The first method refers to R2 signaling and how, through the use of signals, collect calls can be blocked. The second method refers to how, through the use of double answer, the same end can be achieved.

For an incoming collect call, a signal of Group II-8 is sent forward from the caller to the called party. The called party implements the collect call blockage (when enabled) by sending backward to the caller a signal of Group B-7 indicating that the collect calls are not being accepted by the called party. Consequently, the originator of the call gets a busy tone and the local calling party circuit that has been used for the call is dropped when the originator puts the phone on hook.

The double answer allows the destination side to reject or accept a collect call (toll). Since the owner of the collect call is the person being called, the CO recognizes that the call is being dropped just by the fact that the call was dropped. For regular, non-collect calls, the owner of the call is the

person calling and not the party being called. So, if the receiver of the call decides to refuse the call, a double answer is generated within a specified time. If the receiver wants to answer the call, a double answer is not generated and the receiver is then billed for the incoming call.

Table 171: Collect Call Blockage Parameters

Parameter	Description
Enable	The signal of Group B-7 is sent if a Group II-8 (Collect Call) signal is received from the caller or a double answer is generated within a specified time depending on the value defined in the R2 Timer Variants table (see "R2 Timers Variants" on page 204 for more details).
Disable	No signal is sent in response to a Group II-8 (Collect Call) signal and/or no double answer is generated by the called side upon incoming calls.

7. Set the *ANI Category* drop-down menu with the group II forward signal to be sent upon receiving a calling party category request.

This tone indicates the category of the calling party.

Table 172: ANI Category Parameters

Parameter	Description
NatSubscriberNoPrio	The call is set up from a national subscriber's line and is non-priority.
NatSubscriberPrio	The call is set up from a national subscriber's line to which priority treatment of calls has been granted.
NatMaintenance	The call comes from a national maintenance equipment.
NatSpare	Spare.
NatOperator	The call is set up from a national operator's position.
NatData	The call will be used for national data transmission.
IntSubscriberNoPrio	The call is set up from an international subscriber's line and is non-priority.
IntData	The call will be used for international data transmission.
IntSubscriberPrio	The call is set up from an international subscriber's line to which priority treatment of calls has been granted.
IntOperator	The call is set up from an international operator's position.
CollectCall	The call is set up for Call Collect.

8. Set the *Line Free Category* drop-down menu with the group B backward signal to be sent by the incoming R2 register to indicate line free condition of the destination party.

Table 173: Line Free Category Parameters

Parameter	Description
LineFreeNoCharge	The called party's line is free but is not to be charged on answer.
LineFreeCharge	The called party's line is free but is to be charged on answer.

9. Set the *ANI Restricted* drop-down menu with the behaviour of the unit following the reception of a reject request after sending the Send next digit (ANI) request.

The request is generally rejected when the calling party is unable to send its identification.

Table 174: ANI Restricted Parameters

Parameter	Description
Enable	A congestion tone is sent in response to the reject request and the call MUST be dropped.
Disable	The unit uses the same behaviour as the End of ANI Tone and the call WILL be completed.

10. Set the *Incoming Decline Method* drop down to indicate how to cancel a call attempt from R2 if the called party rejects the call when in Seizure Acknowledged state (waiting for answer).

Table 175: Incoming Decline Method

Parameter	Description
Release:	B bit is set to 0 and state is set to Released.
ClearBack	B bit is set to 0 until decline guard expires then B is set to 1 and state is set to Clear-back.

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

R2 Timers Variants

This section allows you to decide whether or not you want to override the default R2 timers parameters. The Mediatrix unit uses the following default values:

Table 176: R2 Timers Default Values

Parameter	Default Value (ms)						
	Bra.	Mex.	Arg.	Sau.	Ven.	Phi.	ITU-T
Seizure Ack Timeout	2000	2000	2000	2000	2000	2000	2000
Fault Seizure Ack Timeout	60000	60000	60000	60000	60000	60000	60000
Double Seizure Timeout	100	100	100	100	100	100	100
Double Answer Timeout	1000	1000	1000	1000	1000	1000	1000
Answer Timeout	0	0	0	0	0	0	0
ReAnswerTimeout	1000	1000	1000	1000	1000	1000	1000
Release Guard Timeout	100	100	100	100	100	100	100
InterCall Guard Timeout	100	100	100	100	100	100	100
Congestion Tone Guard Timeout	1000	1000	1000	1000	1000	1000	1000
Unblocking Timeout	100	100	100	100	100	100	100
Address Complete Timeout	8000	8000	8000	8000	8000	8000	8000

Table 176: R2 Timers Default Values (Continued)

Parameter	Default Value (ms)						
	Bra.	Mex.	Arg.	Sau.	Ven.	Phi.	ITU-T
Wait Answer Timeout	60000	60000	60000	60000	60000	60000	60000
Digit Complete Timeout	4000	4000	4000	4000	4000	4000	4000
Wait GroupB Response Complete Timeout	3000	3000	3000	3000	3000	3000	3000
Wait Immediate Response Complete Timeout	1000	1000	1000	1000	1000	1000	1000
Play Tone Guard Timeout	70	70	70	70	70	70	70
Accept Call Timeout	2000	2000	2000	2000	2000	2000	2000
Clear Forward Guard Timeout	1500	1500	1500	1500	1500	1500	1500
Clear Backward Guard Timeout	1500	1500	1500	1500	1500	1500	1500
Fault On Answered Guard Timeout	250	250	250	250	250	250	250
Fault On Clear Backward Guard Timeout	250	250	250	250	250	250	250
Fault On Seize Ack Guard Timeout	250	250	250	250	250	250	250
Fault On Seize Guard Timeout	250	250	250	250	250	250	250
Decline Guard Timeout	1500	1500	1500	1500	1500	1500	1500

Override Default Country Settings

You can override the default R2 timers. In that case, you will have access to the *R2 Timers Variants* section to define the timers you want.

► To override the R2 timers default settings:

1. In the web interface, click the *R2* link, then the *Timers* sub-link.

Figure 78: R2 Timers Variants Web Page



2. Select to which interface you want to apply the changes in the *Select Interface* drop-down menu at the top of the window.

The number of interfaces available vary depending on the Mediatix unit model you have.

3. Select whether or not you want to override the default setting of R2 timers in the *Override Default Country Settings* drop-down menu.

Table 177: R2 Timers Override

Allocation	Description
Disable	The interface uses the default country configuration.
Enable	The interface uses the specific country configuration as defined in the <i>R2 Timers Variants</i> section. To retrieve the default configuration associated with the current country, click the <i>Reset to Default</i> button. Proceed to “R2 Timers Variants” on page 204 .

Overriding the default settings is considered as advanced configuration. Media5 recommends not to modify the country variants unless you know exactly what you are doing.

R2 Timers Variants

This section allows you to define R2 timers. You can click the *Reset to Default* button at any time to revert back to the default R2 timers.

► To set R2 timers:

1. In the *R2 Timers Variants* section, set the *Seizure ACK Timeout* field with the maximum time, in milliseconds (ms), an outgoing R2 register waits for the seizure acknowledgement signal after sending a seizure signal.

Figure 79: R2 Timers Variants Section

R2 Timers Variants Parameters	Value	
Seizure Ack Timeout:	2000	1
Fault Seizure Ack Timeout:	60000	2
Double Seizure Timeout:	100	3
Double Answer Timeout:	1500	4
Answer Timeout:	0	5
ReAnswer Timeout:	1000	6
Release Guard Timeout:	100	7
InterCall Guard Timeout:	100	8
Congestion Tone Guard Timeout:	1000	9
Unblocking Timeout:	100	10
Address Complete Timeout:	8000	11
Wait Answer Timeout:	60000	12
Digit Complete Timeout:	4000	13
Wait GroupB Response Complete Timeout:	3000	14
Wait Immediate Response Complete Timeout:	1000	15
Play Tone Guard Timeout:	70	16
Accept Call Timeout:	2000	17
Clear Forward Guard Timeout:	1500	18
Clear Backward Guard Timeout:	1500	19
Fault On Answered Guard Timeout:	250	20
Fault On Clear Backward Guard Timeout:	250	21
Fault On Seize Ack Guard Timeout:	250	22
Fault On Seize Guard Timeout:	250	23
Decline Guard Timeout:	1500	24
No Digit Timeout:	0	25

2. Set the *Fault Seizure Ack Timeout* field with the maximum time, in milliseconds (ms), an incoming R2 register waits for a seizure acknowledge failure condition to clear.
3. Set the *Double Seizure Timeout* field with the minimum time, in milliseconds (ms), an outgoing R2 register waits after a double seizure is recognized before releasing the connection.
4. Set the *Double Answer Timeout* field with the maximum time, in milliseconds (ms), an outgoing R2 register waits after receiving a clear-backward signal before releasing the connection.
5. Set the *Answer Timeout* field with the maximum time, in milliseconds, the answer signal AB=01 is applied before the clear backward signal AB=11 is sent.

This variable is generally used to reject collect call (toll) and is only available if the `CallCollectBlocked` is enabled.

A value of 0 means that the signal is applied until the call is disconnected. However, if a special event (flash hook) is detected in the answered state, then the clear backward signal AB=11 is immediately applied for a period corresponding to the *ReAnswer Timeout* parameter.

6. Set the *ReAnswer Timeout* field with the maximum time, in milliseconds, the clear backward signal AB=11 is applied before the answer signal AB=01 is reapplied again.

This variable is generally used to reject collect call (toll) and is only available if the *Collect Call Blocked Enabled* parameter is enabled (see “R2 Signaling Variants” on page 199 for more details). The *ReAnswerTimeout* is only applied if the *AnswerTimeout* or an event generating the clear backward signal is triggered.

7. Set the *Release Guard Timeout* field with the maximum time, in milliseconds (ms), an incoming R2 register waits before sending an idle line signal when a clear forward line signal is received.
8. Set the *InterCall Guard Timeout* field with the maximum time, in milliseconds (ms), an outgoing R2 register waits after receiving an idle line signal before attempting a new seizure of the line.
9. Set the *Congestion Tone Guard Timeout* field with the maximum time, in milliseconds (ms), an incoming R2 register waits after sending a congestion tone before sending a clear forward line signal and transit to the idle state.
10. Set the *Unblocking Timeout* field with the maximum time, in milliseconds (ms), a both-way trunk waits before assuming an idle state when a blocking condition is removed.
This will prevent a too aggressive seizure of the trunk.
11. Set the *Address Complete Timeout* field with the maximum time, in milliseconds (ms), that the caller waits for the reception of an Address Complete Tone after sending all ANI or DNIS digits.
12. Set the *Wait Answer Timeout* field with the maximal time, in milliseconds (ms), that the caller waits for an Answer signal (ANSW) after receiving a Group B Line Free Signal Tone.
This timer is effective only when the line is free.
13. Set the *Digit Complete Timeout* field with the maximal time, in milliseconds (ms), that the caller waits for a Group I forward tone after sending either a Group A next DNIS digit, next ANI digit, or next calling category Tone.
14. Set the *Wait GroupB Response Complete Timeout* field with the maximal time, in milliseconds (ms), that the caller waits for the confirmation of the end of the compelled sequence after receiving a Group B Signal Tone.
The end of the compelled sequence is detected by a transition of the backward tone to off.
15. Set the *Wait Immediate Response Complete Timeout* field with the maximal time, in milliseconds (ms), that the caller waits for the confirmation of the end of the compelled sequence after receiving a Group B Signal Tone.
The end of the compelled sequence is detected by a transition of the backward tone to off. This timer is specific to the immediate accept Signal Tone.
16. Set the *Play Tone Guard Timeout* field with the maximum time, in milliseconds (ms), an incoming R2 register waits after receiving the confirmation of the reception of the Group B Signal Tone before playing one of the calling tones in the caller direction.
17. Set the *Accept Call Timeout* field with the time, in milliseconds (ms), that the unit waits to accept a R2 CAS call.
18. Set the *Clear Forward Guard Timeout* field with the maximum time, in milliseconds (ms), an outgoing R2 register waits after sending a clear forward line signal before transiting to the idle state.
19. Set the *Clear Backward Guard Timeout* field with the maximum time, in milliseconds (ms), an incoming R2 register waits after sending a clear backward line signal before sending the idle line signal and transit in the idle state.
20. Set the *Fault On Answered Guard Timeout* field with the maximum time, in milliseconds (ms), an outgoing R2 register waits for the fault to clear before sending the clear forward line signal.
In the case *bb = 0* is recognized while in the answered state, no immediate action is taken. However, the clear forward signal is sent if *bb = 1* is restored or the answered guard timeout is reached.
21. Set the *Fault On Clear Backward Guard Timeout* field with the maximum time, in milliseconds (ms), an outgoing R2 register waits for the fault to clear before sending the clear forward line signal.

In the case $bb = 0$ is recognized while in the clear backward state, no immediate action is taken. However, the clear forward signal is sent if $bb = 1$ is restored or the clear backward guard timeout is reached.

22. Set the *Fault On Seize Ack Guard Timeout* field with the maximum time, in milliseconds (ms), an outgoing R2 register waits for the fault to clear before sending the clear forward line signal.

In the case $bb = 0$ is recognized while in the seize acknowledge state prior to the answer signal, no immediate action is taken. However, the clear forward signal is sent if $bb = 1$ is restored or the seize acknowledge guard timeout is reached.

23. Set the *Fault On Seize Guard Timeout* field with the maximum time, in milliseconds (ms), an outgoing R2 register waits for the fault to clear before sending the clear forward line signal.

In the case $bb = 0$ is recognized while in the seize state, no immediate action is taken. However, when the seize acknowledgement signal is recognized after the seize ack timeout period has elapsed or the seize guard timeout is reached, the clear forward signal is sent.

24. Set the *Decline Guard Timeout* field to determine the maximum time the $AB=10$ release signal is applied before sending the $AB=11$ clearback signal. This variable applies when *IncomingDeclineMethod* is set to *ClearBack* while declining a call. The value is expressed in milliseconds (ms).
25. Set the *NoDigitTimeout* field to the Maximum time an incoming R2 register waits before sending the congestion tone when no digits are received.
26. This value is expressed in milliseconds (ms)
27. Click *Submit* if you do not need to set other parameters.

R2 Digit Timers Variants

This section allows you to decide whether or not you want to override the default R2 digit timers. The Mediatrix unit uses the following default values:

Table 178: R2 Digit Timers Default Values

Parameter	Default Value (ms)						
	Bra.	Mex.	Arg.	Sau.	Ven.	Phi.	ITU-T
MFC Pulse Inter Digit Timeout	100	100	100	100	100	100	100
MFC Pulse Min On Timeout	150	150	150	150	150	150	150
MFC Max Sequence Timeout	10000	20000	20000	20000	20000	20000	20000
MFC Max On Timeout	5000	10000	10000	10000	10000	10000	10000
MFC Max Off Timeout	5000	10000	10000	10000	10000	10000	10000

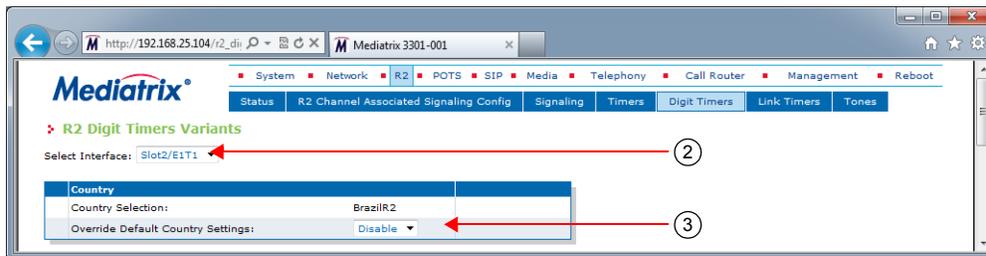
Override Default Country Settings

You can override the default R2 digit timers. In that case, you will have access to the *R2 Digit Timers Variants* section to define the timers you want.

► To override the R2 digit timers default settings:

1. In the web interface, click the *R2* link, then the *Digit Timers* sub-link.

Figure 80: R2 Digit Timers Variants Web Page



2. Select to which interface you want to apply the changes in the *Select Interface* drop-down menu at the top of the window.
The number of interfaces available vary depending on the Mediatrix unit model you have.
3. Select whether or not you want to override the default setting of R2 digit timers in the *Override Default Country Settings* drop-down menu.

Table 179: R2 Digit Timers Override

Allocation	Description
Disable	The interface uses the default country configuration.
Enable	The interface uses the specific country configuration as defined in the <i>R2 Digit Timers Variants</i> section. To retrieve the default configuration associated with the current country, click the <i>Reset to Default</i> button. Proceed to " R2 Digit Timers Variants " on page 208.

Overriding the default settings is considered as advanced configuration. Media5 recommends not to modify the country variants unless you know exactly what you are doing.

R2 Digit Timers Variants

This section allows you to define R2 digit timers. You can click the *Reset to Default* button at any time to revert back to the default R2 digit timers.

► To set R2 digit timers:

1. In the *R2 Digit Timers Variants* section, set the *MFC Pulse Inter Digit Timeout* field with the minimum delay, in milliseconds (ms), between the end of transmission of the last signal of the compelled cycle and the start of the next one.

Figure 81: R2 Digit Timers Variants Section

R2 Digit Timers Variants Parameters	Value
MFC Pulse Inter Digit Timeout:	100
MFC Pulse Min On Timeout:	150
MFC Max Sequence Timeout:	10000
MFC Max On Timeout:	5000
MFC Max Off Timeout:	5000
MF Congestion Tone Duration:	0

2. Set the *MFC Pulse Min On Timeout* field with the minimum time, in milliseconds (ms), a backward tone can be on from the backward perspective.
3. Set the *MFC Max Sequence Timeout* field with the maximum time, in milliseconds (ms), for a complete compelled signaling cycle from the forward perspective.

4. Set the *MFC Max On Timeout* field with the maximum time, in milliseconds (ms), a forward tone can be on from the forward perspective.
5. Set the *MFC Max Off Timeout* field with the maximum time, in milliseconds (ms), a forward tone can be off from the forward perspective.
6. Set the *MF Congestion Tone Duration* field with the maximum time, in milliseconds (ms), the transmission of the congestion tone can last.
7. This value is expressed in milliseconds (ms).
8. Click *Submit* if you do not need to set other parameters.

R2 Link Timers Variants

This section allows you to decide whether or not you want to override the default R2 link timers. The Mediatrix unit uses the following default values:

Table 180: R2 Link Timers Default Values

Parameter	Default Value (ms)						
	Bra.	Mex.	Arg.	Sau.	Ven.	Phi.	ITU-T
Link Activation Timeout	1000	1000	1000	1000	1000	1000	1000
Link Activation Retry Timeout	3000	3000	3000	3000	3000	3000	3000

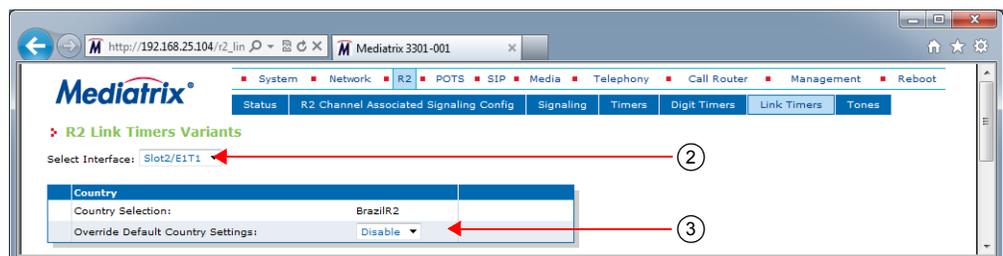
Override Default Country Settings

You can override the default R2 link timers. In that case, you will have access to the *R2 Link Timers Variants* section to define the timers you want.

► **To override the R2 link timers default settings:**

1. In the web interface, click the *R2* link, then the *Link Timers* sub-link.

Figure 82: R2 Link Timers Variants Web Page



2. Select to which interface you want to apply the changes in the *Select Interface* drop-down menu at the top of the window.

The number of interfaces available vary depending on the Mediatrix unit model you have.

3. Select whether or not you want to override the default setting of R2 link timers parameters in the *Override Default Country Settings* drop-down menu.

Table 181: R2 Link Timers Override

Allocation	Description
Disable	The interface uses the default country configuration.
Enable	The interface uses the specific country configuration as defined in the <i>R2 Link Timers Variants</i> section. To retrieve the default configuration associated with the current country, click the <i>Reset to Default</i> button. Proceed to “R2 Link Timers Variants” on page 210 .

Overriding the default settings is considered as advanced configuration. Media5 recommends not to modify the country variants unless you know exactly what you are doing.

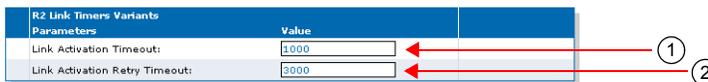
R2 Link Timers Variants

This section allows you to define R2 link timers. You can click the *Reset to Default* button at any time to revert back to the default R2 link timers.

► **To set R2 link timers:**

1. In the *R2 Link Timers Variants* section, set the *Link Activation Timeout* field with the maximum time, in milliseconds (ms), the unit waits for an activation indication coming from the physical link. The activation indication is used to indicate that the physical layer connection has been activated.

Figure 83: R2 Link Timers Variants Section



2. Set the *Link Activation Retry Timeout* field with the maximum time, in milliseconds (ms), the unit waits before attempting to re-establish the physical link. The attempt is made when the physical layer connection has been deactivated.
3. Click *Submit* if you do not need to set other parameters.

R2 Tones Variants

This section allows you to decide whether or not you want to override the default R2 tones parameters. The Mediatrix unit uses the following default values:

Table 182: R2 Tones Default Values

Parameter	Default Value (ms)						
	Bra.	Mex.	Arg.	Sau.	Ven.	Phi.	ITU-T
R2 Tones Forward Groups							
End of DNIS Tone	I15	None	I15	I15	None	I15	I15
End of ANI Tone	I15	I15	I15	I15	I15	I15	I15
Restricted ANI Tone	I12	None	None	None	I12	None	None
R2 Tones Backward Groups							

Table 182: R2 Tones Default Values (Continued)

Parameter	Default Value (ms)						
	Bra.	Mex.	Arg.	Sau.	Ven.	Phi.	ITU-T
Send Next DNIS Digit Tone	A1	A1	A1	A1	A1	A1	A1
Send Previous DNIS Digit Tone	A9	None	A9	A2	A2	A9	A9
Switch to Group II Tone	A3	A3	A3	A3	A3	A3	A3
Network Congestion Tone	A4	A4	A4	A4	A4	A4	A4
Send Calling Party Category Tone	A5	None	A5	A5	A5	A5	A5
Immediate Accept Tone	None	None	A6	A6	A6	A6	A6
Send DNIS Digit N-2 Tone	A7	None	A7	A7	A7	A7	A7
Send DNIS Digit N-3 Tone	A8	None	A8	A8	A8	A8	A8
Repeat all DNIS Tone	None	None	A10	None	A10	A10	A10
Send Next ANI Digit Tone	A5	A2	A5	A5	A9	A5	A5
Send Calling Party Category Tone Switch to Group C	None	A6	None	None	None	None	None
Send Special Information Tone	None	None	B2	B2	B2	B2	B2
User Busy Tone	B3	B2	B3	B3	B3	B3	B3
Network Congestion Tone	B4	B4	B4	B4	B4	B4	B4
Unassigned Number Tone	B8	None	B7	B5	B5	B5	B5
Line Free with Charge Tone	B1	B1	B6	B1	B6	B6	B6
Line Free with Charge Tone (Supplementary)	B6	None	None	None	None	None	None
Line Free without Charge Tone	B7	B5	B7	B6	B7	B7	B7
Line Out of Order Tone	B8	None	B8	B8	B8	B8	B8
Changed Number Tone	B3	None	None	None	None	None	None
Send Next ANI Digit Tone	None	C1	None	None	None	None	None
Repeat All DNIS Tone switch to Group A	None	C2	None	None	None	None	None

Table 182: R2 Tones Default Values (Continued)

Parameter	Default Value (ms)						
	Bra.	Mex.	Arg.	Sau.	Ven.	Phi.	ITU-T
Send Next DNIS Digit Tone switch to Group A	None	C5	None	None	None	None	None
Network Congestion Tone	None	C4	None	None	None	None	None
Send Previous DNIS Digit Tone switch to Group A	None	C6	None	None	None	None	None
Switch to Group II Tone	None	C3	None	None	None	None	None

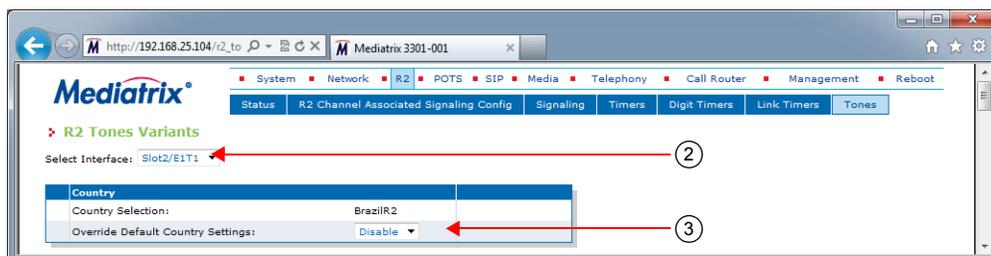
Override Default Country Settings

You can override the default R2 tones. In that case, you will have access to the *R2 Tones Forward Groups* and *R2 Tones Backward Groups* sections to define the tone you want.

► **To override the R2 tones default settings:**

1. In the web interface, click the *R2* link, then the *Tones* sub-link.

Figure 84: R2 Tones Variants Web Page



2. Select to which interface you want to apply the changes in the *Select Interface* drop-down menu at the top of the window.
The number of interfaces available vary depending on the Mediatrix unit model you have.
3. Select whether or not you want to override the default setting of R2 tones parameters in the *Override Default Country Settings* drop-down menu.

Table 183: R2 Tones Override

Allocation	Description
Disable	The interface uses the default country configuration.
Enable	The interface uses the specific country configuration as defined in the <i>R2 Tones Forward Groups</i> and <i>R2 Tones Backward Groups</i> sections. To retrieve the default configuration associated with the current country, click the <i>Reset to Default</i> button. Proceed to “R2 Tones Forward Groups” on page 213 .

Overriding the default settings is considered as advanced configuration. Media5 recommends not to modify the country variants unless you know exactly what you are doing.

R2 Tones Forward Groups

These tones fall into Groups I and II. All Group I and II tones use the ITU-T R2 forward group tone frequencies. Most of the tones in Group I are used for addressing and identification. Group II tones give information about the origin of the call. Group II tones are also sent by an outgoing MFC/R2- or International MFC/R2-register in response to one of the following backward signals:

- ▶ Change over to the reception of Group B signals.
- ▶ Send calling party's category.

Table 184: R2 Group I Forward Tones

MF	Tone	Description
1	I-1	Digit 1 (Language: French, if first signal sent in intl. link)
2	I-2	Digit 2 (Language: English, if first signal sent intl. link)
3	I-3	Digit 3 (Language: German, if first signal sent in intl. link)
4	I-4	Digit 4 (Language: Russian, if first signal sent in intl. link)
5	I-5	Digit 5 (Language: Spanish, if first signal sent in intl. link)
6	I-6	Digit 6 (Language: Spare, if first signal sent in intl. link)
7	I-7	Digit 7 (Language: Spare, if first signal sent in intl. link)
8	I-8	Digit 8 (Language: Spare, if first signal sent in intl. link)
9	I-9	Digit 9 (Discriminating digit, if first signal sent in intl. link)
10	I-10	Digit 0 (Discriminating digit, if first signal sent in intl. link)
11	I-11	Country code indicator, outgoing half-echo suppressor required
12	I-12	Country code indicator, no echo suppressor required
13	I-13	Test call indicator (call by automatic test equipment)
14	I-14	Country code indicator, outgoing half-echo suppressor inserted
15	I-15	Signal is not used

You can click the *Reset to Default* button at any time to revert back to the default R2 tones.

▶ To set the R2 tones forward groups:

1. In the *R2 Tones Forward Groups* section, select the forward Group 1 tone used to send after the DNIS digits in the *End of DNIS Tone* drop-down menu.

You have the choice between *none* and I1 to I15 Group 1 forward signals MF Tone.

Figure 85: R2 Tones – Forward Groups Section

R2 Tones Forward Groups	Value
End of DNIS Tone	I15
End of ANI Tone	I15
Restricted ANI Tone	I12

2. Select the forward Group 1 tone used to send after the ANI digits in the *End of ANI Tone* drop-down menu.

You have the choice between *none* and I1 to I15 Group 1 forward signals MF Tone.

3. Select the forward Group 1 tone used to reject a query in the *Restricted ANI Tone* drop-down menu.

This tone is generally used in response to the identification request when the caller party is unable to send his identification to the called party. If no tone is defined, the End of ANI tone is sent to the caller.

You have the choice between *none* and I1 to I15 Group 1 forward signals MF Tone.

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

R2 Tones Backward Groups

Backward tones fall into Groups A and B. The Group A tones acknowledge Group I forward signals. Under certain conditions, Group A tones also acknowledge Group II tones. Group B tones convey the following information to an outgoing MFC/R2 register:

- ▶ The condition of the switch equipment in the incoming exchange.
- ▶ The condition of the called subscriber's line.

Table 185: R2 Group A Backward Tones

MF	Tone	Description
1	A-1	Send next digit (n + 1)
2	A-2	Send last but one digit (n - 1)
3	A-3	Address-complete, changeover to reception of Group B signals
4	A-4	Congestion in the national network
5	A-5	Send calling party's category
6	A-6	Address-complete, charge, set-up speech conditions
7	A-7	Send last but two digit (n - 2)
8	A-8	Send last but three digit (n - 3)
9	A-9	Spare for national use
10	A-10	Spare for national use
11	A-11	Send country code indicator
12	A-12	Send language or discrimination digit
13	A-13	Send nature of circuit
14	A-14	Request for information on use of an echo suppressor
15	A-15	Congestion in an international exchange or at its output

Table 186: R2 Group B Backward Tones

MGF	Tone	Description
1	B-1	Spare for national use
2	B-2	Send special information tone
3	B-3	Subscriber's line busy
4	B-4	Congestion
5	B-5	Unallocated number
6	B-6	Subscriber's line free, charge
7	B-7	Subscriber's line free, no charge
8	B-8	Subscriber's line out of order
9	B-9	Spare for national use
10	B-10	Spare for national use
11	B-11	Spare for national use
12	B-12	Spare for national use

Table 186: R2 Group B Backward Tones (Continued)

MGF	Tone	Description
13	B-13	Spare for national use
14	B-14	Spare for national use
15	B-15	Spare for national use

Table 187: R2 Group C Backward Tones

MGF	Tone	Description
1	C-1	Send next number of Subscriber A
2	C-2	Send first digit BNUM
3	C-3	Send Group II and Group B signals
4	C-4	Congestion
5	C-5	Send next digit BNUM
6	C-6	Repeat last digit BNUM
7	C-7	Spare for national use
8	C-8	Spare for national use
9	C-9	Spare for national use
10	C-10	Spare for national use
11	C-11	Spare for national use
12	C-12	Spare for national use
13	C-13	Spare for national use
14	C-14	Spare for national use
15	C-15	Spare for national use

► **To set the R2 tones backward groups:**

1. In the *R2 Tones Backward Groups* section, select the backward Group A tone used to request the next DNIS digit in the *Send Next DNIS Digit Tone* drop-down menu.
You have the choice between *none* and A1 to A15 Group A backward signals MF Tone.

Figure 86: R2 Tones – Backward Groups Section

R2 Tones Backward Groups	Value	
Send Next DNIS Digit Tone	A1	1
Send Previous DNIS Digit Tone	None	2
Switch to Group II Tone	A3	3
Network Congestion Tone	A4	4
Send Calling Party Category Tone	None	5
Immediate Accept Tone	None	6
Send DNIS Digit N-2 Tone	None	7
Send DNIS Digit N-3 Tone	None	8
Repeat all DNIS Tone	A2	9
Send Next ANI Digit Tone	None	10
Send Calling Party Category Tone switch to Group C	A6	11
Send Special Information Tone	None	12
User Busy Tone	B2	13
Network Congestion Tone	B4	14
Unassigned Number Tone	None	15
Line Free with Charge Tone	B1	16
Line Free with Charge Tone (Supplementary)	None	17
Line Free without Charge Tone	B5	18
Line Out of Order Tone	None	19
Changed Number Tone	None	20
Send Next ANI Digit Tone	C1	21
Repeat all DNIS Tone switch to Group A	C2	22
Send Next DNIS Digit Tone switch to Group A	C5	23
Network Congestion Tone	C4	24
Send Previous DNIS Digit Tone switch to Group A	C6	25
Switch to Group II Tone	C3	26

2. Select the backward Group A tone used to request the previous DNIS digit in the *Send Previous DNIS Digit Tone* drop-down menu.
You have the choice between *none* and A1 to A15 Group A backward signals MF Tone.
3. Select the backward Group A tone used to request to the caller a switch of Group II signals in the *Switch to Group II Tone* drop-down menu.
You have the choice between *none* and A1 to A15 Group A backward signals MF Tone.
4. Select the backward Group A tone to be sent when a congestion network is detected in the *Network Congestion Tone* drop-down menu.
You have the choice between *none* and A1 to A15 Group A backward signals MF Tone.
5. Select the backward Group A tone sent when the backward group requests the calling party category in the *Send Calling Party Category Tone* drop-down menu.
You have the choice between *none* and A1 to A15 Group A backward signals MF Tone.
6. Select the backward Group A tone sent when the backward group accepts the call immediately in the *Immediate Accept Tone* drop-down menu.
You have the choice between *none* and A1 to A15 Group A backward signals MF Tone.
7. Select the backward Group A tone used to request the previous - 1 DNIS digit in the *Send DNIS Digit N-2 Tone* drop-down menu.
You have the choice between *none* and A1 to A15 Group A backward signals MF Tone.
8. Select the backward Group A tone used to request the previous - 2 DNIS digit in the *Send DNIS Digit N-3 Tone* drop-down menu.
You have the choice between *none* and A1 to A15 Group A backward signals MF Tone.
9. Select the backward Group A tone used to request all DNIS digits in the *Repeat All DNIS Tone* drop-down menu.
You have the choice between *none* and A1 to A15 Group A backward signals MF Tone.
10. Select the backward Group A tone used to request the next ANI digit in the *Send Next ANI Digit Tone* drop-down menu.
You have the choice between *none* and A1 to A15 Group A backward signals MF Tone.

11. Select the backward Group A tone used to request the calling party category and then switch to Group C signals in the *Send Calling Party Category Tone Switch to Group C* drop-down menu.

You have the choice between *none* and A1 to A15 Group A backward signals MF Tone.
12. Select the backward Group B tone used to send a special information tone in the *Send Special Information Tone* drop-down menu.

You have the choice between *none* and B1 to B15 Group B backward signals MF Tone.
13. Select the backward Group B tone used to signal a user busy in the *User Busy Tone* drop-down menu.

You have the choice between *none* and B1 to B15 Group B backward signals MF Tone.
14. Select the backward Group B tone used to signal a network congestion in the *Network Congestion Tone* drop-down menu.

You have the choice between *none* and B1 to B15 Group B backward signals MF Tone.
15. Select the backward Group B tone used to signal a unassigned number in the *Unassigned Number Tone* drop-down menu.

You have the choice between *none* and B1 to B15 Group B backward signals MF Tone.
16. Select the backward Group B tone used to signal that the line is free and charge must be applied in the *Line Free with Charge Tone* drop-down menu.

You have the choice between *none* and B1 to B15 Group B backward signals MF Tone.
17. Select a supplementary backward Group B tone used to detect that the line is free and charge must be applied in the *Line Free with Charge Tone (Supplementary)* drop-down menu.

This is a supplementary (optional) tone used on the reception only. You have the choice between *none* and B1 to B15 Group B backward signals MF Tone.
18. Select the backward Group B tone used to signal that the line is free and no charges must be applied in the *Line Free without Charge Tone* drop-down menu.

You have the choice between *none* and B1 to B15 Group B backward signals MF Tone.
19. Select the backward Group B tone used to signal that the line is out of order in the *Line Out of Order Tone* drop-down menu.

You have the choice between *none* and B1 to B15 Group B backward signals MF Tone.
20. Select the backward Group B tone used to signal that the subscriber has changed number in the *Changed Number Tone* field.

You have the choice between *none* and B1 to B15 Group B backward signals MF Tone.
21. Select the backward Group C tone used to request the next ANI digit in the *Send Next ANI Digit Tone* drop-down menu.

You have the choice between *none* and C1 to C15 Group C backward signals MF Tone.
22. Select the backward Group C tone used to request all DNIS digits and then switch to Group A signals in the *Repeat All DNIS Tone switch to Group A* drop-down menu.

You have the choice between *none* and C1 to C15 Group C backward signals MF Tone.
23. Select the backward Group C tone used to request the next DNIS digit and then switch to Group A signals in the *Send Next DNIS Digit Tone switch to Group A* drop-down menu.

You have the choice between *none* and C1 to C15 Group C backward signals MF Tone.
24. Select the backward Group C tone used to signal a network congestion in the *Network Congestion Tone* drop-down menu.

You have the choice between *none* and C1 to C15 Group C backward signals MF Tone.
25. Select the backward Group C tone used to request the previous DNIS digit and then switch to Group A signals in the *Send Previous DNIS Digit Tone switch to Group A* drop-down menu.

You have the choice between *none* and C1 to C15 Group C backward signals MF Tone.

26. Select the backward Group A tone used to request to the caller a switch of Group II signals in the *Switch to Group II Tone* drop-down menu.

You have the choice between *none* and C1 to C15 Group C backward signals MF Tone.

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

PRI R2 CAS Statistics

This section describes configuration that is available only in the MIB parameters of the Mediatix 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 Mediatix unit collects meaningful statistics for each PRI digital card that can be read via SNMP and CLI.

The Mediatix unit collects statistics for each of its two cards, if available. Slot 2 and Slot 3 indicate the physical location of the cards in the unit, Slot 2 being on the left when looking at the rear of the unit.

▶ To view the PRI statistics:

1. In the *ex1Pri_1MIB*, locate the *statisticsGroup* and expand it.

The following table describes the statistics available.

Table 188: R2 CAS Statistics Displayed

Statistic	Description
statsInfoFramesTransmitted	Number of HDLC frames transmitted. Note: The term frames does not refer to the structure defined in I.431.
statsInfoFramesReceived	Number of HDLC frames received. Note: The term frames does not refer to the structure defined in I.431.
statsInfoOctetsTransmitted	Number of octets transmitted. This value is obtained by cumulating the octets transmitted in the HDLC frames. Note: The term frames does not refer to the structure defined in I.431.
statsInfoOctetsReceived	Number of octets received. This value is obtained by cumulating the octets received in the HDLC frames. Note: The term frames does not refer to the structure defined in I.431.
statsInfoFCSErrors	Frame check sequence (FCS) errors indicate that frames of data are being corrupted during transmission. FCS error count is the number of frames that were received with a bad checksum (CRC value) in the HDLC frame. These frames are dropped and not propagated in the upper layers. This value is available on E1 and T1.
statsInfoFramesDropped	Number of frames dropped. This value is obtained by cumulating the number of frames dropped when transferring the data from the framer chip to the device internal buffer. This value is available on E1 and T1.
statsInfoOctetsDropped	Number of octets dropped. This value is obtained by cumulating the number of octets dropped when transferring the data from the framer chip to the device internal buffer. This value is available on E1 and T1.

Table 188: R2 CAS Statistics Displayed (Continued)

Statistic	Description
statsInfoNegativeFrameSlipsTransmitted	A frame is skipped when the frequency of the transmit clock is greater than the frequency of the transmit system interface working clock based on 2.048 MHz (on E1) or 1.544 MHz (on T1). This value is available on E1 and T1.
statsInfoNegativeFrameSlipsReceived	A frame is skipped when the frequency of the received route clock is greater than the frequency of the receive system interface working clock based on 2.048 MHz (on E1) or 1.544 MHz (on T1). This value is available on E1 and T1.
statsInfoPositiveFrameSlipsTransmitted	A frame is repeated when the frequency of the transmit clock is less than the frequency of the transmit system interface working clock based on 2.048 MHz (on E1) or 1.544 MHz (on T1). This value is available on E1 and T1.
statsInfoPositiveFrameSlipsReceived	A frame is repeated when the frequency of the receive route clock is less than the frequency of the receive system interface working clock based on 2.048 MHz (on E1) or 1.544 MHz (on T1). This value is available on E1 and T1.
statsInfoFramingError	The framing error count indicates that a FAS (Frame Alignment Signal) word has been received with an error. The FAS-bits are present in every even frame of timeslot 0 on E1. The FAS-bits are present in ESF format on T1. This value is available on E1 and T1.
statsInfoCodeViolations	The code violations count indicates that an encoding error on the PCM line has been detected. This value is available on E1 and T1.
statsInfoCRCErrors	The CRC errors count is incremented when a multiframe has been received with a CRC error. The CRC error count is available in CRC multiframe mode only on E1. The CRC error count is in ESF format on T1.
statsInfoE-BitError	The E-Bit error count gives information about the outgoing transmit PCM line if the E-bits are used by the remote end for submultiframe error indication. Incrementing is only possible in the multiframe synchronous state. Due to signaling requirements, the E-bits of frame 13 and frame 15 of the CRC multiframe can be used to indicate an error in a received submultiframes: <pre> Submultiframe I status E-bit located in frame 13 Submultiframe II status E-bit located in frame 15 no CRC error : E = 1 CRC error : E = 0 </pre> This value is only available in E1.
statsInfoBlockError	The Block Error count is incremented once per multiframe if a multiframe has been received with a CRC error or a bad frame alignment has been detected. This value is only available for ESF format on T1 only.

▶ **To reset the statistics:**

1. In the *ex1Pri_1MIB*, set the `statsInfoResetStats` variable to **10: resetStats**.

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

```
ex1Pri_1.statsInfoResetStats=10
```

E&M CAS Parameters

Page Left Intentionally Blank

CHAPTER

25

E&M CAS Configuration

This chapter describes how to configure the E&M CAS parameters of the Mediatrix unit.



Note: This chapter applies to the following models:

- Mediatrix 3531
- Mediatrix 3532
- Mediatrix 3621
- Mediatrix 3631
- Mediatrix 3632

Introduction

CAS stands for Channel Associated Signaling. With this method of signaling, each traffic channel has a dedicated signaling channel. In other words, the signaling 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.

E&M (earth & magneto, or ear & mouth) is a type of CAS signalling that defines line signaling and register signaling. It is also called Signalling System R1 and is mainly used in North America.

E&M was originally developed to allow PABXs in different geographic locations to communicate over an analog private circuit. Some digital interfaces such as CAS also use versions of E&M signaling.

The terms forwards and backwards are heavily used in descriptions of E&M. Forwards is the direction from the calling party to the called party. Backwards is the direction from the called party to the calling party.

You can configure Mediatrix unit parameters for the E1/T1 E&M CAS.

Line Signals for the Digital Version of E&M

Line signalling uses the ABCD bits of CAS. Several types of E&M signalling exist.

Line Signals for the Analogue Version of E&M

E&M has its roots in older analogue signalling. The digital versions of E&M replicate the operation of older analogue signalling versions.

Inter-Register Signals (Defined in ITU-T Q.310-Q.332)

Inter-register signalling uses either R1 tones (defined in Q.310-Q.332) or DTMF depending on the signalling type and detailed user-defined variant configuration.

The inter-register signals are sent in-band. They may pass transparently through several nodes in the network between the two terminating switches.

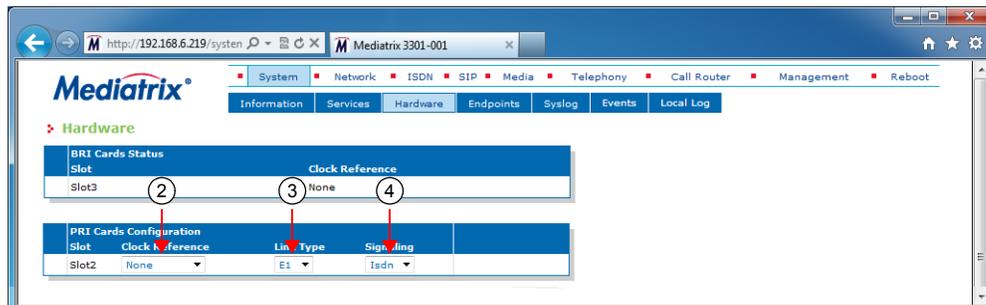
Selecting the E&M Signalling Protocol

You must set the unit to use the E&M signalling protocol. You can do so in the *System / Hardware* page. The *Hardware* page differs depending on the product and model you have.

► To configure the Mediatrix unit hardware:

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

Figure 87: System – Hardware Web Page



2. In the *PRI Cards Configuration* section, select the reference of the clock source in the *Clock Reference* drop-down menu.

If you want to configure the clock reference of a specific interface, you must set the *Clock Mode* drop-down menu to **Master**. See “E&M Channel Associated Signaling” on page 226 for more details.

Table 189: Clock Reference

Reference	Description
None	The internal clock does not synchronize with any other source.
Other Card	The internal clock synchronizes with the other E&M interface of the Mediatrix unit. This interface must be configured in Slave mode (<i>Clock Mode</i> drop-down menu of the <i>E&M Channel Associated Signaling</i> section) to provide the clock reference to the other interfaces. Note: This choice is not available on the Mediatrix 3521, 3621 and 3631 models.

3. Select whether the line uses *T1* or *E1* in the *Line Type* drop-down menu.
4. Select the **E&M** signaling in the *Signaling* drop down menu.

When changing from E&M to ISDN/R2 or ISDN/R2 to E&M, you must change your routes accordingly. For instance, if you are in ISDN with a route *isdn-Slot2/E1T1*, then change to E&M, you must change the route to *e&m-Slot2/E1T1*.

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

E&M Auto-Configuration

The E&M Auto-configuration feature allows you to detect and to configure all E&M interfaces so that the E&M link goes up and becomes usable with a minimal user interaction. When launching an auto-configuration process, it stops automatically when all interfaces have been tested. For each interface, the auto-configuration process is considered successful when the link becomes up or a failure when all combinations have been tried without having a link up.



Caution: Launching the auto-configuration may terminate abruptly all ongoing E&M calls.



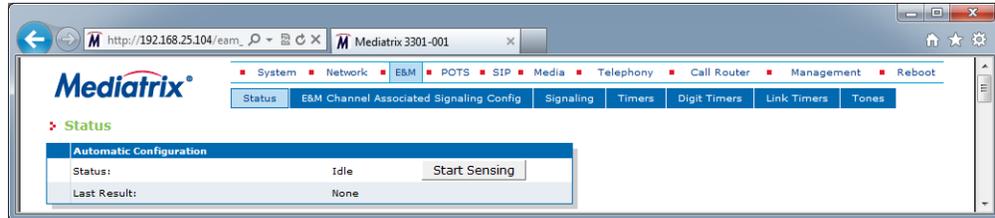
Note: Auto-configuration on all E&M interfaces may take some time to complete. Some of the current E&M settings might be replaced by new values.

Please note that some parameters cannot be auto configured. For instance, the clock mode is configured according to the endpoint type, master for NT and slave for TE.

► **To launch the auto-configuration process:**

1. In the web interface, click the *E&M* link, then the *Status* sub-link.

Figure 88: E&M – Status Configuration Section



2. Click the **Start Sensing** button.
The process starts.

Preset

The *E&M Preset Configuration* section allows you to load a set of preset configuration for your E&M connections. These preset files are located in the file system's persistent memory. They differ depending on the Mediatrix unit you are using. Depending on your unit's profile, it may be possible that no preset files are available.

Using preset files is especially useful for units that do not use the default values provided by Media5 (for instance, T1 instead of E1 for Mediatrix 3000 units). Please note that only script files work. Any other type of file present in the file system cannot be run here.

You can also export your current E&M configuration in a preset. Please note that these user-defined presets are not kept in the event of a partial or factory reset.

To see the content of the unit's file system persistent memory, go to File Manager (["Chapter 53 - File Manager" on page 543](#)). All installed configuration scripts/images are listed.

► **To load and execute a preset file:**

1. In the *E&M Status* tab, *E&M Preset Configuration* section, select one of the available preset files in the *Local Preset* drop-down menu.

Figure 89: E&M – Status Configuration Section



2. Click **Apply**.
The configuration is applied.

► **To export the current E&M configuration as a preset:**

1. In the *E&M Preset Configuration* section, type a name for the preset in the *Preset Name* field.

Figure 90: E&M – Status Configuration Section



2. Click **Save**.

The current E&M configuration is exported. Please note that these user-defined presets are not kept in the event of a partial or factory reset.

When the clock device is not synchronized, the description value of the file is "Automatically Generated". When synchronized, the description is "Automatically Generated on Date/Time". See the File Manager ("Chapter 53 - File Manager" on page 543) for more details on how to see and manage the files in the unit's file system.

Partial Reset

When a partial reset is triggered, the user-defined presets are deleted.

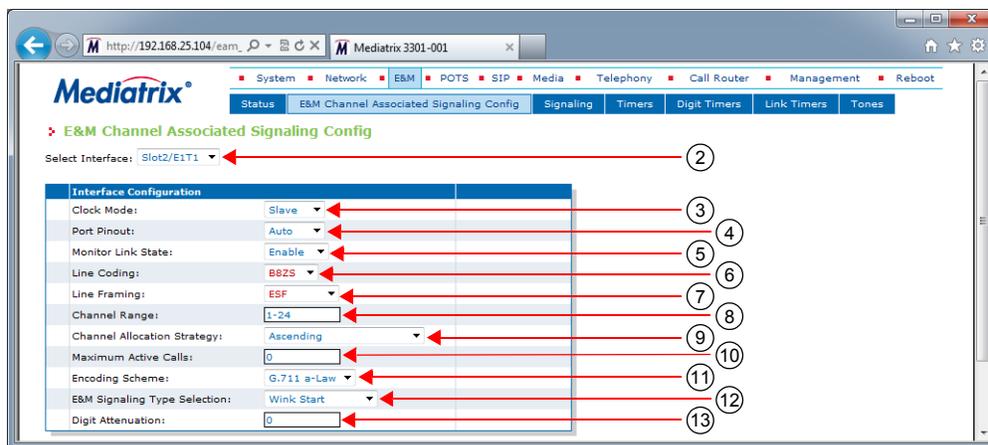
E&M Channel Associated Signaling

The *E&M Channel Associated Signaling* section allows you to define the general parameters related to E&M.

► **To configure the E&M CAS parameters:**

1. In the web interface, click the *E&M* link, then the *E&M Channel Associated Signaling Config* sub-link.

Figure 91: E&M Channel Associated Signaling Web Page



2. Select to which interface you want to apply the changes in the *Select Interface* drop-down menu at the top of the window.
The number of interfaces available vary depending on the Mediatrix unit model you have.
3. Select the clock mode of the interface in the *Clock Mode* drop-down menu.
The interface can either generate the clocking for the line or accept the clock from the line.

Table 190: E&M Interface Clock Mode

Mode	Description
Master	The interface generates the clock.
Slave	The interface accepts the clock from the line.

The clock source can be selected from the *Clock Reference* drop-down menu (see "Selecting the E&M Signalling Protocol" on page 223 for more details). The clock mode could be used, for instance, to synchronize several units in master clock mode via an E1 line.

- Select the port pinout in the *Port Pinout* drop-down menu.

Table 191: Port Pinout

Mode	Description
Auto	The pinout is set according to the Clock Mode parameter setting (Step 3).
Master	Forces the pinout to Master regardless of the clock mode.
Slave	Forces the pinout to Slave regardless of the clock mode.

- Set the *Monitor Link State* drop-down menu with the physical link state of the E&M interface.

Table 192: Interface Link State

Parameter	Description
Enable	The E&M endpoint's operational state is affected by its interface physical link state. When the link state of an E&M interface is down, the operational state of its matching endpoint becomes "disable".
Disable	The E&M endpoint's operational state is not affected by its interface physical link state

Note that if the *Monitor Link State* parameter is enabled and the *Ignore SIP OPTIONS on no usable endpoints* parameter is also enabled in the *SIP / Interop* page, this will influence how the SIP options are answered. See "[SIP Interop](#)" on page 279 for more details.

- Select the transmission encoding of bits in the *Line Coding* drop-down menu.

Table 193: Transmission Encoding

Coding	Description
B8ZS	Bipolar with 8-Zeros Substitution (T1 lines).
HDB3	High-Density Bipolar with 3-zeros (E1 lines).
AMI	Alternate Mark Inversion (E1 and T1 lines).

Make sure that the transmission encoding matches with the remote system. For further information, see ITU-T Recommendation G.703.

- Select the frame format in the *Line Framing* drop-down menu.

Line Framing is used to synchronize the channels on the frame relay circuit (when a frame starts and finishes). Without it, the sending and receiving equipment would not be able to synchronize their frames.

Table 194: Line Framing

Format	Description
SF	Super frame. Sometimes known as D4 (T1 lines).
ESF	Extended super frame (T1 lines).
CRC4	Cyclic redundancy check 4 (E1 lines).
NO-CRC4	No Cyclic redundancy check 4 (E1 lines).

For further information, see ITU-T Recommendation G.704.

- Define the range of active bearer channels in the *Channel Range* field.

9. Select the strategy for selecting bearer channels in the *Channel Allocation Strategy* drop-down menu.

Table 195: Channel Allocation Strategy

Allocation	Description
Ascending	Starting from the lowest-numbered non-busy bearer channel and going toward the highest-numbered non-busy bearer channel, the Mediatrix unit selects the first bearer channel available.
Descending	Starting from the highest-numbered non-busy bearer channel and going toward the lowest-numbered non-busy bearer channel, the Mediatrix unit selects the first bearer channel available.
RoundRobinAscending	The Mediatrix unit starts from the bearer channel that follows the bearer channel used for the last call. For instance, if channel #1 was used in the last call, the unit starts with channel #2. Going toward the highest-numbered non-busy bearer channel, the unit selects the first channel available. If the highest channel is unavailable, the search continues from the lowest-numbered non-busy bearer channel.
RoundRobinDescending	The Mediatrix unit starts from the bearer channel that precedes the bearer channel used for the last call. For instance, if channel #3 was used in the last call, the unit starts with channel #2. Going toward the lowest-numbered non-busy bearer channel, the unit selects the first channel available. If the lowest channel is unavailable, the search continues from the highest-numbered non-busy bearer channel.

10. Define the maximum number of active calls on the interface in the *Maximum Active Calls* field.
This limits the total number of concurrent calls on the interface. Entering **0** indicates no maximum number of active calls.
11. Set the *Encoding Scheme* drop-down menu with the voice encoding scheme in the bearer capabilities.
This encoding scheme is used when initiating a call on the E&M side. The supported encoding schemes are *G.711 u-Law* and *G.711 a-Law*.
12. Select the *E&M Signaling Type Selection* drop-down menu with the proper E&M signalling type.

Table 196: Signalling Type Selection

Signalling Type	Description
Wink start	Sets configuration parameters for basic Wink Start signalling. After setting the SignallingType, individual configuration parameters can be overridden for detail adjustment. Note that the outgoing and incoming register signaling uses DTMF signaling type by default.
Immediate Start	Sets configuration parameters for basic Immediate Start signalling. After setting the Signaling Type, individual configuration parameters can be overridden for detail adjustment. Note that the outgoing and incoming register signaling uses DTMF signaling type by default.
Feature Group B	Sets configuration parameters for the Feature Group B signalling defined by National Exchange Carrier Association. After setting the Signaling Type, individual configuration parameters can be overridden for detail adjustment. Note that the outgoing and incoming register signaling uses MF R1 signaling type by default.

Table 196: Signalling Type Selection (Continued)

Signalling Type	Description
Feature Group D	Sets configuration parameters for the Feature Group D signalling defined by National Exchange Carrier Association. After setting the Signaling Type, individual configuration parameters can be overridden for detail adjustment. Note that the outgoing and incoming register signaling uses MF R1 signaling type by default.

13. Set the *Digit Attenuation* field with the additional attenuation, in dB, for MFR1/DTMF digits generation.

By default, MFR1/DTMF digits generation power is determined by variant selection. This parameter provides a mean to reduce this power.

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

E&M Signalling Variants

This section allows you to decide whether or not you want to override the default E&M signalling parameters. The Mediatrix unit uses the following default values:

Table 197: E&M Signaling Parameters Default Values

Parameter	Default Value (ms)			
	Wink Start	Immediate Start	FGB ^a	FGD ^b
Bits BCD	8	8	8	8
ANI Length	0	0	0	0
DNIS Length	0	0	0	0
Incoming Register Signaling	DTMF	DTMF	MfR 1	MfR 1
Outgoing Register Signaling	DTMF	DTMF	MfR 1	MfR 1
Incoming Dial Map	%dnis%t	%dnis%t	%kp%dnis%st	%kp%ani%st%kp%dnis%st
Outgoing Dial Map	%dnis%t	%dnis%t	%kp%dnis%st	%kp%dnis%st
Wait Wink	Enable	Disable	Enable	Enable
Wait Wink Ack	Disable	Disable	Disable	Enable
Send Wink	Enable	Disable	Enable	Enable
Send Wink Ack	Disable	Disable	Disable	Enable

a. Feature Group B

b. Feature Group D

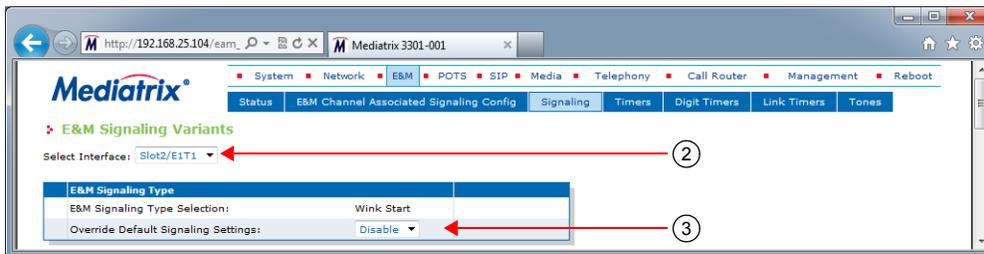
Override Default Signaling Settings

You can override the default E&M signaling parameters. In that case, you will have access to the *E&M Signaling Variants* section to define the signaling you want.

► To override the E&M signaling default settings:

1. In the web interface, click the *E&M* link, then the *Signaling* sub-link.

Figure 92: E&M Signaling Variants Web Page



2. Select to which interface you want to apply the changes in the *Select Interface* drop-down menu at the top of the window.

The number of interfaces available vary depending on the Mediatrix unit model you have.

3. Select whether or not you want to override the default setting of E&M signalling parameters in the *Override Default Signaling Settings* drop-down menu.

Table 198: E&M Signaling Override

Allocation	Description
Disable	The interface uses the default configuration associated with the selected Signaling Type. The configuration set in the current row has no effect on the default configuration of the selected Signaling Type.
Enable	The interface uses the specific signalling configuration as defined in the <i>E&M Signaling Variants</i> section. To retrieve the default configuration associated with the current Signaling Type, click the <i>Reset to Default</i> button. Proceed to “E&M Signalling Variants” on page 230.

Overriding the default settings is considered an advanced configuration. Media5 recommends not to modify the signalling variants unless you know exactly what you are doing.

E&M Signalling Variants

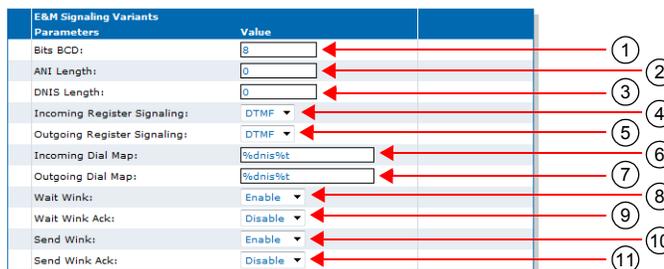
This section allows you to define E&M signalling parameters. You can click the *Reset to Default* button at any time to revert back to the default E&M signalling.

► To set E&M signalling parameters:

1. In the *E&M Signaling Variants* section, set the B, C and D bits when the device transmits line signals in the *Bits BCD* field.

The device ignores the B, C and D bits of received line signals.

Figure 93: E&M Signaling Variants Section



BCD bits definition

- 0..7 : BCD bits are set to the specified value.
- 8 : BCD bits follow the A bit.



Note: On E1-CAS, the ABCD bit value cannot be set to 0000. If the BCD variable is set to 000 or to follow the A bit, then the bitmask BCD=001 will be used instead.

2. Set the *ANI Length* field with the expected length of Automatic Number Identification (ANI) to be requested or sent.

ANI is the number of the calling party.

- 0: Variable ANI length.
- 1..20: Specific ANI length.

3. Set the *DNIS Length* field with the expected length of the Dialed Number Identification Service (DNIS).

DNIS is the called party or the destination number.

- 0: Variable DNIS length used.
- 1..20: Specific DNIS length expected.

4. Set the *Incoming Register Signaling* drop-down menu with the proper incoming register signaling method.

Table 199: Incoming Register Signalling Parameters

Parameter	Description
MfR1	Multi Frequency - R1.
DTMF	Dual Tone Multi Frequency.

5. Set the *Outgoing Register Signaling* drop-down menu with the proper outgoing register signaling method.

Table 200: Outgoing Register Signalling Parameters

Parameter	Description
MfR1	Multi Frequency - R1.
DTMF	Dual Tone Multi Frequency.

6. Set the *Incoming Dial Map* field with the dial map expression to match against on the incoming side.

The dial map expression uses a special format using macros that enables you to construct a custom dial map using the ANI, DNIS and other special tones as separator. The dial map macros supported are:

- %dnis : DNIS (Dialed Number Identification Service).
- %ani : ANI (Automatic Number Identification).
- %kp : KP (start-of-pulsing) tone (MF R1 only).
- %st : ST (end-of-pulsing) tone (MF R1 only).
- %t : Interdigit timeout.
- A,B,C,D,*,# : Control tones (DTMF only).
- A,B,C,D,E : Control tones (MF R1 only).

Examples:

- %dnis*%ani : (dnis)*(ani)
- %kp%dnis%st%kp%ani%st : KP(dnis)STKP(ani)ST
- A%dnisBA%aniB : A(dnis)BA(ani)B

7. Set the *Outgoing Dial Map* field with the dial map format for the outgoing dial string.

The dial string generation uses a special format using macros that enables you to construct a custom dial string using the ANI, DNIS and other specials tones used as separator. The dial string uses regular expression to replace the macros with the proper call parameter value. The dial map macros supported are:

- %dnis : DNIS (Dialed Number Identification Service).
- %ani : ANI (Automatic Number Identification).
- %kp : KP (start-of-pulsing) tone (MF R1 only).
- %st : ST (end-of-pulsing) tone (MF R1 only).
- %t : Interdigit timeout.
- A,B,C,D,*,# : Control tones (DTMF only).
- A,B,C,D,E : Control tones (MF R1 only).

Examples : ANI=1234 DNIS=6789 KP=A ST=D

- %dnis*%ani : 6789*1234
- %kp%dnis%st%kp%ani%st : A6789DA1234D
- A%dnisBA%aniB : A6789BA1234B

8. Set the *Wait Wink* drop-down menu with whether or not the outgoing register should wait for a wink before proceeding with digit transmission.
9. Set the *Wait Wink Ack* drop-down menu with whether or not the outgoing register should wait for a wink acknowledge after all digit reception.
10. Set the *Send Wink* drop-down menu with whether or not the incoming register should send a wink to notify the remote side that digit information can be sent.
11. Set the *Send Wink Ack* drop-down menu with whether or not the incoming register should send a wink to acknowledge the receipt of all digits.
12. Click *Submit* if you do not need to set other parameters.

E&M Timers Variants

This section allows you to decide whether or not you want to override the default E&M timers parameters. The Mediatix unit uses the following default values:

Table 201: E&M Timers Default Values

Parameter	Default Value (ms)			
	Wink Start	Immediate Start	FGB ^a	FGD ^b
Backward Wait Pre Wink Timeout	50	50	50	50
Backward Send Wink Timeout	200	200	200	200
Backward Wait First Digit Timeout	10000	10000	10000	10000
Backward Clear Backward Timeout	2000	2000	2000	2000
Backward Digit Complete Timeout	4000	4000	4000	4000
Forward Wait Wink Timeout	5000	5000	5000	5000
Forward Wait Max Wink on Timeout	5000	5000	5000	5000
Forward Wait Pre Dial Timeout	140	140	140	140
Forward Wait Answer Timeout	180000	180000	180000	180000
Forward Clear Forward Timeout	2000	2000	2000	2000

Table 201: E&M Timers Default Values (Continued)

Parameter	Default Value (ms)			
	Wink Start	Immediate Start	FGB ^a	FGD ^b
Release Guard Timeout	200	200	200	200

- a. Feature Group B
- b. Feature Group D

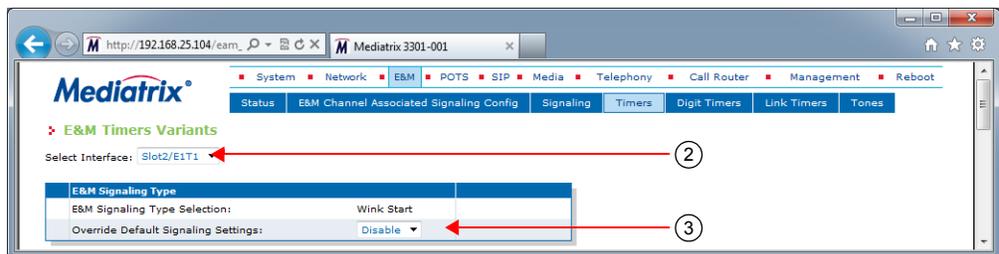
Override Default Signaling Settings

You can override the default E&M timers. In that case, you will have access to the *E&M Timers Variants* section to define the timers you want.

► **To override the E&M timers default settings:**

1. In the web interface, click the *E&M* link, then the *Timers* sub-link.

Figure 94: E&M Timers Variants Web Page



2. Select to which interface you want to apply the changes in the *Select Interface* drop-down menu at the top of the window.
The number of interfaces available vary depending on the Mediatrix unit model you have.
3. Select whether or not you want to override the default setting of E&M timers in the *Override Default Signaling Settings* drop-down menu.

Table 202: E&M Timers Override

Allocation	Description
Disable	The interface uses the default configuration associated with the selected Signaling Type. The configuration set in the current row has no effect on the default configuration of the selected Signaling Type.
Enable	The interface uses the specific signaling configuration as defined in the <i>E&M Timers Variants</i> section. To retrieve the default configuration associated with the current signalling type, click the <i>Reset to Default</i> button. Proceed to “ E&M Timers Variants ” on page 233.

Overriding the default settings is considered as advanced configuration. Media5 recommends not to modify the signalling variants unless you know exactly what you are doing.

E&M Timers Variants

This section allows you to define E&M timers. You can click the *Reset to Default* button at any time to revert back to the default E&M timers.

► To set E&M timers:

1. In the *E&M Timers Variants* section, set the *Backward Wait Pre Wink Timeout* field with the amount of time, in milliseconds (ms), an incoming register waits before sending the wink that acknowledges the seizure.

Figure 95: E&M Timers Variants Section

E&M Timers Variants Parameters	Value
Backward Wait Pre Wink Timeout:	50
Backward Send Wink Timeout:	200
Backward Wait First Digit Timeout:	10000
Backward Clear Backward Timeout:	2000
Backward Digit Complete Timeout:	4000
Forward Wait Wink Timeout:	5000
Forward Wait Max Wink On Timeout:	5000
Forward Wait Pre Dial Timeout:	140
Forward Wait Answer Timeout:	180000
Forward Clear Forward Timeout:	2000
Release Guard Timeout:	200

2. Set the *Backward Send Wink Timeout* field with the duration, in milliseconds (ms), of the wink signal is applied by the incoming register to signal seizure acknowledgment.
3. Set the *Backward Wait First Digit Timeout* field with the maximum time, in milliseconds (ms), an incoming register waits for the first incoming digit after the line seizure.
4. Set the *Backward Clear Backward Timeout* field with the maximum time, in milliseconds (ms), an incoming register waits after sending a clear backward line signal before transiting to the idle state.
5. Set the *Backward Digit Complete Timeout* field with the maximum time, in milliseconds (ms), the incoming register waits for the next digit before considering the digit sequence as completed.
6. Set the *Forward Wait Wink Timeout* field with the maximum time, in milliseconds (ms), an outgoing register waits for seizure acknowledgement after seizing the line.
7. Set the *Forward Wait Max Wink On Timeout* field with the maximum time, in milliseconds (ms), an outgoing register waits for the seizure acknowledgement wink to complete.
8. Set the *Forward Wait Pre Dial Timeout* field with the amount of time, in milliseconds (ms), an outgoing register waits after the wink to start dialing.
9. Set the *Forward Wait Answer Timeout* field with the maximum time, in milliseconds (ms), an outgoing register waits for the call to be answered.
10. Set the *Forward Clear Forward Timeout* field with the maximum time, in milliseconds (ms), an outgoing register waits after sending a clear forward line signal before transiting to the idle state.
11. Set the *Release Guard Timeout* field with the maximum time, in milliseconds (ms), a register waits after sending an idle line signal to prevent a new seizure of the line.
12. Click *Submit* if you do not need to set other parameters.

E&M Digit Timers Variants

This section allows you to decide whether or not you want to override the default E&M digit timers. The Mediatrix unit uses the following default values:

Table 203: E&M Digit Timers Default Values

Parameter	Default Value (ms)			
	Wink Start	Immediate Start	FGB ^a	FGD ^b
KP On Timeout	100	100	100	100
KP Off Timeout	68	68	68	68

- a. Feature Group B
- b. Feature Group D

Override Default Signaling Settings

You can override the default E&M digit timers. In that case, you will have access to the *E&M Digit Timers Variants* section to define the timers you want.

► **To override the E&M digit timers default settings:**

1. In the web interface, click the *E&M* link, then the *Digit Timers* sub-link.

Figure 96: E&M Digit Timers Variants Web Page



2. Select to which interface you want to apply the changes in the *Select Interface* drop-down menu at the top of the window.
The number of interfaces available vary depending on the Mediatrix unit model you have.
3. Select whether or not you want to override the default setting of E&M digit timers in the *Override Default Signaling Settings* drop-down menu.

Table 204: E&M Digit Timers Override

Allocation	Description
Disable	The interface uses the default configuration associated with the selected Signaling Type. The configuration set in the current row has no effect on the default configuration of the selected Signaling Type.
Enable	The interface uses the specific signaling configuration as defined in the <i>E&M Digit Timers Variants</i> section. To retrieve the default configuration associated with the current signalling, click the <i>Reset to Default</i> button. Proceed to “E&M Digit Timers Variants” on page 235.

Overriding the default settings is considered as advanced configuration. Media5 recommends not to modify the signalling variants unless you know exactly what you are doing.

E&M Digit Timers Variants

This section allows you to define E&M digit timers. You can click the *Reset to Default* button at any time to revert back to the default E&M digit timers.

► **To set E&M digit timers:**

1. In the *E&M Digit Timers Variants* section, set the *KP On Timeout* field with the time, in milliseconds (ms), during which the MF R1 KP tone is on.

Figure 97: E&M Digit Timers Variants Section



2. Set the *KP Off Timeout* field with the duration, in milliseconds (ms), of the pause after the MF R1 KP tone.
3. Click *Submit* if you do not need to set other parameters.

E&M Link Timers Variants

This section allows you to decide whether or not you want to override the default E&M link timers. The Mediatrix unit uses the following default values:

Table 205: E&M Link Timers Default Values

Parameter	Default Value (ms)			
	Wink Start	Immediate Start	FGB ^a	FGD ^b
Link Activation Timeout	1000	1000	1000	1000
Link Activation Retry Timeout	3000	3000	3000	3000

a. Feature Group B

b. Feature Group D

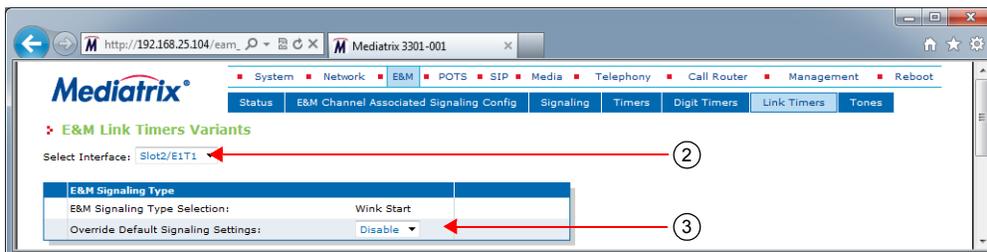
Override Default Signalling Settings

You can override the default E&M link timers. In that case, you will have access to the *E&M Link Timers Variants* section to define the timers you want.

► **To override the E&M link timers default settings:**

1. In the web interface, click the *E&M* link, then the *Link Timers* sub-link.

Figure 98: E&M Link Timers Variants Web Page



2. Select to which interface you want to apply the changes in the *Select Interface* drop-down menu at the top of the window.
The number of interfaces available vary depending on the Mediatrix unit model you have.
3. Select whether or not you want to override the default setting of E&M link timers parameters in the *Override Default Signaling Settings* drop-down menu.

Table 206: E&M Link Timers Override

Allocation	Description
Disable	The interface uses the default configuration associated with the selected Signaling Type. The configuration set in the current row has no effect on the default configuration of the selected Signaling Type.

Table 206: E&M Link Timers Override (Continued)

Allocation	Description
Enable	The interface uses the specific signaling configuration as defined in the <i>E&M Link Timers Variants</i> section. To retrieve the default configuration associated with the current signalling, click the <i>Reset to Default</i> button. Proceed to “ E&M Link Timers Variants ” on page 237.

Overriding the default settings is considered as advanced configuration. Media5 recommends not to modify the signalling variants unless you know exactly what you are doing.

E&M Link Timers Variants

This section allows you to define E&M link timers. You can click the *Reset to Default* button at any time to revert back to the default E&M link timers.

► To set E&M link timers:

- In the *E&M Link Timers Variants* section, set the *Link Activation Timeout* field with the maximum time, in milliseconds (ms), the unit waits for an activation indication coming from the physical link.
The activation indication is used to indicate that the physical layer connection has been activated.

Figure 99: R2 Link Timers Variants Section

- Set the *Link Activation Retry Timeout* field with the maximum time, in milliseconds (ms), the unit waits before attempting to re-establish the physical link.
The attempt is made when the physical layer connection has been deactivated.
- Click *Submit* if you do not need to set other parameters.

E&M Tones Variants

This section allows you to decide whether or not you want to override the default E&M tones parameters. The Mediatrix unit uses the following default values:

Table 207: E&M Tones Default Values

Parameter	Default Value (ms)			
	Wink Start	Immediate Start	FGB ^a	FGD ^b
KP Tone	MFC 10	MFC 10	MFC 10	MFC 10
ST Tone	MFC 13	MFC 13	MFC 13	MFC 13

a. Feature Group B

b. Feature Group D

Override Default Signalling Settings

You can override the default E&M tones. In that case, you will have access to the *E&M Tones Variants* section to define the tone you want.

► **To override the E&M tones default settings:**

1. In the web interface, click the *E&M* link, then the *Tones* sub-link.

Figure 100: E&M Tones Variants Web Page



2. Select to which interface you want to apply the changes in the *Select Interface* drop-down menu at the top of the window.

The number of interfaces available vary depending on the Mediatrix unit model you have.

3. Select whether or not you want to override the default setting of E&M tones parameters in the *Override Default Signaling Settings* drop-down menu.

Table 208: E&M Tones Override

Allocation	Description
Disable	The interface uses the default configuration associated with the selected Signaling Type. The configuration set in the current row has no effect on the default configuration of the selected Signaling Type.
Enable	The interface uses the specific signalling configuration as defined in the <i>E&M Tones Variants</i> section. To retrieve the default configuration associated with the current signalling, click the <i>Reset to Default</i> button. Proceed to “E&M Tones Variants” on page 238.

Overriding the default settings is considered as advanced configuration. Media5 recommends not to modify the signalling variants unless you know exactly what you are doing.

E&M Tones Variants

This section allows you to define E&M tones. You can click the *Reset to Default* button at any time to revert back to the default E&M tones.

► **To set the E&M tones:**

1. In the *E&M Tones Variants* section, set the *KP Tone* drop-down menu with the proper KP (start-of-pulsing) signal.

You have the choice between *none* and MFR0 to MFR14 Tones.

Figure 101: E&M Tones Variants Section



2. Set the *ST Tone* drop-down menu with the proper ST (end-of-pulsing) signal. You have the choice between *none* and MFR0 to MFR14 Tones.
3. Click *Submit* if you do not need to set other parameters.

PRI E&M Statistics

This section describes configuration that is available only in the MIB parameters of the Mediatrix 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 Mediatrix unit collects meaningful statistics for each PRI digital card that can be read via SNMP and CLI. The Mediatrix unit collects statistics for each of its two cards, if available. Slot 2 and Slot 3 indicate the physical location of the cards in the unit, Slot 2 being on the left when looking at the rear of the unit.

▶ **To view the PRI statistics:**

1. In the *ex1Pri_1MIB*, locate the *statisticsGroup* and expand it.

The following table describes the statistics available.

Table 209: E&M Statistics Displayed

Statistic	Description
statsInfoFramesTransmitted	Number of HDLC frames transmitted. Note: The term frames does not refer to the structure defined in I.431.
statsInfoFramesReceived	Number of HDLC frames received. Note: The term frames does not refer to the structure defined in I.431.
statsInfoOctetsTransmitted	Number of octets transmitted. This value is obtained by cumulating the octets transmitted in the HDLC frames. Note: The term frames does not refer to the structure defined in I.431.
statsInfoOctetsReceived	Number of octets received. This value is obtained by cumulating the octets received in the HDLC frames. Note: The term frames does not refer to the structure defined in I.431.
statsInfoFCSErrors	Frame check sequence (FCS) errors indicate that frames of data are being corrupted during transmission. FCS error count is the number of frames that were received with a bad checksum (CRC value) in the HDLC frame. These frames are dropped and not propagated in the upper layers. This value is available on E1 and T1.
statsInfoFramesDropped	Number of frames dropped. This value is obtained by cumulating the number of frames dropped when transferring the data from the framer chip to the device internal buffer. This value is available on E1 and T1.
statsInfoOctetsDropped	Number of octets dropped. This value is obtained by cumulating the number of octets dropped when transferring the data from the framer chip to the device internal buffer. This value is available on E1 and T1.
statsInfoNegativeFrameSlipsTransmitted	A frame is skipped when the frequency of the transmit clock is greater than the frequency of the transmit system interface working clock based on 2.048 MHz (on E1) or 1.544 MHz (on T1). This value is available on E1 and T1.
statsInfoNegativeFrameSlipsReceived	A frame is skipped when the frequency of the received route clock is greater than the frequency of the receive system interface working clock based on 2.048 MHz (on E1) or 1.544 MHz (on T1). This value is available on E1 and T1.

Table 209: E&M Statistics Displayed (Continued)

Statistic	Description
statsInfoPositiveFrameSlipsTransmitted	A frame is repeated when the frequency of the transmit clock is less than the frequency of the transmit system interface working clock based on 2.048 MHz (on E1) or 1.544 MHz (on T1). This value is available on E1 and T1.
statsInfoPositiveFrameSlipsReceived	A frame is repeated when the frequency of the receive route clock is less than the frequency of the receive system interface working clock based on 2.048 MHz (on E1) or 1.544 MHz (on T1). This value is available on E1 and T1.
statsInfoFramingError	The framing error count indicates that a FAS (Frame Alignment Signal) word has been received with an error. The FAS-bits are present in every even frame of timeslot 0 on E1. The FAS-bits are present in ESF format on T1. This value is available on E1 and T1.
statsInfoCodeViolations	The code violations count indicates that an encoding error on the PCM line has been detected. This value is available on E1 and T1.
statsInfoCRCErrors	The CRC errors count is incremented when a multiframe has been received with a CRC error. The CRC error count is available in CRC multiframe mode only on E1. The CRC error count is in ESF format on T1.
statsInfoE-BitError	The E-Bit error count gives information about the outgoing transmit PCM line if the E-bits are used by the remote end for submultiframe error indication. Incrementing is only possible in the multiframe synchronous state. Due to signaling requirements, the E-bits of frame 13 and frame 15 of the CRC multiframe can be used to indicate an error in a received submultiframes: <pre> Submultiframe I status E-bit located in frame 13 Submultiframe II status E-bit located in frame 15 no CRC error : E = 1 CRC error : E = 0 </pre> This value is only available in E1.
statsInfoBlockError	The Block Error count is incremented once per multiframe if a multiframe has been received with a CRC error or a bad frame alignment has been detected. This value is only available for ESF format on T1 only.

► **To reset the statistics:**

1. In the *ex1Pri_1MIB*, set the `statsInfoResetStats` variable to **10: resetStats**.

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

```
ex1Pri_1.statsInfoResetStats=10
```

SIP Parameters

Page Left Intentionally Blank

CHAPTER 26

SIP Gateways

This chapter describes how to add and remove SIP gateways in the Mediatrrix 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.

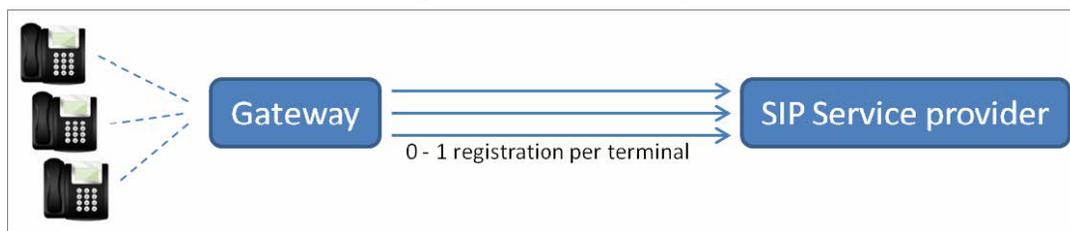
Adding a SIP gateway triggers a warning message if the total number of registrations configured reached the defined limit. See [“Number of Registrations” on page 259](#) for more details.

There are two types of SIP Gateways:

Trunk Gateway

A trunk gateway is generally used when the device is connected to a PBX or phone network; it can also be used when connected to terminal equipment while using a SIP trunk to a SIP server.

Figure 102: Trunk Gateway



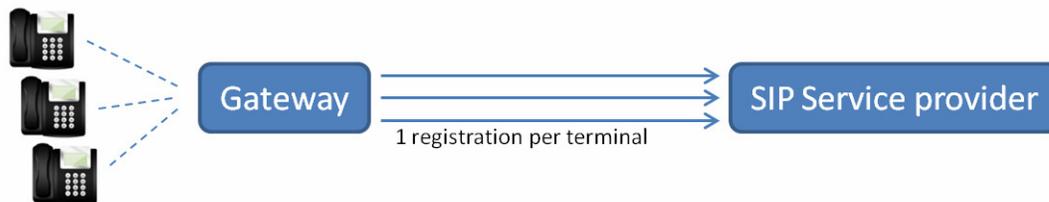
The characteristics of a trunk gateway are as follows:

- ▶ It works with endpoint and user (unit) registrations.
- ▶ SIP dialogs are established independently of each other, depending on the SIP keep alive mechanism defined. See [“Keep Alive” on page 251](#) for more details on the SIP keep alive mechanism.
- ▶ A listening port allows for dialogs to be established by any peer.
- ▶ When the destination is a FQDN, each SIP transaction is possibly sent to a different IP address, depending on the DNS query result. A trunk gateway assumes all SIP servers identified by a single FQDN have a synchronized state.
- ▶ Connections can be persistent or not, depending on the type of transport: UDP and TCP transports are limited to non-persistent connections; TLS establishes persistent connections to the outbound proxy, home domain proxy and registrar and non-persistent connections to other targets.
- ▶ The call router shows a single SIP source/destination for the gateway.

Endpoint Gateway

An endpoint gateway is generally used when the device is connected to terminal equipment where each endpoint has a separate SIP connection to the SIP server.

Figure 103: Endpoint Gateway



An endpoint gateway is a type of gateway introduced to satisfy use cases with failover/failback based on registrations for a single user.

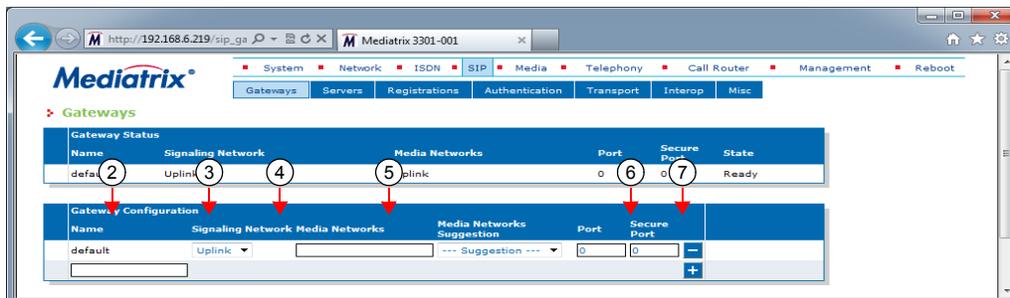
The characteristics of an endpoint gateway are as follows:

- ▶ It works with endpoint registrations only (no unit registrations can be associated to an endpoint gateway).
- ▶ SIP dialogs for a given SIP user can only be established once the user is registered to the server.
- ▶ It creates a persistent connection for each SIP user. This connection allows for dialogs to be established only by the server to which the user is registered. “No listening port” allows a connection to be established by a peer.
- ▶ Failover/failback to another server requires the SIP user to register on that server prior to establishing a dialog.
- ▶ The call router and gateway status tables show an instance of the gateway for each user of the gateway.

▶ To configure multiple SIP gateways:

1. In the web interface, click the *SIP* link, then the *Gateways* sub-link.

Figure 104: SIP – Gateways Web Page



You can add a new gateway by clicking the **+** button. The Mediatix 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 type of SIP gateway to be configured in the *Type* drop-down menu.
The default value is “Trunk”; select “Endpoint” for an endpoint gateway.
4. 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.

- 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 "InterfaceName" 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 Mediatrix 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 from the offer.

- If the gateway type is set to "Trunk", 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.



Note: When the gateway type is set to "Endpoint" the SIP Port and Secure Port have no effect and must be set to 0 since each user has a unique UDP/TCP port.

For "Endpoint" gateways, only the base port can be set with the variable `Persistent Base Port` in the *SIP Transport* configuration web interface.

- If the gateway type is set to "Trunk", 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.

- 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 210: SIP Gateway States

State	Description
Ready	The gateway is ready to make and receive calls.

Table 210: SIP Gateway States

State	Description
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.
Unregistered	Indicates some registrations that are mandatory for this gateway failed. See “Unregistered Unit Behaviour” on page 263 for more details.
Invalid Config	The gateway cannot start due to an inconsistent configuration.

CHAPTER 27

SIP Servers

This chapter describes how to configure the SIP server parameters of the Mediatrix unit.

It describes the following:

- ▶ How to define the SIP servers IP information.
- ▶ How to define the SIP gateways IP information.

Introduction

The Mediatrix unit uses the following types of servers:

Table 211: 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 <i>To</i> and <i>From</i> 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)

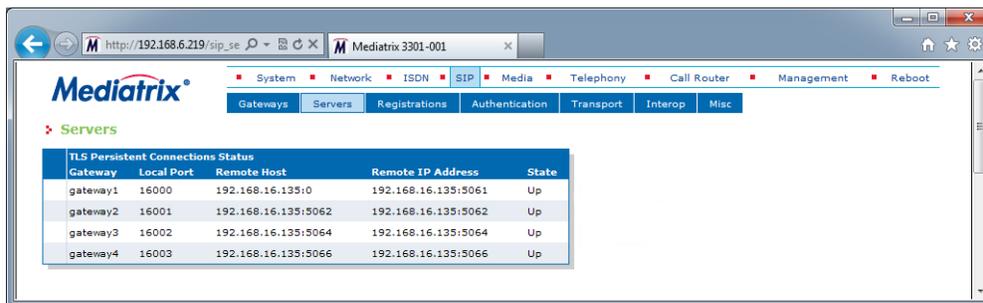
A proxy that receives requests from a client, even though it may not be the server resolved by the Request-URI. Typically, a user agent is manually configured with an outbound proxy.

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 Mediatrix 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. TLS connection is currently only supported with Trunk gateway.

Figure 105: SIP – TLS Persistent Connections Status Section



The following information is available:

Table 212: 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. <ul style="list-style-type: none"> Up: The TLS connection is established. Down: The TLS connection is not established.

SIP Servers Configuration

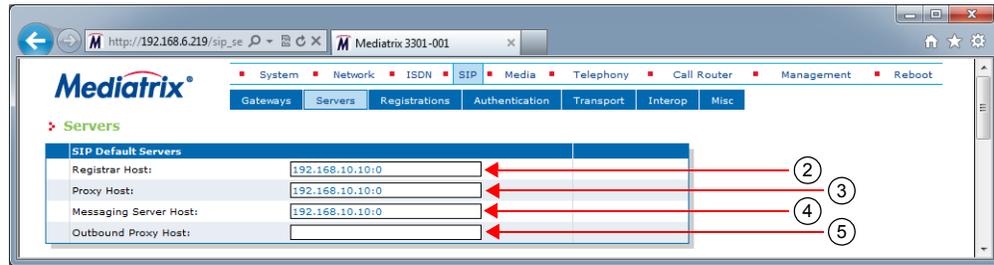
This section describes how to configure the IP address and port number of the SIP servers.

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 106: 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 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 255.

5. 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.



Note: The Endpoint gateway can only have a single next hop. If no outbound proxy is set then, if used, the proxy host, the registrar host and the messaging server host must be set to the same FQDN or IP Address. If the hosts are not set to the same URL or IP address, the SIP Gateway State will be set to Invalid Config. See [Table 210 on page 245](#) for the list of SIP Gateway states.

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

Multiple SIP Gateways

The Mediatix 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 26 - SIP Gateways](#)” on page 243 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 107: SIP Servers – Specific Registrar Section

Registrar Servers		
Gateway	Gateway Specific	Registrar Host
default	No	192.168.0.10:5060

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 317](#)) sections.

Figure 108: SIP Servers – Messaging Section

Messaging Servers		
Gateway	Gateway Specific	Messaging Server Host
default	No	192.168.10.10:0

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 109: SIP Servers – Specific Proxy Section

Gateway	Gateway Specific	Proxy Host	Outbound Proxy Host
default	No	192.168.0.10:0	0.0.0.0:0

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`



Note: The Endpoint gateway can only have a single next hop. If no outbound proxy is set then, if used, the proxy host, the registrar host and the messaging server host must be set to the same FQDN or IP Address. If the hosts are not set to the same URL or IP address, the SIP Gateway State will be set to Invalid Config. See [Table 210 on page 245](#) for the list of SIP Gateway states.

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). Setting the address to **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 Mediatrix unit sends messages periodically to the server to ensure that it can still be reached. The SIP keep alive mechanism is only supported with Trunk gateways.

► 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 110: Keep Alive Section



Table 213: Keep Alive Parameters

Parameter	Description
None	No keep alive is performed.
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 <i>Transmission Timeout</i> field in “SIP Interop” on page 279), 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 <i>Transmission Timeout</i> field in “SIP Interop” on page 279), 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.

On Endpoint gateways, the keep alive mechanism is always considered to be “None”.

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 214: 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 253 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 251 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 111: SIP Servers – Specific Keep alive Targets

Keep Alive Destination Gateway	Alternate Destination
default	192.168.0.10:0

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

Outbound Proxy Loose Router Configuration

This section describes configuration that is available only in the MIB parameters of the Mediatrix 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 248.

You can use two types of configuration:

- Default configurations that apply to all the endpoints of the Mediatrix unit.
- Specific configurations that override the default configurations.

You can define specific configurations for each endpoint in your Mediatrix unit. For instance, you could enable a codec for all the endpoints of the Mediatrix 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 215: 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 247 for details.

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 215: Outbound Proxy Router Status (Continued)

Type	Description
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.
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 216: 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 28

SIP Registration

This chapter describes how to configure the registration parameters of the Mediatrix unit.

Endpoints Registration

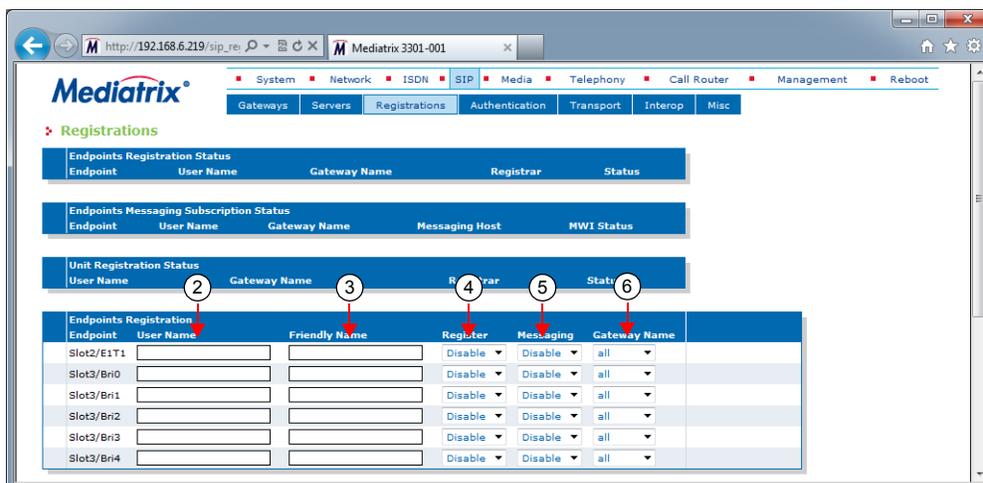
Each endpoint of the Mediatrix unit has its own registration information. You can set information for each endpoint such as its telephone number and friendly name.

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 259 for more details.

► To set endpoints registration information:

1. In the web interface, click the *SIP* link, then the *Registrations* sub-link.

Figure 112: 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.



Note: If two or more endpoints have the same user name, a single registration request and/or subscription request will be performed under that user name.

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 217: 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 248.

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 26 - SIP Gateways](#)” on page 243 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 Mediatrix 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 *sipEp MIB*, set the *UserAgentContactDomain* variable in the *UserAgent* table or,
2. In the CLI or a configuration script, use:
SipEp.UserAgent[EpId=index].ContactDomain=value

Accept Language

The *AcceptLanguage* parameter allows a user to indicate the preferred language that will be used for displayed phrases, session descriptions, status responses carried as message bodies in the response. It is used to fill the Accept-Language SIP header field.

You can configure the parameter by:

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

► **To set *AcceptLanguage*:**

1. In the *SipEp Mib*. set the *AcceptLanguage* variable in *UserAgent* table or,
 2. In the CLI or a configuration script use
SipEp.UserAgent[index-value].AcceptLanguage=<value>
- Index is the endpoint name

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 Mediatrix 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 259 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 113: SIP Registrations – Unit Registration Section

Unit Registration Index	User Name	Gateway Name	
1	<input type="text"/>	all	- +

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 26 - SIP Gateways](#)” on page 243 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 260](#) 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 114: SIP Registrations – Registration Configuration Section

Registration Configuration	
Default Registration Refresh Time:	<input type="text" value="60"/>
Proposed Expiration Value In Registration:	<input type="text" value="0"/>
Default Expiration Value In Registration:	<input type="text" value="3600"/>

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 Mediatrix 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 262](#) 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 Mediatrix unit. See [“Registration Refresh” on page 261](#) 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 Mediatrix unit. See [“Registration Expiration” on page 261](#) 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 Mediatrix unit. See [“Expiration Value in Registration” on page 261](#) 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 Mediatrix 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 243](#)) pairs. The Mediatrix 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 115: Example, Gateway Configuration

Gateway Configuration				
Name	Network Interface	Port	Secure Port	
default	Uplink	0	0	-
gw1	Rescue	0	0	-
gw2	Lan1	0	0	-
				+

Figure 116: Example, Registrations Configuration

Endpoints Registration				
Endpoint	User Name	Friendly Name	Register	Gateway Name
Slot2/E1T1	ur1	ur1	Enable	all
Slot3/E1T1	ur2	ur2	Enable	gw2

Unit Registration		
Index	User Name	Gateway Name
1	ta1	all
2	ta2	all
3	ta3	gw1
4	ta4	default
		+

The following table describes how to compute the total number of registrations for this example:

Table 218: Number of Registrations Example

Parameter	Setting	Nb of Registrations
Endpoint Registration 1 in Figure 116	Gateway Name set to all ^a	3
Endpoint Registration 2 in Figure 116	Gateway Name set to gw2	1
Unit Registration 1 in Figure 116	Gateway Name set to all	3
Unit Registration 2 in Figure 116	Gateway Name set to all	3
Unit Registration 3 in Figure 116	Gateway Name set to gw1	1
Unit Registration 4 in Figure 116	Gateway Name set to default	1
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 115](#). 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 Mediatrix 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 Mediatrix unit.
- ▶ Specific configurations that override the default configurations.

You can define specific configurations for each endpoint in your Mediatrix unit. For instance, you could enable a codec for all the endpoints of the Mediatrix 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 258](#)), 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 258](#)), 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_Gateway"]="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 258](#)), 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 ‘RefreshTime’ variable (“Registration Refresh” on page 261).

► **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"]="Value"
```

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 219: 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 220: 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 Unit 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 221: Unregistered Unit 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 unit behaviour:**

1. In the *sipEpMIB*, locate the *registrationGroup* folder.
2. Set the `defaultUnitRegistrationUnregisteredBehavior` variable.
You can also use the following line in the CLI or a configuration script:
`sipEp.defaultUnitRegistrationUnregisteredBehavior="value"`
where *Value* may be as follows:.

Table 222: Unregistered Unit Behaviour Values

Value	Meaning
100	NoEffect
200	DisableGateway

Behaviour on Initial-Registration Reception

You can configure the behaviour of the Mediatix unit upon reception of a 380 or 504 carrying an XML body with a specified 'initial-registration' action.

The following values are supported:

Table 223: 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. When there are duplicates, only one REGISTER request is sent for all the duplicates.
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 224: 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 Mediatrix 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 Mediatrix 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

29

SIP Authentication

This chapter describes how to configure authentication parameters of the Mediatrix unit.



Caution: The *SIP > Authentication* page is not accessible if you have the User or Observer access right. See “Users” on page 537 for more details.

Authentication Configuration

Authentication information allows you to add some level of security to the Mediatrix unit endpoints by setting user names and passwords.

You can add four types of authentication information:

Table 225: 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 Mediatrix 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 Mediatrix 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 Mediatrix 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 Mediatrix 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 **Username**. 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 117: SIP Configuration – Authentication Web Page

✚ Authentication

Authentication	Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name	Actions
	1	Unit				Enable			Edit [v] + -
	2	Unit				Enable			Edit ^ [v] + -
	3	Unit				Enable			Edit ^ [v] + -
	4	Unit				Enable			Edit ^ [v] + -
	5	Unit				Enable			Edit ^ [v] + -
	6	Unit				Enable			Edit ^ [v] + -
	7	Unit				Enable			Edit ^ [v] + -
	8	Unit				Enable			Edit ^ [v] + -
	9	Unit				Enable			Edit ^ [v] + -
	10	Unit				Enable			Edit ^ [v] + -
	11	Unit				Enable			Edit ^ [v] + -
	12	Unit				Enable			Edit ^ [v] + -
	13	Unit				Enable			Edit ^ [v] + -
	14	Unit				Enable			Edit ^ [v] + -
	15	Unit				Enable			Edit ^ [v] + -
	16	Unit				Enable			Edit ^ [v] + -
	17	Unit				Enable			Edit ^ [v] + -
	18	Unit				Enable			Edit ^ [v] + -
	19	Unit				Enable			Edit ^ [v] + -
	20	Unit				Enable			Edit ^ [v] + -

Number of rows to add: +

[D] Edit All Entries Refresh Registration

2. Do one of the following:
 - a. 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.
 - b. 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.
 - c. If you want to edit a single authentication entry, locate the proper row in the table and click the **Edit** button.
 - d. If you want to edit 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 226: Authentication Panel – Single Entry

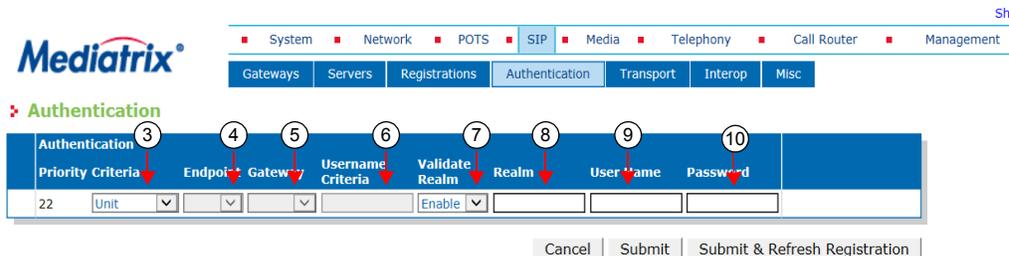
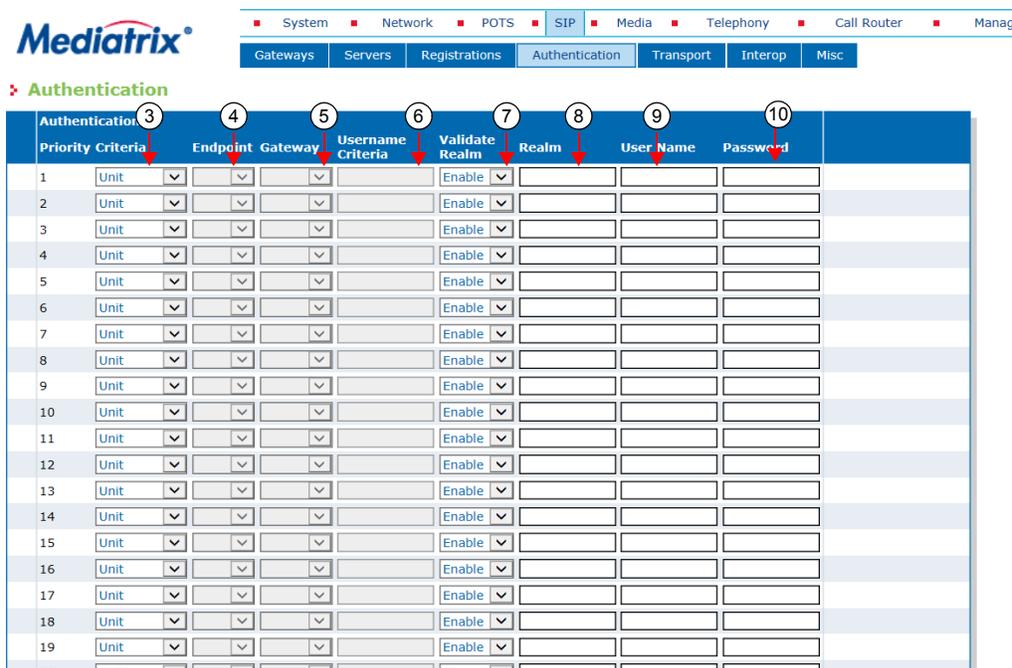


Table 227: Authentication Panel – Page



3. Select which criterion to use for matching an authentication request with an authentication entry in the *Criteria* column.

Table 228: 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..

4. Enter a string that identifies an endpoint in the UserAgent.
This field is available only if you have selected **Endpoint** in the *Criteria* column for the specific row.
5. Enter a string that identifies a SIP gateway in the *GatewayStatus* table.
This field is available only if you selected **Gateway** in the *Criteria* column for the specific row.
6. Enter a string that identifies a username in the SIP request to authenticate. this fiel is available only if you selected Username in the *Criteria* column for the specific row.

7. Select whether or not the current credentials are valid for any realm in the corresponding *Validate Realm* drop-down menu.

Table 229: Realm Authentication Parameters

Parameter	Description
Disable	The current credentials are valid for any realm. The corresponding <i>Realm</i> field is read-only and cannot be modified.
Enable	The credentials are used only for a specific realm set in the corresponding <i>Realm</i> field.

8. Enter a realm for each authentication row in the *Realm* column.
When authentication information is required from users, the realm identifies who requested it.
9. Enter a string that uniquely identifies this endpoint in the realm in the *User Name* column.
10. Enter a user password in the *Password* column.
11. 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.

CHAPTER

30

SIP Transport Parameters

This chapter describes the SIP transport parameters you can set.

SIP Transport Type

You can globally set the transport type for all the endpoints of the Mediatrix unit to either UDP (User Datagram Protocol), TCP (Transmission Control Protocol), or TLS (Transport Layer Security).

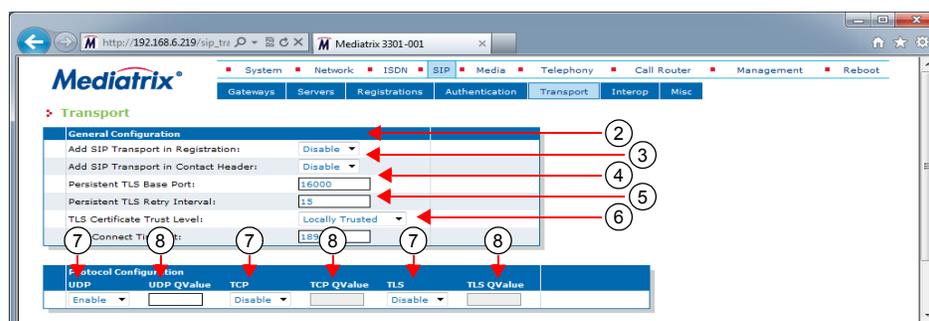
The Mediatrix unit will include its supported transports in its registrations.

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 Mediatrix 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 118: 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 Mediatrix 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 Mediatrix 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 Mediatrix 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 Mediatrix 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 persistent connections with SIP servers when the TLS transport is enabled in the *Persistent Base Port* field.
5. Set the time interval, in seconds, before retrying the establishment of a persistent connection in the *Failback Interval* field.

This is the interval that the Mediatrix unit waits before retrying periodically to establish a persistent connection using a single IP address or a FQDN. This timer is started when a persistent connection goes down or fails to connect to the destination.

A gateway automatically performs failover and failback procedure when it is configured with more than one transport protocol or when responses to DNS queries return more than one IP address.

The failover and failback procedures are triggered when a SIP transaction fails. The type of transaction that enables the failover depends on the type of the gateway. Additional SIP conditions can be configured through *sipFailoverConditions* variables (see “[SIP Failover Conditions](#)” on page 277).

During failover, the failed transaction is reattempted on another IP address with a lower priority (according to the DNS response). When the *Failback Interval* expires, the IP address with a higher priority is reattempted.

6. In the *TLS Trusted Certificate Level* field, define how a peer certificate is considered trusted for a TLS connection.

Table 230: 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 49 - Certificates Management ” on page 501 for more details). The certificate revocation status is not verified.
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.

Endpoint gateway supports UDP transport only. On a Trunk gateway, 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 58 & “SNTP Configuration” on page 57 for more details).
- install the security certificates used to authenticate the server to which you will connect (see “Chapter 49 - Certificates Management” on page 501 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 Mediatrix 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

Transport TLS Cipher Suite Settings

You can define the allowed cipher suites for the network security settings when using TLS connection.

Table 231: Cipher Suites Configuration Parameters

Parameter	Description
CS1	<p>This is the default value and represents the cipher suites configuration prior to this variable being introduced. This should be changed if additional network security is required. This value includes the following cipher suites:</p> <ul style="list-style-type: none"> • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_3DES_EDE_CBC_SHA • TLS_RSA_WITH_RC4_128_SHA

Table 231: Cipher Suites Configuration Parameters

Parameter	Description
CS2	<p>This represents a secure configuration using SHA-1. This value includes the following cipher suites:</p> <ul style="list-style-type: none"> • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_3DES_EDE_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
CS3	<p>This represents the most secure configuration using SHA-2. Only the most secure cipher suites are allowed when using this value.</p> <ul style="list-style-type: none"> • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 • TLS_CDH_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256

► **To set the TLS transport cipher suite configuration parameter:**

1. In the *SipEpMIB*, set the TLS transport cipher suite configuration in the `TransportTlsciphersuite` variable.

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

```
SipEp.TransportTlsciphersuite="value"
```

where *Value* may be as follows:

Table 232: Cipher Suites Configuration Values

Value	Meaning
100	CS1
200	CS2
300	CS3

Transport Tls Version Settings

You can define the allowed TLS versions when using TLS persistent connections.

You can configure this parameter as follows:

- by using a MIB browser

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

Table 233: Tls Version Configuration Settings

Parameter	Description
SSLv3	Allow SSL version 3 and all TLS versions.
TLSv1	Allow TLS versions 1 and up.
TLSv1_1	Allow TLS versions 1.1 and up.
TLSv1_2	Allow TLS versions 1.2 and up.

The default value is TLSv1.

▶ **To set the Transport Tls Version configuration parameter:**

1. In the *SipEpMIB*, locate the *TransportGroup* folder.
2. Set the Transport Tls Version configuration in the `transportTlsVersion` parameter.

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

```
SipEp.TransportTlsVersion = "value"
```

where value may be:

Table 234: Tls Version Configuration Values

Value	Meaning
100	SSLv3
200	TLSv1
300	TLSv1_1
400	TLSv1_2

UDP Source Port Behaviour

On Trunk gateway type, you can configure whether or not the Mediatrix 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. This variable has no effect on Endpoint gateways. Endpoint gateways always use the same UDP port for sending and receiving messages.

The following parameters are available:

Table 235: 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 236: 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 Mediatrix unit so that it requests client authentication when acting as a TLS server.

The following parameters are available:

Table 237: TLS Client Authentication Parameters

Parameter	Description
disable	The Mediatrix 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 <i>Certificate Validation</i> drop-down menu of the <i>TLS Interop</i> section (<i>SIP > Interop</i> web page). See “TLS Interop” on page 286 for more details.

► **To set TLS client authentication:**

1. In the *sipEpMIB*, set whether or not the Mediatrix 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 238: TLS Client Authentication Values

Value	Meaning
0	disable
1	enable

Force DNS NAPTR In TLS

The Mediatrix 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 315](#) for more details).

The following parameters are available:

Table 239: 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 240: Force DNS NAPTR in TLS Values

Value	Meaning
0	disable
1	enable

SIP Failover Conditions

You can configure additional SIP-level conditions for failover. These conditions can also be configured specifically per gateway.

► **To set the SIP failover conditions:**

1. In the *sipEpMIB*, set the `DefaultSipFailoverConditions` variable to the proper SIP failover condition value.

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

```
sipEp.defaultSipFailoverConditions="value"
```

where *Value* is a sequence of keywords separated by commas; spaces and tabs are ignored. If *Value* is empty, only the connection-level failover conditions apply.

Supported keywords list is:

- `5xxOnRegistration`: 5xx (Server Failure) response received on a registration attempt.

 **Note:** The syntax is designed to support multiple keywords even though only a single keyword is defined for now.

2. If you want to set failover conditions for a specific SIP gateway, set the following variables:
 - `gwSpecificFailoverEnableConfig` variable for the specific SIP gateway you want to configure to **enable**.
 - `gwSpecificFailoversipFailoverConditions` 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.gwSpecificFailover.EnableConfig[GatewayName="default"]="5xxOnRegistration"
sipEp.gwSpecificFailover.SipFailoverConditions[GatewayName="specific_gateway"]="value"
```

where:

- *Specific_Gateway* is the name of the SIP gateway you want to configure.

- *Value* is a SIP failover condition as defined in Step 1.

Persistent Port Interval

You can set the interval used to cycle through a range of ports.

► **To set the persistent port interval:**

1. In the *sipEpMIB*, set the *TransportPersistentPortInterval* parameter or,
2. In the CLI or a configuration script, use:
`sipEp.TransportPersistentPortInterval = "value".`

Where a value equal to 0 indicates that the cycling mechanism is disabled.

CHAPTER 31

Interop Parameters

This chapter describes the interoperability parameters that allow the Mediatrx unit to properly work, communicate, or connect with specific IP devices.

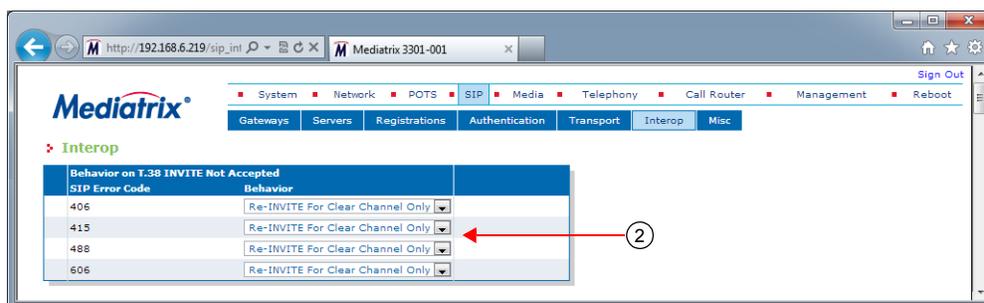
Behavior on T.38 INVITE Not Accepted

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 119: 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 241: 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

This section describes the SIP interoperability parameters of the Mediatrx 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 Mediatrix 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 242: 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 120: 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 243: 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 Mediatrix unit when answering a SIP OPTIONS request in the *OPTIONS Method Support* drop-down menu.

Table 244: OPTIONS Method Support Parameters

Parameter	Description
None	The Mediatrix unit responds with an error 405 Method not allowed.
AlwaysOK	The Mediatrix 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 OPTIONS on no usable endpoints* drop-down menu.

Table 245: 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 <i>OPTIONS Method Support</i> drop-down menu (see Step 10).
Disable	The SIP OPTIONS requests are answered as configured in the <i>OPTIONS Method Support</i> 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 155](#)
 - ISDN BRI interface: [“BRI Configuration” on page 167](#)
 - R2 PRI interface: [“R2 Channel Associated Signaling” on page 194](#)
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 287](#)).

6. Set the *Behavior On Machine Detection* drop-down menu with the SIP device's behaviour when a machine (fax or modem) is detected during a call.

Table 246: 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 that 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 Mediatrix 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 247: 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.
Ignore Uri Parameters	Matches the username and the host port part of the contact's SIP URI. All URI parameters are ignored.
Ignore URI and Port Parameters	Matches the username part of the contact's SIP URI. ALL URI and host port 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 Mediatrix 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 *Apply* if you do not need to set other parameters.

SDP Interop

This section describes the SDP interoperability parameters of the Mediatrix 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 248: 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 <i>Telephony > CODECS</i> page – by clicking the Edit button of each codec and looking in the <i>Voice Priority</i> and <i>Data Priority</i> 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 <i>Telephony > CODECS</i> page – by clicking the Edit button of each codec and looking in the <i>Voice Priority</i> and <i>Data Priority</i> 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 121: SDP Interop Section



2. Select whether or not the Mediatrix 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 249: Offer/Answer Model Parameters

Parameter	Description
Disable	<p>The peer can freely:</p> <ul style="list-style-type: none"> • Send back a brand new list of codecs or add new ones to the offered list. • Add new media lines. <p>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.</p>

Table 249: Offer/Answer Model Parameters

Parameter	Description
Enable	The following guidelines from the Offer-Answer Model must be strictly followed. An answer must: <ul style="list-style-type: none"> • Include at least one codec from the list that the Mediatrix 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 Mediatrix 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 250: Less Media Announcements Parameters

Parameter	Description
Disable	The Mediatrix unit rejects the response with less media announcements than in the offer.
Enable	The Mediatrix 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 Mediatrix 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 251: 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 Mediatrix 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 252: 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 Mediatrrix unit when answering a request offering more than one active media in the *Allow Multiple Active Media in Answer* drop-down menu.

Figure 122: 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 253: “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'.
recvonly	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 289](#) for more details).

8. Set the *Codec vs Bearer Capabilities Mapping Preferred Codec Choice* drop-down menu with the behaviour of the *Codec vs. Bearer Capabilities Mapping* table.

This modifies the selection of the preferred codec in the incoming SDP. This parameter is available only on ISDN interfaces.

The *Codec vs. Bearer Capabilities Mapping* table parameters are located in the *Telephony > CODECS > CODEC vs. Bearer Capabilities Mapping* section. See [“Codec vs. Bearer Capabilities Mapping” on page 188](#) for more details.

Table 254: *Codec vs Bearer Capabilities Mapping Preferred Codec Choice* Parameters

Parameter	Description
First Codec	The first valid codec in the incoming SDP is considered the preferred one and is used when looking up the <i>Codec vs. Bearer Capabilities Mapping</i> table.
Prioritize Clear Channel	When a clear channel codec is in the incoming SDP, it is always considered as the preferred one, no matter where it stands in the codec list, and is used when looking up the <i>Codec vs. Bearer Capabilities Mapping</i> table.

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

 **Note:** If you are experiencing media negotiation problems (because the Mediatrix 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 interoperability parameters of the Mediatrix 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 123: 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 276).

The following values are available:

Table 255: 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 <i>Management > Certificates</i> page (“ Chapter 49 - Certificates Management ” on page 501). 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 <i>Host Name</i> .
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 interoperability parameters of the Mediatrix unit .

► To set the Misc interop parameters:

1. In the *Misc Interop* section of the *Interop* page, select whether or not the Mediatrix 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 Mediatrix 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 Mediatrix unit sets the call property “type of number” to **international** if the user name has the prefix '+’.

Figure 124: 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 256: 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 257: 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 258: Escape Format Parameters

Parameter	Description
Lower Hexadecimal	Escaped characters are displayed in a lowercase hexadecimal format.
Upper Hexadecimal	Escaped characters are displayed in an uppercase hexadecimal 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 Mediatrix 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 Mediatrix 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 432](#) 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 385](#) for more details).

Max-Forwards Header

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 Mediatrrix unit allows you to define various direction attributes pertaining to the media stream.

When Putting a Call on Hold

The Mediatrrix 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 259: Direction Attributes

Parameter	Description
inactive	The stream is put on hold by marking it as <i>inactive</i> . 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 <i>sendonly</i> . This method allows the Mediatrrix 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 260: Direction Attributes Values

Value	Meaning
100	inactive
200	sendonly

This configuration has no effect if the `interopSdpDirectionAttributeEnable` variable is set to **disable** (see “[Direction Attribute](#)” on page 289 for more details).

Direction Attribute

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 261: SDP Direction Attribute

Parameter	Description
disable	No direction attribute is present in the SDP sent by the Mediatrrix unit. The Mediatrrix 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 Mediatrrix 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 290. 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 262: 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 289](#) 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 263: SDP Detect Peer Direction Attribute Parameters

Parameter	Description
disable	The Mediatrix 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 264: 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 265: 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 266: On Hold SDP Connection Address Values

Value	Meaning
100	HoldAddress
200	MediaAddress

Answering a Hold Offer with the Direction Attribute “sendonly”

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 267: “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 <i>InteropOnHoldSdpConnectionAddress</i> variable (“On Hold SDP Connection Address” on page 290).
recvonly	If the stream is currently active or receive only, it is marked as <i>recvonly</i> 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 <i>InteropOnHoldSdpConnectionAddress</i> variable (“On Hold SDP Connection Address” on page 290). 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 268: “sendonly” Direction Attribute

Value	Meaning
100	inactive

Table 268: “sendonly” Direction Attribute (Continued)

Value	Meaning
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 289 for more details).

SDP Direction Attribute Level

You can define the preferred location where the stream direction attribute is set.

The following parameters are supported:

Table 269: 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.
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 270: SDP Direction Attribute Level

Value	Meaning
100	MediaOrSessionLevel
200	MediaAndSessionLevel

Local Ring Behaviour on Provisional Response

You can set the Mediatrix 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 125: 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.

Figure 125: Local Ring Behaviour (Continued)

Parameter	Description
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 126: Local Ring Values

Value	Meaning
0	disable
1	LocalRingWhenNoEstablishedMediaStream
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 Mediatrix unit to be compatible with 3rd party vendor equipment.

The following parameters are supported:

Table 271: 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 272: 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 248 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

You can configure the Mediatrix 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 273: 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 127: DNS SRV Record Lock Values

Value	Meaning
0	disable
1	enable

Listening for Early RTP



Note: This feature applies to the following models:

- Mediatrix 3208 / 3216
- Mediatrix 3308 / 3316
- Mediatrix 3716 / 3731 / 3732 / 3741 / 3742
- Mediatrix 4100 Series
- Mediatrix LP Series
- Mediatrix C7 Series

You can set the Mediatrix 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 274: 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.



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 128: Early RTP Values

Value	Meaning
0	disable
1	enable

Resolve Route Header

The Mediatrix 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 275: 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 129: 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 276: 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 130: 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 277: 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: <ul style="list-style-type: none"> • * 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 131: Ignore Require Header Values

Value	Meaning
0	disable
1	enable

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 278: 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 132: 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 16 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 279: Macros Supported

Macro	Description
%version%	Application version.

Table 279: Macros Supported (Continued)

Macro	Description
%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 Mediatrix 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 280: 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 281: SIP INFO Values

Value	Meaning
200	Ok
415	UnsupportedMediaType

Keep Alive Option Format

You can configure the Keep Alive OPTION requests format.

The following parameters are supported:

Table 282: Keep Alive Option Format Parameters

Parameter	Description
ShortFrom	The unit sends the OPTION request with the standard format with only the unit's IP address in the from header. This is the default.
FullFrom	The unit sends the OPTION request with the standard format with the first registered username and IP address in the from header.



Note: The SipEp service must be restarted to apply a new username to the Keep Alive.

► **To set the keep alive option format:**

1. In the *sipEpMIB*, locate the *InteropGroup* folder.
2. Set the `InteropKeepAliveOptionFormat` variable with the proper value.

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

```
sipEp.InteropKeepAliveOptionFormat="value"
```

where *Value* may be as follows:

Figure 133: Keep Alive Option Format Values

Value	Meaning
100	ShortFrom
200	FullFrom

Unsupported Content-Type

You can define the behaviour of the Mediatrix unit upon reception of a SIP packet containing multiple unsupported Content-Type in the payload.

The following parameters are supported:

Table 283: 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 284: Unsupported Content-Type Values

Value	Meaning
100	Reject
200	Allow
300	Ignore

CHAPTER

32

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
- ▶ SIP 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 271 for more details.



Note: The Penalty Box feature is disabled when a gateway of type "endpoint" is configured in the gateway.

Penalty Box vs Transport Types

Media5 recommends to use this feature with care when supporting multiple transports (see “[Chapter 30 - SIP Transport Parameters](#)” on page 271 for more details) or you may experience unwanted behaviours.

When the Mediatrix 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 Mediatrix 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 Mediatrix unit and there are no more options to try after this host.

Let’s say for instance that the Mediatrix 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

Mediatrix 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 Mediatrix 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 Mediatrix 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 Mediatrix 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 Mediatrix 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 Mediatrix 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 134: 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

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
408: Request timeout	482: Loop Detected	513: Message Too Large
410: Gone	483: Too many hops	600: Busy everywhere
413: Request Entity too long	484: Address incomplete	603: Decline
		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 135: SIP To Cause Error Mapping Section

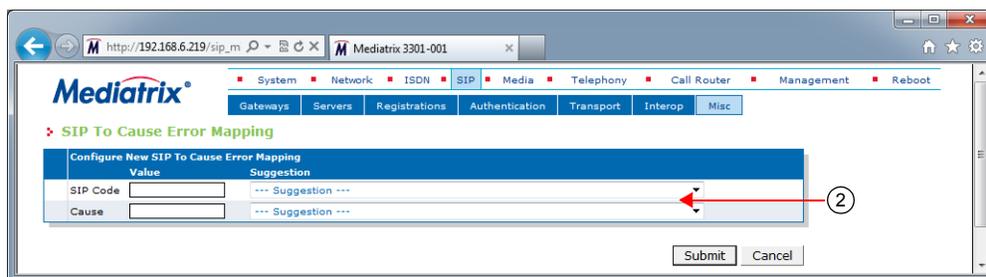


This brings you to the *Configure New SIP To Cause Error Mapping* panel.

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 136: 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 305](#) 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 285 lists the default mappings as per RFC 3398.

Table 285: 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 285: 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 137: 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 138: 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 307 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 286 lists the default mappings as per RFC 3398.

Table 286: 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 286: 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 Mediatrix 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 139: Reason Header Section



Table 287: 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 entries 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 288: 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	<ul style="list-style-type: none"> • 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 Mediatrix 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 Mediatrix 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 140: PRACK Section



Table 289: PRACK User Agent Server Parameters

Parameter	Description
Unsupported	The option tag “100rel” is ignored if present in the <i>Supported</i> or <i>Required</i> 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 <i>Supported</i> or <i>Required</i> header of initial received INVITEs, provisional responses are sent reliably as per RFC 3262 by adding the option tag “100rel” to the <i>Require</i> 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 290: PRACK User Agent Client Parameters

Parameter	Description
Unsupported	The option tag “100rel” is not added in the <i>Supported</i> or <i>Required</i> header of sent INVITEs as per RFC 3261. If the provisional response contains a <i>Require</i> 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 <i>Supported</i> header of sent initial INVITEs as per RFC 3262. If the received provisional response contains a <i>Require</i> header field with the option tag “100rel”, the response is sent reliably using the PRACK method.

Table 290: PRACK User Agent Client Parameters (Continued)

Parameter	Description
Required	The option tag "100rel" is added to the <i>Require</i> header of sent initial INVITEs as per RFC 3262. If the received provisional response contains a <i>Require</i> 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 Mediatrix 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 291: 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 292: 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 141: Session Refresh Section



Disabling this service is not recommended since it will make 'dead' calls impossible to detect. See [“Background Information” on page 312](#) 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 293: 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 310](#)).

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. REPLACER

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 Mediatix 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 Mediatix unit might not be followed. This has the advantageous effect of establishing the call even if the two endpoints have conflicting values. The Mediatix 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 Mediatix 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 Mediatix 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:

- 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, it overrides the home domain proxy (*Proxy Host* field of the *Servers* sub-page – *SIP Default Servers* section “[SIP Servers Configuration](#)” on page 248) in the address of record and the request-URI. When it overrides the home domain proxy in the request-URI, the request-URI also contains a *maddr* parameter with the resolved home domain proxy to make sure the requests are routable.

Figure 142: SIP Gateway Configuration Section

Gateway Configuration	
Gateway Name	SIP Domain Override
default	<input type="text"/>
defaultV6	<input type="text"/>

- 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 143: SIP Transfer Section



Table 294: 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 155](#) 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 *Method* 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 243](#).

Figure 144: Diversion Configuration Section



Table 295: Diversion Parameters

Parameter	Description
None	No diversion information is sent in SIP messages.
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 145: DNS Configuration Section



Table 296: 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 Mediatrix 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 Mediatrix 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 146: Event Handling Parameters

Event Handling Gateway Name	Reboot	CheckSync
gateway1	Rejected	Rejected
gateway2	Rejected	Rejected
gateway3	Rejected	Rejected
gateway4	Rejected	Rejected

Table 297: Reboot Event Handling Parameters

Parameter	Description
Rejected	The "reboot" notification is rejected on reception.
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 298: 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 Mediatrix 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 147: Messaging Subscription Parameters



Table 299: 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.

Advice of Charge Configuration

The Mediatrix unit allows you to configure the Advice Of Charge (AOC) to send the current charge (D)uring a call via an AOC-D message or the total charge at the (E)nd of call via an AOC-E message.



Note: The AOC feature is not available LP/4100/C7 Series models.

► **To set the AOC parameters:**

1. In the *AOC* section of the *Misc* page, set the *AOC-D Support* and *AOC-E Support* parameters for each available gateway to define if and how AOC-D and AOC-E messages are sent.

Figure 148: AOC-D and AOC-E Configuration Parameters



Table 300: AOC-D and AOC-E Configuration Parameters

Parameter	Description
Disabled	No AOC information is sent. Received AOC information is discarded.
Transparent	AOC information is forwarded to the peer interface if AOC messages are received from the network.

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

Additional DNS Parameters

This section describes configuration that is available only in the MIB parameters of the Mediatrrix 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

DNS Failure Concealment

You can configure the way failed DNS queries are handled.

Table 301: DNS Failure Concealment Parameters

Parameter	Description
None	When a DNS query times out or returns an error, the SIP transaction fails.
OnNoResolution	When a DNS query times out or returns an error, the result from the last successful query for the same FQDN is used.

▶ **To set the DNS failure concealment parameter:**

1. In the *sipMIB*, locate the *DnsGroup* folder.
2. Set the DNS failure concealment configuration in the `DnsFailureConcealment` variable.

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

```
sip.DnsFailureConcealment="value"
```

where *Value* may be as follows:

Table 302: DNS Failure Concealment Values

Value	Meaning
100	None
300	OnNoResolution



Note: This variable applies only to gateway type 'Endpoint'; it has no effect on Trunk gateways, and therefore, DNS failure concealment is always considered to be "none".

Media Parameters

Page Left Intentionally Blank

CHAPTER

33

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.

Codec Descriptions

The Mediatrix 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 Mediatrix 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 303: 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 Mediatrix C7 Series and 4102S models.

G.711 A-Law and μ -Law

The audio data is encoded as 8 bits per sample, after logarithmic scaling.

Table 304: 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 328 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 328 for more details.
Comfort noise	Uses custom comfort noise as defined in <i>RFC 3389</i> .
Available for voice	Yes
Available for fax	Yes
Available for modem	Yes

G.723.1

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 305: 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 330 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

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 306: 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 331 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 328 for more details.
Comfort noise	Uses custom comfort noise as defined in <i>RFC 3389</i> .
Payload type	Configurable as per “G.726 Codecs Parameters” on page 331 .
Available for voice	Yes
Available for fax	Yes (32 kbps and 40 kbps)
Available for modem	Yes (32 kbps and 40 kbps)

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 Mediatrix unit supports G.729A and G.729AB for encoding and G.729, G.729A and G.729AB for decoding.

Table 307: 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 333 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 333 for more details.
Payload type	18
Available for voice	Yes
Available for fax	No
Available for modem	No

Clear Mode

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 308: 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 334 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 334 .
Available for voice	Yes
Available for fax	Yes
Available for modem	Yes

Clear Channel

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 behaves like the Clear Mode codec (as defined in RFC 4040) but it uses “X-CLEAR-CHANNEL” mime type instead of the “CLEAR MODE” mime type during codec negotiation.

This codec always uses the RTP transport.

Table 309: 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 335 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 335 .
Available for voice	Yes
Available for fax	Yes
Available for modem	Yes

X-CCD Clear Channel

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 X-CCD behaves like the Clear Mode codec (as defined in RFC 4040) but it uses the “X-CCD” mime type instead of the “CLEARMODE” mime type during codec negotiation.

This codec always uses the RTP transport.

Table 310: 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 337 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 337 .
Available for voice	Yes
Available for fax	Yes
Available for modem	Yes

T.38

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 311: T.38 Features

Feature	Description
Packetization time	N/A

Table 311: T.38 Features (Continued)

Feature	Description
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 34 - Security” on page 345 for more details.

Codec Parameters

The *Codec* section allows you to enable or disable the codecs of the Mediatrix unit, as well as access the codec-specific parameters.

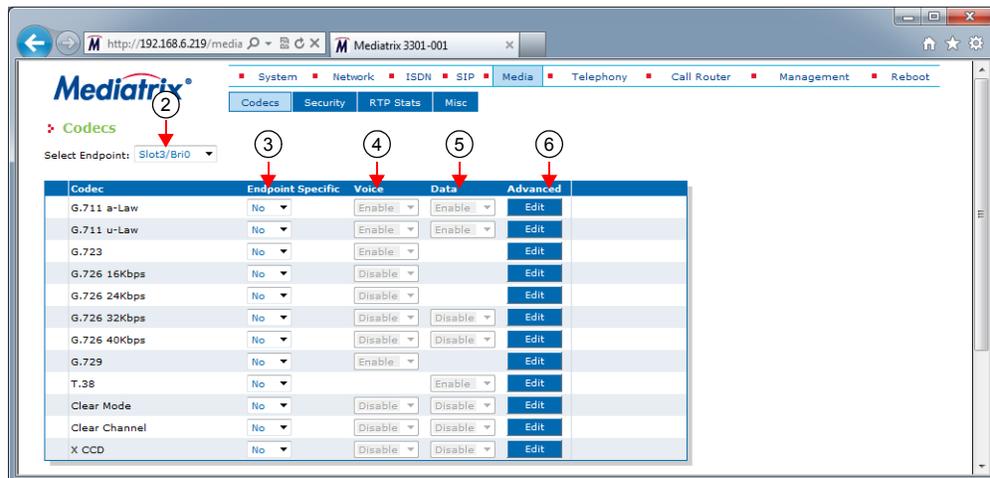
You can use two types of configuration:

- ▶ Default configurations that apply to all the endpoints of the Mediatrix unit.
- ▶ Specific configurations that override the default configurations. You can define specific configurations for each endpoint in your Mediatrix unit.

▶ **To enable or disable the codecs:**

1. In the web interface, click the *Telephony* link, then the *CODECS* sub-link.

Figure 149: 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 Mediatrix unit. The number of interfaces available vary depending on the Mediatrix 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.

Codec vs. Bearer Capabilities Mapping

The *Codec vs. Bearer Capabilities Mapping* section allows you to select the codec to prioritize or select in the outgoing INVITE when the incoming SETUP's ITC (Information Transfer Capability) matches the configured one. On the other hand, you can also select the ITC value to set in the outgoing SETUP's bearer capabilities when the incoming INVITE's codec matches the configured one.

Depending on the mapping type, a codec is prioritized or selected. Prioritized means it is the first in the list of offered codecs when initiating a call on the IP side and Selected means it is the only codec offered.

This parameter is available only on ISDN interfaces.

You can define up to three mappings.



Note: You can also modify the selection of the preferred codec in the incoming SDP by using the the interop parameter *Codec vs Bearer Capabilities Mapping Preferred Codec Choice* in the *SIP > Interop > SDP* section. See "[SDP Interop](#)" on page 282 for more details.

► To set the codec vs. bearer capabilities mapping

1. Define if the outgoing codec's priority should reflect the incoming ITC and vice versa in the *Enable* column drop-down menu.

Figure 150: Codec vs. Bearer Capabilities Mapping Section

Index	Enable	CODEC	Mapping Type	ITC
1	Disable	G.729	Prioritize	speech
2	Disable	G.729	Prioritize	speech
3	Disable	G.729	Prioritize	speech

Table 312: Outgoing Codec Priority

Parameter	Description
Disable	The mapping is not applied: <ul style="list-style-type: none"> • The codec's order in the outgoing INVITE follows the codec priority. • The ITC in the outgoing SETUP is the default one (3.1 kHz) unless a mapping in the Call Routing table modifies it.

Table 312: Outgoing Codec Priority (Continued)

Parameter	Description
Enable	<p>If the ITC value in the incoming SETUP matches the value of the corresponding <i>ITC</i> drop-down menu, the first codec in the outgoing INVITE is the one set in the <i>CODEC</i> drop-down menu.</p> <p>If the first codec in the incoming INVITE matches the value set in the <i>CODEC</i> drop-down menu, the ITC value in the outgoing SETUP is the one set in the <i>ITC</i> drop-down menu.</p>

2. Select a codec in the *CODEC* column drop-down menu.
 This is the codec to be prioritized or selected in an outgoing INVITE when the incoming SETUP's ITC matches the value set in the corresponding *ITC* drop-down menu. This codec is also checked against an incoming INVITE's priority codec. If it matches, then the outgoing SETUP's ITC is set to the value in the corresponding *ITC* drop-down menu.
 See Step 3 for a description of prioritization versus selection of a codec.
3. Set the mapping type of the codec in the *Mapping Type* drop-down value.

Table 313: Codec Mapping Type

Parameter	Description
Prioritize	The codec is set on top of the list in an outgoing INVITE when the incoming SETUP's ITC matches the value set in the corresponding <i>ITC</i> drop-down menu.
Select	The codec is the only one offered in an outgoing INVITE when the incoming SETUP's ITC matches the value set in the corresponding <i>ITC</i> drop-down menu.

4. Select an ITC value in the *ITC* column drop-down menu.
 This is the ITC value to be set in the outgoing SETUP when the incoming INVITE's priority codec matches the value of the corresponding *CODEC* drop-down menu. This value is also checked against an incoming SETUP's bearer capabilities. If it matches, then the outgoing INVITE's prioritized or selected codec is set to the value of the corresponding *CODEC* drop-down menu.

Table 314: Information Transfer Capability Values

Value	Description
speech	Voice terminals (telephones).
unrestricted	Unrestricted digital information (64 kbps).
3.1Khz	Transparent 3.1 kHz audio channel.

For an incoming ISDN call using UDI (Unrestricted Digital), the *Codec vs Bearer Capabilities Mapping* entries with the ITC set to **Unrestricted** is used only if the codec is Clear Mode, Clear Channel, XCCD, G.711 a-law or G.711 u-law. G.711 a-law and G.711 u-law are also used only if they match the ISDN port *Preferred Encoding Scheme* value (see "[PRI Configuration](#)" on page 155 and "[BRI Configuration](#)" on page 167 for more details).

See Step 3 for a description of prioritization versus selection of a codec.

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

Generic Voice Activity Detection (VAD)

VAD defines how the Mediatrrix 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 151: 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 315: 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

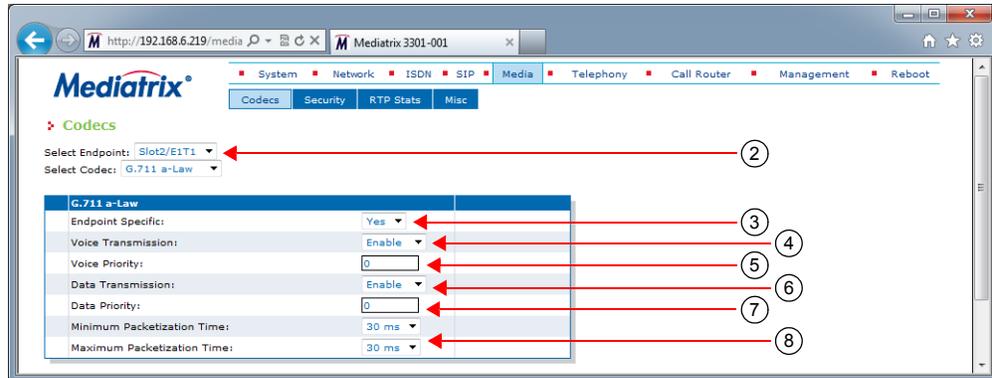
These sections use the same parameters, so only one of them is described below.

► 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 Mediatrrix unit. The number of interfaces available vary depending on the Mediatrrix unit model you have.

Figure 152: 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 Mediatrix 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 Mediatrix 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.

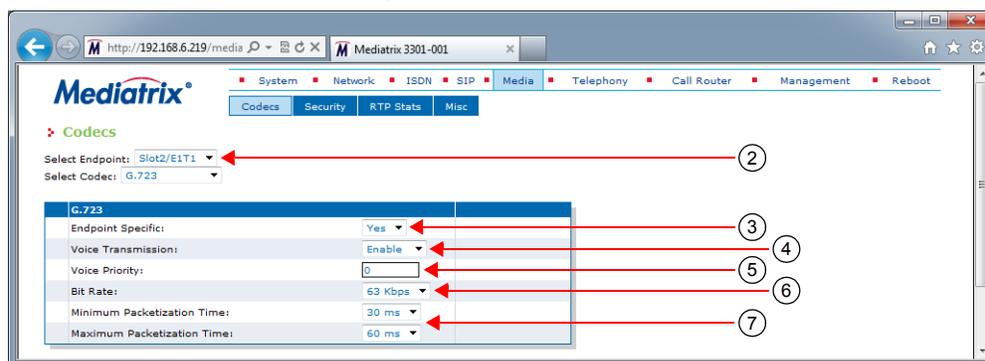
Note that the G.723 codec is not available on the Mediatrix C7 Series and 4102S models.

► 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 Mediatrix unit. The number of interfaces available vary depending on the Mediatrix unit model you have.

Figure 153: 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 Mediatrix 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

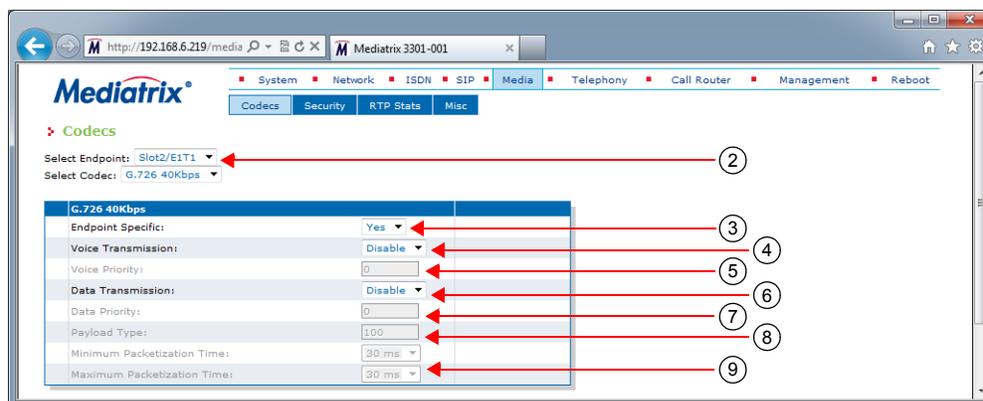
These sections offer almost the same parameters, except that you cannot use the G.726 16 Kbps and G.726 24 Kbps codecs for fax transmission.

▶ 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 Mediatrrix unit. The number of interfaces available vary depending on the Mediatrrix unit model you have.

Figure 154: 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 Mediatrix 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 Mediatrix 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 316: 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

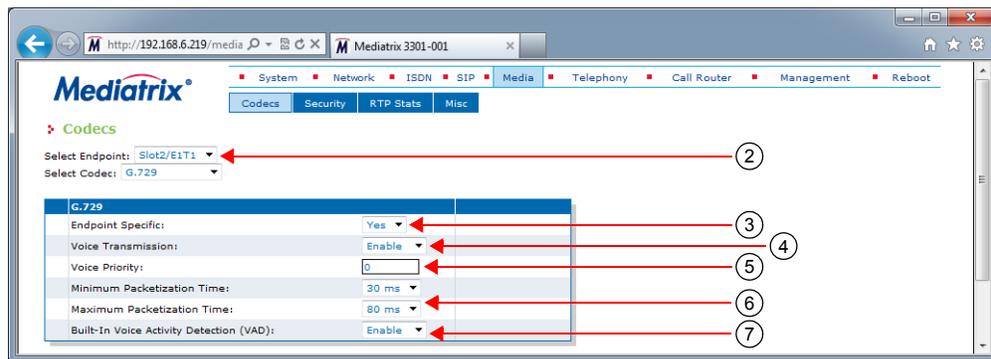
The following are the G.729 codec parameters you can set.

► **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 Mediatrix unit. The number of interfaces available vary depending on the Mediatrix unit model you have.

Figure 155: 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 Mediatrix 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 317: 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 Mediatrrix 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

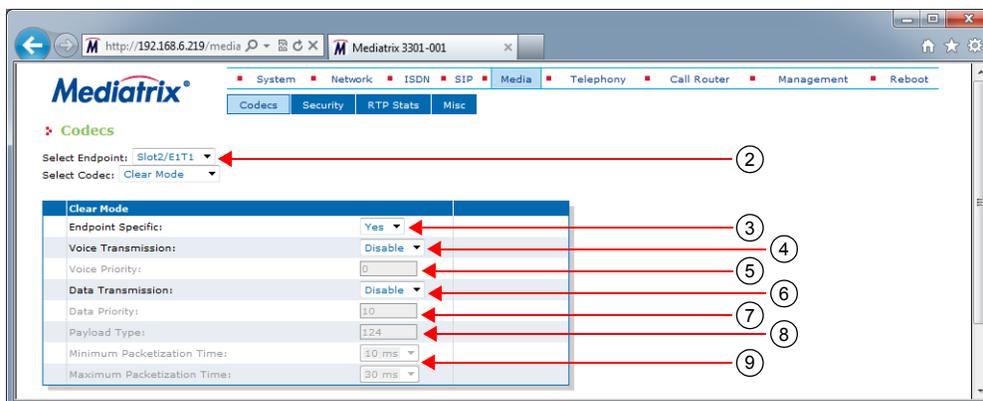
The following are the Clear Mode codec parameters you can set.

► **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 Mediatrrix unit. The number of interfaces available vary depending on the Mediatrrix unit model you have.

Figure 156: 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 Mediatrix 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 Mediatrix 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

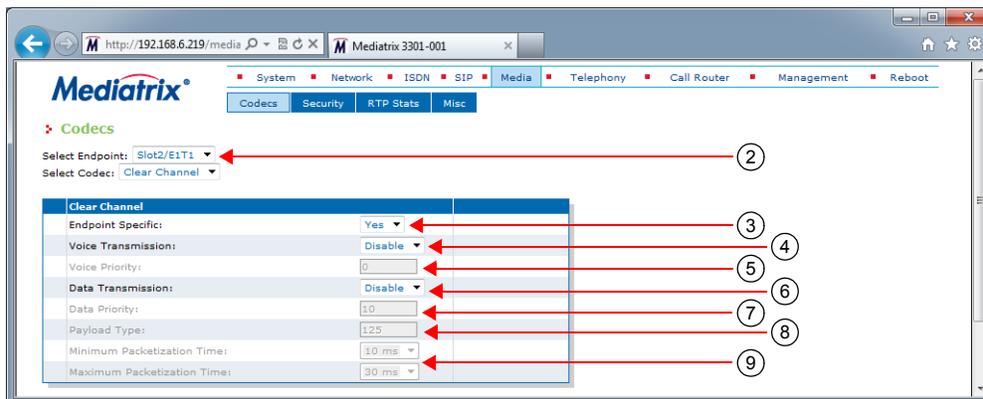
The following are the Clear Channel codec parameters you can set.

► **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 Mediatrix unit. The number of interfaces available vary depending on the Mediatrix unit model you have.

Figure 157: 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 Mediatrix 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 Mediatrix 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

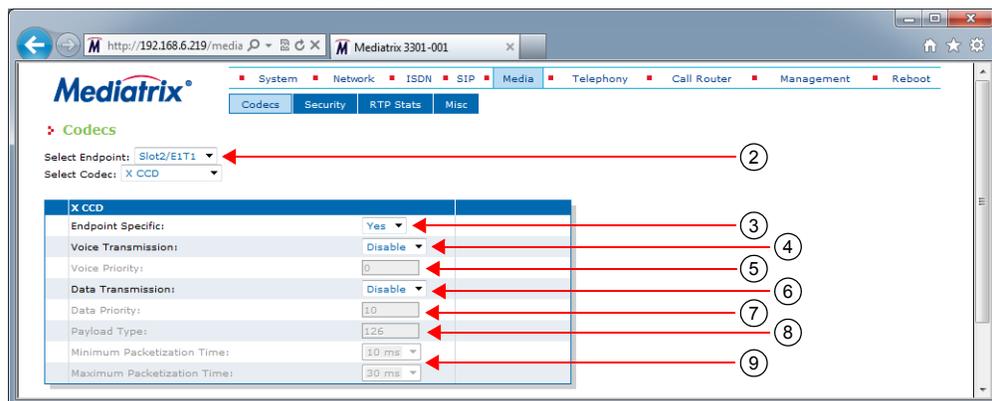
The following are the X-CCD Clear Channel codec parameters you can set.

► 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 Mediatrix unit. The number of interfaces available vary depending on the Mediatrix unit model you have.

Figure 158: 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 Mediatrix 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 Mediatrix 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 Mediatrix 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:

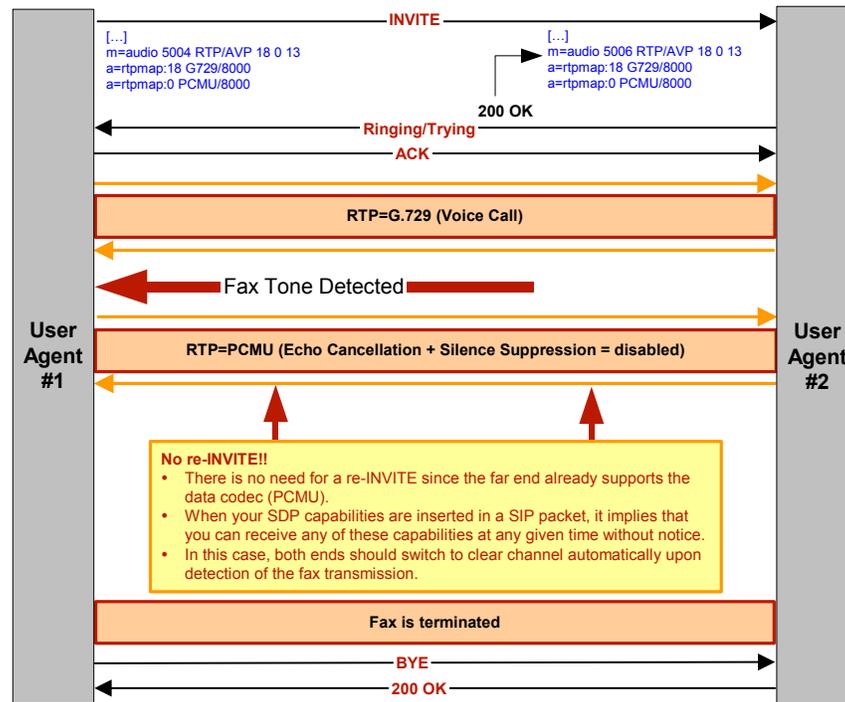
1. The fax codec may be re-negotiated by using a re-INVITE.
2. The goal of the re-INVITE is to allow both user agents to agree on a fax codec, which is either:
 - a. Clear channel (G.711 or G.726) without Echo Cancellation nor Silence Suppression (automatically disabled).
 - b. T.38.
3. Upon fax termination, if the call is not BYE, the previous voice codec is recovered with another re-INVITE.

All endpoints of the Mediatrix 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 Mediatrix unit can send faxes in clear channel. The following is a clear channel fax call flow:

Figure 159: Clear Channel Fax Call Flow



DSP Limitation

The Mediatrix 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 Mediatrix 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 Mediatrix 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 Mediatrix 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 Mediatrix unit opens the T.38 channel only after receiving the “200 OK” message from the peer. This means that the Mediatrix 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 Mediatrix 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: Media5 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.

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 Mediatrix unit uses an internal order for codecs with the same priority.



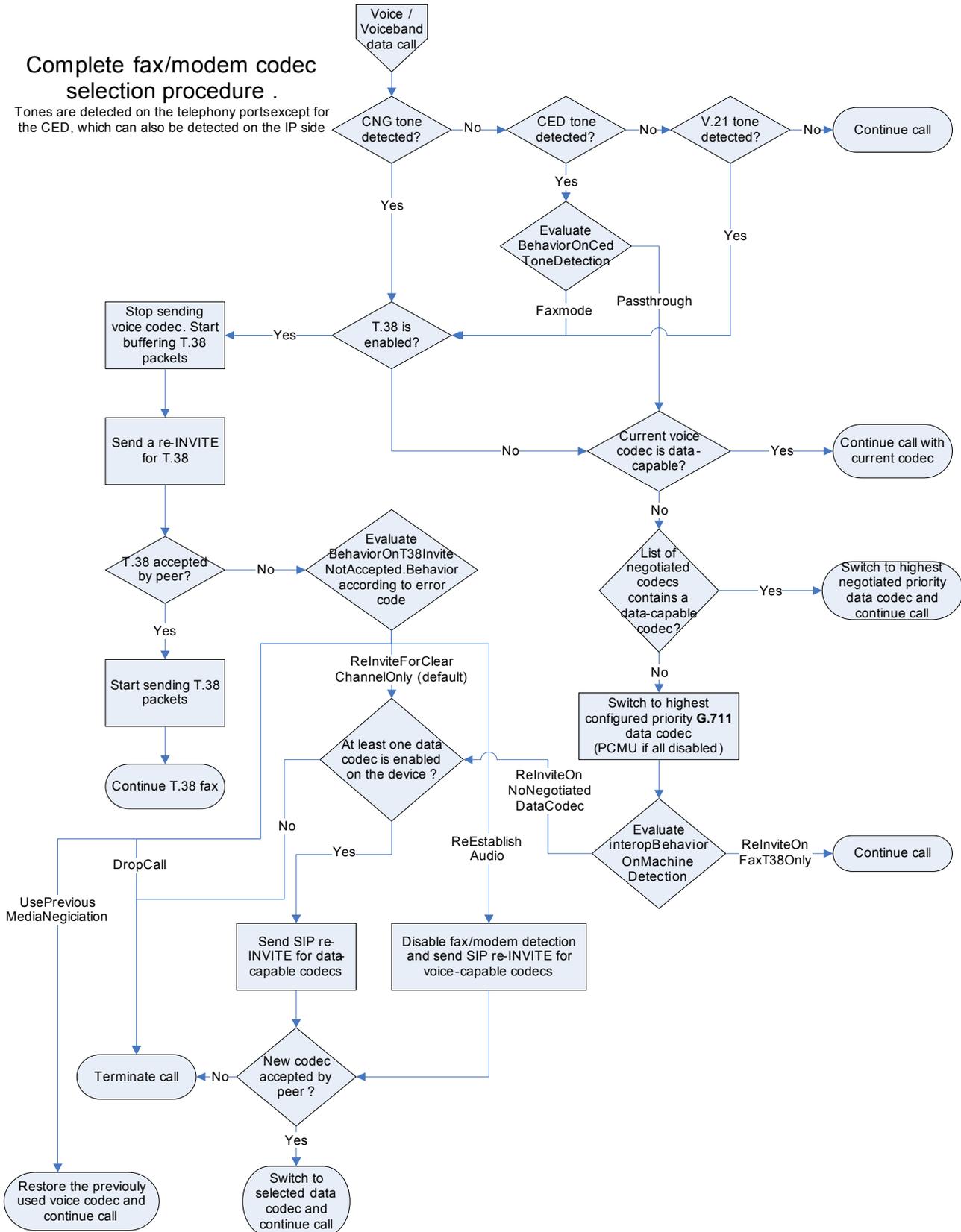
Note: Currently, the only T.38 priority accepted is **10**. Priority between 1 and 9 is refused.

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 Mediatrix 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 Mediatrix 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 Mediatrix unit follows a procedure when selecting data codec. This procedure is the default behaviour of the Mediatrix unit. Some interop variables may modify this procedure. Tones are detected on the analog ports only.

Figure 162: Data Codec Selection Procedure



CHAPTER

34

Security

This chapter describes how to properly configure the security parameters of the Mediatrix unit.

Introduction

You can define security features on the Mediatrix unit. This section applies to media security parameters. Applying security on the Mediatrix unit involves several steps:

- ▶ Properly set the time on the Mediatrix unit by configuring a valid SNTP server ([“SNTP Configuration” on page 57](#)) and time zone ([“Time Configuration” on page 58](#)).
- ▶ Transfer a valid CA certificate into the Mediatrix unit ([“Chapter 49 - Certificates Management” on page 501](#)).
- ▶ Use secure signalling by enabling the TLS transport protocol ([“Chapter 30 - SIP Transport Parameters” on page 271](#)).



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 Mediatrix unit's overall performance as SRTP requires CPU power. The more lines use SRTP, the more overall performance is affected. This is especially true with the Mediatrix 4116, LP16, 4124 and LP24 models. This could mean that a user picking up a telephone on these models may not have a dial tone due to lack of resources. See also [“DSP Limitation” on page 397](#) 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 365](#)).
 - 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 Mediatrix unit.

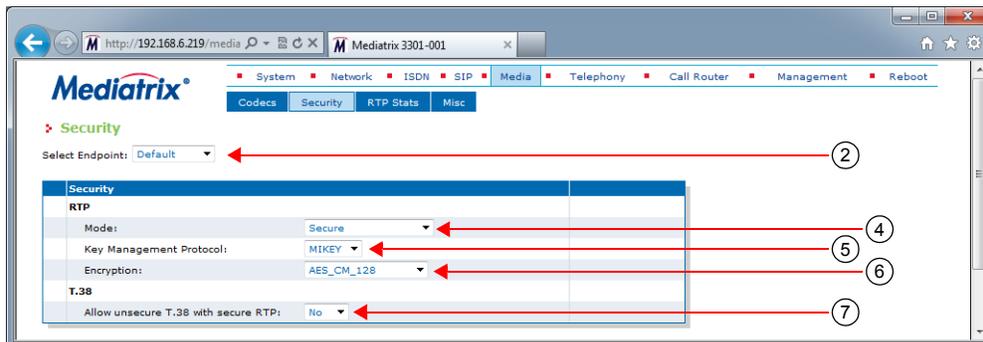
Since the SRTP encryption and authentication needs more processing, the number of calls that the Mediatrix unit can handle simultaneously may be reduced, depending of the codecs enabled. You could set the Mediatrix unit not to impact the number of simultaneous calls by enabling only G.711 codecs and disabling every other voice or data codec, even T.38.

The Mediatrix 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 163: 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 Mediatrix unit. The number of interfaces available vary depending on the Mediatrix 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 318: Default RTP Mode

Mode	Description
Unsecure	The Mediatrix unit supports only unsecure RTP. It rejects secure RTP offers it receives.
Secure	The Mediatrix unit supports only secure RTP. It rejects unsecure RTP offers it receives.
Secure with fallback	The Mediatrix 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 30 - SIP Transport Parameters” on page 271 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 Mediatrix 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 Mediatrix 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 Mediatrix 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 319: 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 320: 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 321: 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 Mediatrix 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 322: 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 *mipMIB*, set the `enforceSymmetricRtpEnable` variable with the proper behaviour.

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

```
mip.enforceSymmetricRtpEnable="value"
```

where *Value* may be as follows:

Figure 164: Symmetric RTP Values

Value	Meaning
0	disable
1	enable

CHAPTER
35

RTP Statistics Configuration

The Mediatrix 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

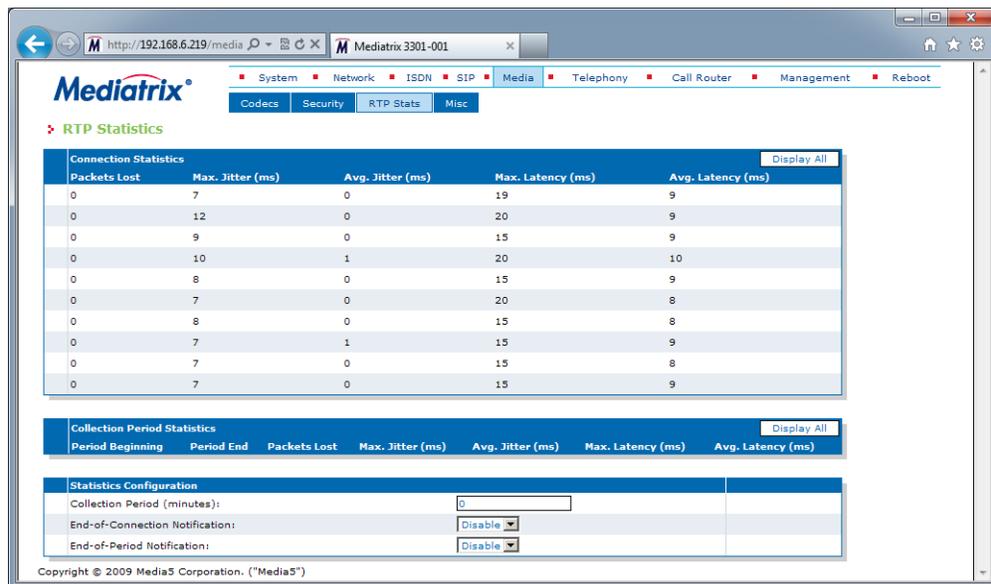
The Mediatrix unit collects two types of statistics:

- ▶ 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 165: Telephony – RTP Stats Web Page



The following table describes the statistics available.

Table 323: 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 323: 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 subtracting 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 323: 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.

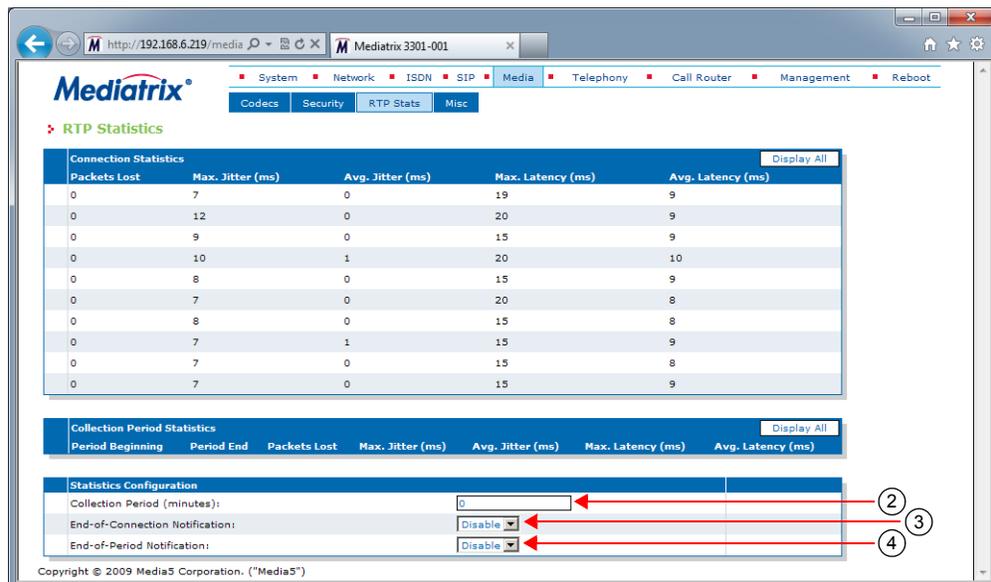
Statistics Configuration

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 35 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 166: 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 324: 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 325: 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 Mediatrix 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 Mediatrix unit keeps.

Table 326: 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 *mipMIB*, go to the *ChannelStatistics* table.
You can also use the following line in the CLI:
`get mipMIB.channelStatistics`

► **To reset channel statistics values to zero:**

1. In the *mipMIB*, set `ChannelStatistics.Reset` to *Reset* for the endpoint to reset.
You can also use the following line in the CLI:
`set mipMIB.channelStatistics.Reset=Reset`
2. In the *mipMIB*, 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 mipMIB.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
36

Miscellaneous Media Parameters

This chapter describes how to configure parameters that apply to all codecs.

- ▶ Jitter Buffer Configuration
- ▶ DTMF Transport Configuration
- ▶ Machine Detection Configuration
- ▶ Base Ports Configuration

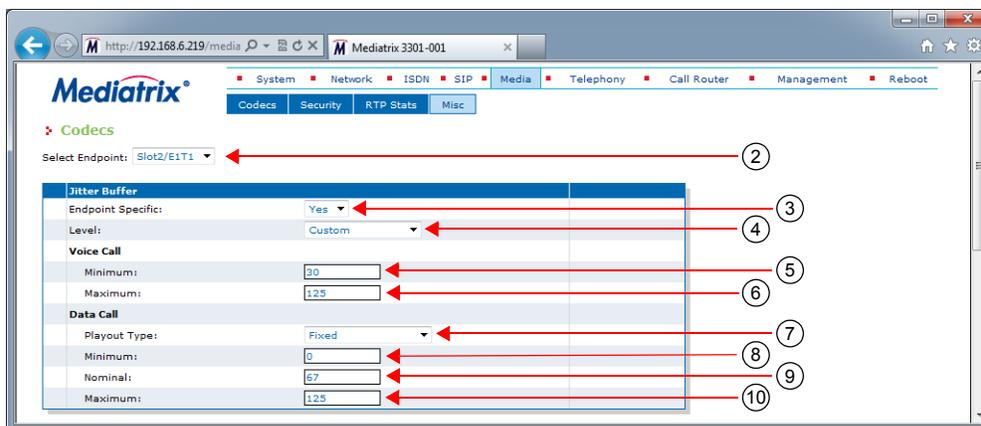
Jitter Buffer Configuration

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 167: 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 Mediatrix unit. The number of interfaces available vary depending on the Mediatrix 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 327: 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Minimum value: 70 ms • Maximum value: 135 ms
Custom	The jitter buffer uses the configuration of the <i>Minimum</i> and <i>Maximum</i> 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 Media5 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 357](#) 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 Media5 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: $30 + 4 \times 20 = 110$ 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 328: 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 <i>Nominal</i> 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 357](#) for more details.
11. Click *Submit* if you do not need to set other parameters.

About Changing Jitter Buffer Values

Media5 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 Mediatrix 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 329: 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 355).
Enable	The call is started in voiceband data mode.

▶ To start a call in voiceband data mode:

1. In the *telMIB*, 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 330: 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 Mediatrix 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 Mediatrix unit. The number of interfaces available vary depending on the Mediatrix 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 168: DTMF Transport Section



3. Select the DTMF transport type in the *Transport Method* drop-down menu. The following choices are available:

Table 331: 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 <i>draft-choudhuri-sip-info-digit-00</i> .
Signaling protocol Dependant	The signalling protocol has the control to select the DTMF transport mode. The SDP body includes both RFC 2833 and <i>draft-choudhuri-sip-info-digit-00</i> 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 332: DTMF Out-of-Band Transport Methods

Method	Description
draftChoudhuriSipInfoDigit00	Transmits DTMFs by using the method defined in <i>draft-choudhuri-sip-info-digit-00</i> . 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 Mediatrix unit receives and sends out-of-band DTMFs as per ITU Q.24. DTMFs supported are 0-9, A-D, *, #.

Table 332: DTMF Out-of-Band Transport Methods (Continued)

Method	Description
Info DTMF Relay	<p>Transmits DTMFs by using a custom method. This custom method requires no SDP negotiation and assumes that the other peer uses the same method.</p> <p>It uses a SIP INFO message with a content of type <i>application/dtmf-relay</i>. The body of the message contains the DTMF transmitted and the duration of the DTMF:</p> <pre>Signal= 1 Duration= 160</pre> <p>When transmitting, the duration is the one set in the <code>interopDtmfTransportDuration</code> variable (see “DTMF Transport over the SIP Protocol” on page 360).</p> <p>When receiving, the duration of the DTMF received is not used and the DTMF is played for 100 ms.</p> <p>DTMFs are transmitted one at a time.</p> <p>Available digits are “0123456789ABCD*#”. The Mediatix unit also supports the “;p” characters when receiving DTMFs.</p>

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 Mediatix 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 355](#), 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 Mediatix 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 Mediatix 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.

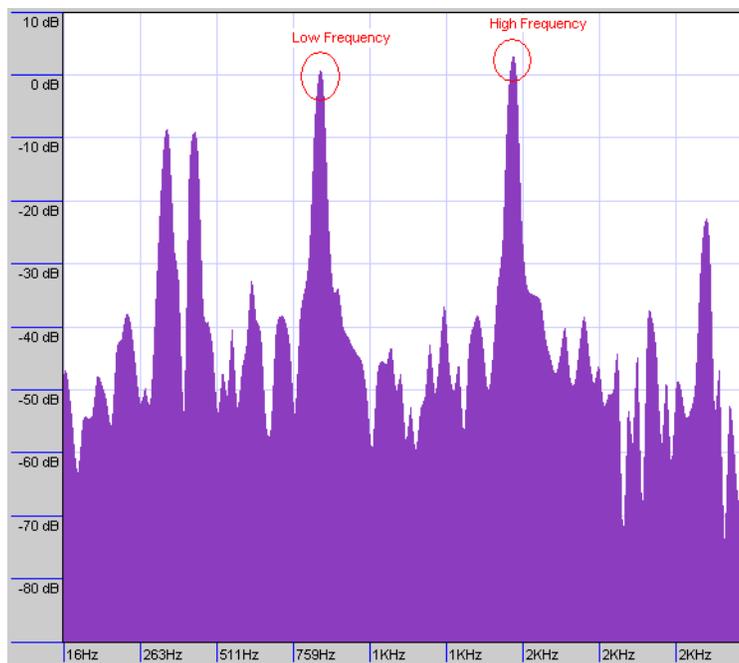
Table 333: DTMF Keypad Frequencies

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 169: DTMF Detection Example



► To configure the DTMF detection:

1. In the *telI/MIB*, 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:

```
Tellf.InteropDtmfDetection[InterfaceId=xxx].RiseTimeCriteria = "Value"
```

where *Value* may be as follows:

Table 334: DTMF Detection Values

Value	Method	
100	CheckSr	<p>Enables the Step Rise criteria and disables the Confirm DTMF SNR criteria.</p> <p>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.</p> <p>Disabling the Step Rise criteria may result in deteriorated talk-off performance, but increases the detection of malformed DTMF.</p>
200	ConfirmSnr	<p>Enable the Confirm DTMF SNR criteria and disable the Step Rise criteria.</p> <p>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.</p>

2. Set the `interopDtmfDetectionPositiveTwist` variable.

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

```
Tellf.InteropDtmfDetection[InterfaceId=xxx].PositiveTwist = "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.

3. Set the `interopDtmfDetectionNegativeTwist` variable.

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

```
Tellf.InteropDtmfDetection[InterfaceId=xxx].NegativeTwist = "Value"
```

Defines the value for the Negative Twist DTMF detection parameter.

When the low-group frequency of a DTMF is more powerful than the high-group frequency, the difference between the low-group frequency absolute power and the high-group frequency absolute power must be smaller than or equal to the value set in this parameter. 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.

4. Set the `interopDtmfDetectionMaxPowerThreshold` variable.

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

```
Tellf.InteropDtmfDetection[InterfaceId=xxx].MaxPowerThreshold = "Value"
```

The average power of a DTMF must be below the value set in this parameter to be no longer detected.

The value is expressed in dBm (relative to 1mW of power).

5. Set the `interopDtmfDetectionMinPowerThreshold` variable.

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

```
Tellf.InteropDtmfDetection[InterfaceId=xxx].MinPowerThreshold = "Value"
```

The average power of a DTMF must be above the value set in this parameter for at least 30ms to be detected.

The value is expressed in dBm (relative to 1mW of power).

6. Set the `interopDtmfDetectionBreakPowerThreshold` variable.

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

```
Tellf.InteropDtmfDetection[Interfaceld=xxx].BreakPowerThreshold = "Value"
```

When the average power of a DTMF falls below the value set in this parameter for at least 20ms, it is considered that the DTMF ended.

The value is expressed in dBm (relative to 1mW of power).

Using the Payload Type Found in the Answer

This section describes configuration that is available only in the MIB parameters of the Mediatix 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 Mediatix 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 355](#) for more details).

The following parameters are available:

Table 335: 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 `interopUsedDtmfPayloadTypeFoundInAnswer` variable with the proper behaviour.

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

```
sipEp.interopUsedDtmfPayloadTypeFoundInAnswer="Value"
```

where *Value* may be as follows:

Figure 170: 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 Mediatix 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 355](#) for more details).

► **To set the initial quantity of RTP packets:**

1. In the *mipMIB*, set the `InteropDtmfRtpInitialPacketQty` variable with the proper quantity. You can also use the following line in the CLI or a configuration script:
`mip.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 Mediatrix 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 Mediatrix unit. The number of interfaces available vary depending on the Mediatrix 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 171: 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 336: 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 337: CNG CED Detection Settings

Setting	Description
Enable	Upon recognition of the CED tone, the unit behaves as defined in the <i>Behavior on CED Tone Detection</i> parameter Step 6).

Table 337: CNG CED Detection Settings (Continued)

Setting	Description
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 338: 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 339: 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 *CED 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 Mediatrix 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 Mediatrix unit. The number of interfaces available vary depending on the Mediatrix 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 172: Base Ports Section

Base Ports	
RTP:	<input type="text" value="5004"/>
SRTP:	<input type="text" value="5004"/>
T.38:	<input type="text" value="5004"/>

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 34 - Security](#)” on page 345), 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.

Telephony Parameters

Page Left Intentionally Blank

CHAPTER

37

DTMF Maps Configuration

This chapter describes how to configure and use the DTMF maps of the Mediatix unit.

- ▶ 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 Mediatix 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 340: 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
9011 + up to 15 digits	International number

The solution to this problem is to load the Mediatix unit with a DTMF map that corresponds to the dial plan.

A Mediatrix 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 341: 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 372](#).

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 Mediatrix unit can make the call. A DTMF map for this could be:

```
[2-9]xxxxxT
```



Note: When making the actual call and dialing the number, the Mediatrix 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 372](#) 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 340 on page 369](#) outlined various call types one could make. All these possibilities could be covered in one DTMF map:

```
(0T|00T|[1-7]xxx|8xxxxxxx|#xxxxxxx|91xxxxxxxxxxx|9011x.T)
```

Validating a DTMF Map

The Mediatrix unit validates the DTMF map as you are entering it and it forbids any invalid value.

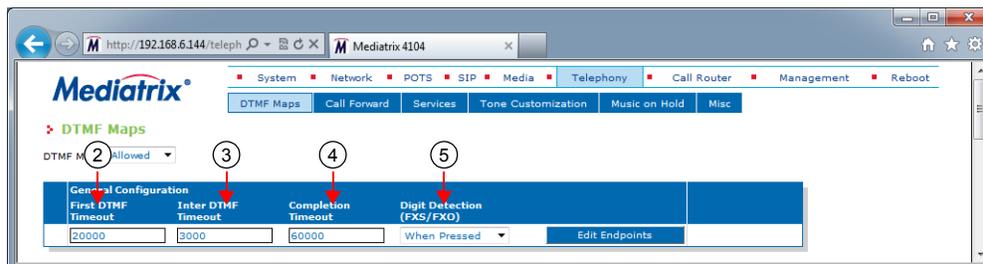
General DTMF Maps Parameters

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 173: 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 373 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 **3000** 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 373 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 373 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 342: 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 <i>First DTMF Timeout</i> , <i>Inter Digit Timeout</i> and <i>Completion Timeout</i> 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.

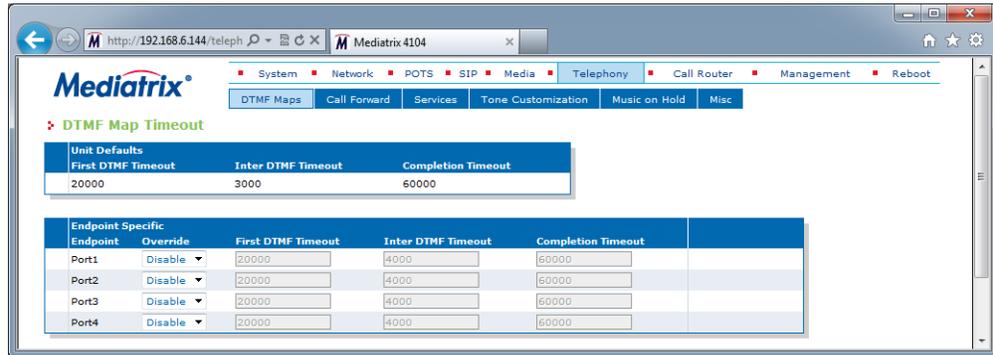
Configuring Timeouts per Endpoint

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 174: 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.

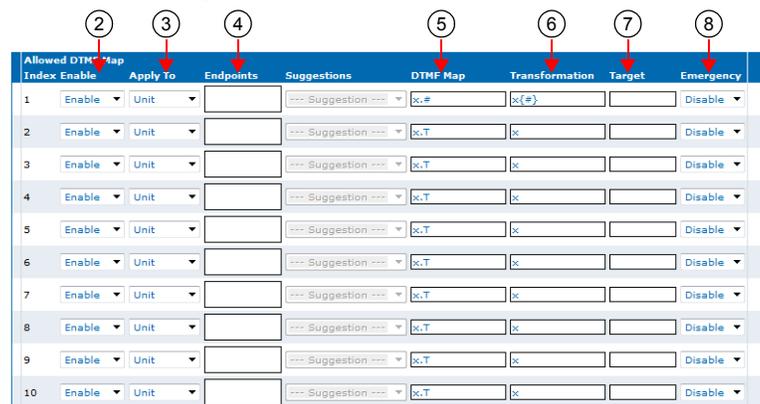
Allowed DTMF Maps

You can create/edit ten DTMF maps for the Mediatrix 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 175: Allowed DTMF Map Section



- Select the entity to which apply the allowed DTMF map in the *Apply to* column.

Table 343: 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 <i>Endpoint</i> column of the same row.

- 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.

- 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 369. A DTMF map string may have a maximum of 64 characters.

- 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 344: 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

- 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

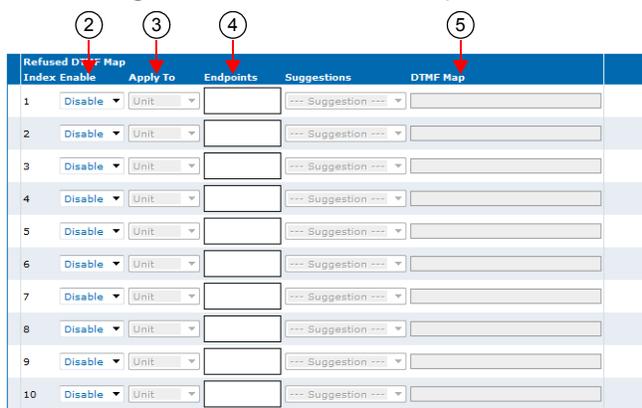
A refused DTMF map forbids to call specific numbers; for instance, you want to accept all 1-8xx numbers except 1-801. You can create/edit ten refused DTMF maps for the Mediatrix unit.

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 176: Refused DTMF Map Section



3. Select the entity to which apply the refused DTMF map in the *Apply to* column.

Table 345: 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 <i>Endpoint</i> 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 369](#). A DTMF map string may have a maximum of 64 characters.
6. Click *Submit* if you do not need to set other parameters.

CHAPTER

38

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 Mediatrix unit.
- ▶ Specific configurations that override the default configurations. You can define specific configurations for each endpoint in your Mediatrix unit.



Note: This web page is available only on the following models:

- Mediatrix 3208 / 3216
- Mediatrix 3308 / 3316
- Mediatrix 3716
- Mediatrix 3731
- Mediatrix 3732
- Mediatrix 3741
- Mediatrix 3742
- Mediatrix 4100 Series
- Mediatrix LP Series
- Mediatrix C7 Series

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.

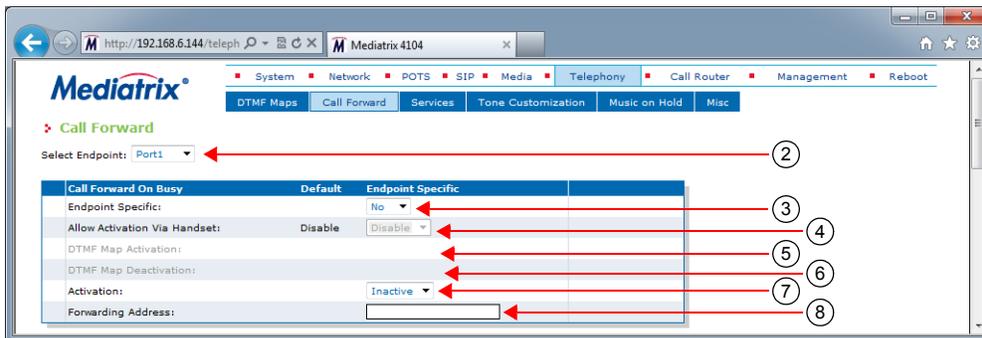
You can enable the Call Forward On Busy feature in two ways:

- ▶ 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 177: 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 Mediatrix 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 37 - DTMF Maps Configuration](#)” on page 369). 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 Mediatrix 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 37 - DTMF Maps Configuration](#)” on page 369). 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 Mediatrix 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 346: 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.

Table 346: Activation State (Continued)

State	Description
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 <i>Forwarding Address</i> 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 Mediatrix 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 178: 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 37 - DTMF Maps Configuration” on page 369](#)). 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 Mediatrix 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 37 - DTMF Maps Configuration” on page 369](#)). 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 Mediatrix 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 347: 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 <i>Forwarding Address</i> 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 Mediatrix 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 179: 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 37 - DTMF Maps Configuration](#)” on page 369). 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 Mediatrix 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 37 - DTMF Maps Configuration](#)” on page 369). 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 Mediatrix 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 348: 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 <i>Forwarding Address</i> 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

39

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 Mediatrix 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 Mediatrix unit.
- ▶ Specific configurations that override the default configurations. You can define specific configurations for each endpoint in your Mediatrix unit.

General Configuration

The *General Configuration* sub-section of the *Services Configuration* section allows you to define the Hook Flash Processing feature.

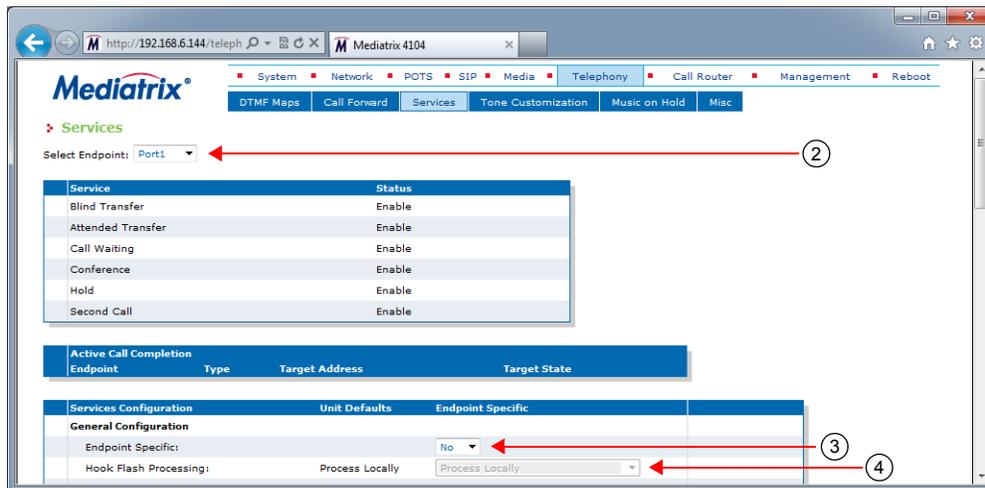


Note: Performing a flash hook and pressing the flash button means the same thing. However, not all telephone models have a flash button.

► To set general services parameters:

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

Figure 180: 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 Mediatrix unit. The number of interfaces available vary depending on the Mediatrix 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 349: 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 Mediatrix unit. The number of interfaces available vary depending on the Mediatrix 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 181: 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



Note: This section applies only to the following models:

- Mediatrix 3208 / 3216
- Mediatrix 3308 / 3316
- Mediatrix 3716
- Mediatrix 3731
- Mediatrix 3732
- Mediatrix 3741
- Mediatrix 3742
- Mediatrix 4100 Series
- Mediatrix LP Series
- Mediatrix C7 Series

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 Mediatrix unit. The number of interfaces available vary depending on the Mediatrix 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 182: Telephony – Call Completion Section

Call Completion	
Allow CCBS Activation Via Handset:	Disable ▾
CCBS DTMF Map Activation:	
Allow CCNR Activation Via Handset:	Disable ▾
CCNR DTMF Map Activation:	
DTMF Map Deactivation:	
Expiration Timeout:	180
Method:	Monitoring Only
Auto Reactivate:	Disable ▾
Auto Reactivate Delay:	30
Early-Media Behaviour:	None ▾
Polling Interval:	5

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 37 - DTMF Maps Configuration on page 369”](#)). 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 Mediatrix 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 37 - DTMF Maps Configuration on page 369”](#)). 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 Mediatrix 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 37 - DTMF Maps Configuration](#)” on page 369). 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 Mediatrix 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 350: Call Completion Method Parameters

Method	Description
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).

Media5 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 351: 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.



Note: The CCBS and CCNR cannot be started to complete a second call.

▶ **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



Note: This section applies only to the following models:

- Mediatrix 3208 / 3216
- Mediatrix 3308 / 3316
- Mediatrix 3716
- Mediatrix 3731
- Mediatrix 3732
- Mediatrix 3741
- Mediatrix 3742
- Mediatrix 4100 Series
- Mediatrix LP Series
- Mediatrix C7 Series

The Call Transfer service offers two ways to transfer calls:

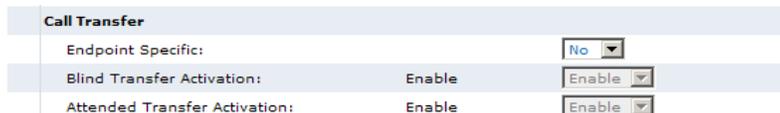
- ▶ Blind Transfer

► 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 Mediatrix 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 183: 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 403](#) and [“Second Call” on page 404](#).
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 403](#) and [“Second Call” on page 404](#).
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 314](#).

► 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.



Note: Attended call transfers can only be used to transfer a call already established. You cannot use the Attended Call Transfer for an incoming call. For example, in this case where C is the incoming call.

1. A calls B.
2. B answers the call
3. C calls B
4. B puts A on hold (Flash hook) and answers C
5. B hangs up the phone.

When B hangs up at step 5, A and C will not be connected. C will rather be released. B will ring and when B answers, B will be in communication with A.

Call Waiting



Note: This section applies only to the following models:

- Mediatrix 3208 / 3216
- Mediatrix 3308 / 3316
- Mediatrix 3716
- Mediatrix 3731
- Mediatrix 3732
- Mediatrix 3741
- Mediatrix 3742
- Mediatrix 4100 Series
- Mediatrix LP Series
- Mediatrix C7 Series

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 Mediatix 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 field is available only in the specific endpoints configuration.

Figure 184: Call Waiting Section

3. From the *Call Waiting Activation* drop-down menu, select **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 403.
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 37 - DTMF Maps Configuration](#)” on page 369). 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 Mediatix unit. You cannot have a different sequence for each endpoint.
5. In the *Activation DTMF Map* field, define the digits that users must dial to activate the Call Waiting service. Note that dialing this DTMF map does not have any effect unless the call waiting service’s status is ‘enabled’.
6. In the *Deactivation DTMF Map* field, define the digits that users must dial to deactivate the Call Waiting service. Note that dialing this DTMF map does not have any effect unless the call waiting service’s status is ‘enabled’.
7. Click *Apply* 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 2nd caller that the destination is currently busy in a call but was notified of this new incoming call.

Conference



Note: This section applies only to the following models:

- Mediatrix 3208 / 3216
- Mediatrix 3308 / 3316
- Mediatrix 3716
- Mediatrix 3731
- Mediatrix 3732
- Mediatrix 3741
- Mediatrix 3742
- Mediatrix 4100 Series
- Mediatrix LP Series
- Mediatrix C7 Series

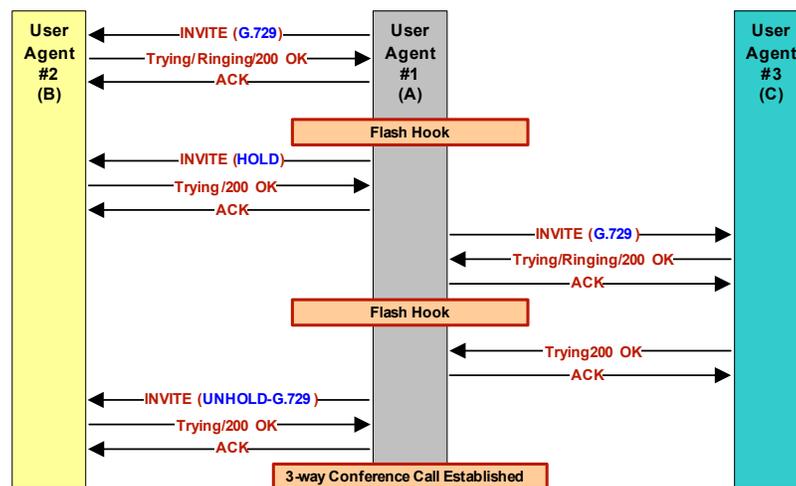
The Conference Call service allows a user to link two or more calls together to form a single conversation, called a conference.

- ▶ 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 403](#), [“Second Call” on page 404](#), and [“Call Transfer” on page 391](#).

The following is a conference call flow example:

Figure 185: Conference Call Flow



DSP Limitation

The Mediatrix 4108, 4116, 4124, C7, LP16 and LP24 models currently 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 Mediatrix 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 Mediatrix unit. The Mediatrix unit is limited to two conferences per DSP.

Please note that:

- ▶ One FXS line requires one channel.
- ▶ Each conference requires one additional channel
- ▶ The Mediatrix 4108/C7 has one DSP
- ▶ The Mediatrix 4116/LP16 have two DSPs
- ▶ The Mediatrix 4124/LP24 have three DSPs

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 Mediatrix 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 186: 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

This section describes configuration that is available only in the MIB parameters of the Mediatrix 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 Mediatrix 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 398](#) for more details).

You can use two types of configuration:

- ▶ Default configurations that apply to all the endpoints of the Mediatrix unit.
- ▶ Specific configurations that override the default configurations.

You can define specific configurations for each endpoint in your Mediatrix unit. For instance, you could enable a codec for all the endpoints of the Mediatrix 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 352: 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**.
- `GwSpecificConferenceServerUri` 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



Note: This section applies only to the following models:

- Mediatrix 3208 / 3216
- Mediatrix 3308 / 3316
- Mediatrix 3716
- Mediatrix 3731
- Mediatrix 3732
- Mediatrix 3741
- Mediatrix 3742
- Mediatrix 4100 Series
- Mediatrix LP Series
- Mediatrix C7 Series

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 Mediatrix 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 187: Delayed Hotline Section

Delayed Hotline		
Endpoint Specific:	Disable	No <input type="button" value="v"/>
Delayed Hotline Activation:	Disable	Disable <input type="button" value="v"/>
Delayed Hotline Condition:	FirstDtmTimeout	FirstDtmTimeout <input type="button" value="v"/>
Delayed Hotline Target:	<input type="text"/>	

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 188: Delayed Hotline Section



Table 353: Delayed Hotline Conditions

Parameter	Description
FirstDtmfTimeout	The delayed hotline is activated when the timeout configured in the <i>First DTMF Timeout</i> field of the <i>Telephony > DTMF Maps</i> page elapses (“ General DTMF Maps Parameters ” on page 372).
InterDtmfOrCompletionTimeout	The delayed hotline is activated when the timeout configured in the <i>Completion Timeout</i> field of the <i>Telephony > DTMF Maps</i> page elapses or when the DTMFs collection fails because the <i>Inter DTMF Timeout</i> parameter elapses (“ General DTMF Maps Parameters ” on page 372).
AnyTimeout	The delayed hotline is activated when the timeout configured in the <i>Completion Timeout</i> field of the <i>Telephony > DTMF Maps</i> page elapses and when the DTMFs collection fails because the <i>Inter DTMF Timeout</i> parameter elapses (“ General DTMF Maps Parameters ” on page 372).

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 189: 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.

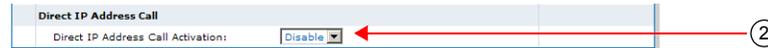
The user can dial an IP address and enter an optional telephone number. Note that the optional telephone number is matched by using the same digit maps as a normal call.

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 190: 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 Mediatrix unit with the IP address 192.168.0.23. The phone number assigned to Line 2 of this Mediatrix unit is 1234. You must then dial the following digits:

**192*168*0*23#1234

In this case, the Mediatrix unit sends an INVITE `1234@192.168.0.23`.

Call Hold



Note: This section applies only to the following models:

- Mediatrix 3208 / 3216
- Mediatrix 3308 / 3316
- Mediatrix 3716
- Mediatrix 3731
- Mediatrix 3732
- Mediatrix 3741
- Mediatrix 3742
- Mediatrix 4100 Series
- Mediatrix LP Series
- Mediatrix C7 Series

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 Mediatrix 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 191: 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



Note: This section applies only to the following models:

- Mediatrix 3208 / 3216
- Mediatrix 3308 / 3316
- Mediatrix 3716
- Mediatrix 3731
- Mediatrix 3732
- Mediatrix 3741
- Mediatrix 3742
- Mediatrix 4100 Series
- Mediatrix LP Series
- Mediatrix C7 Series

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 403](#).

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 Mediatrix 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 192: 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



Note: This section applies only to the following models:

- Mediatrrix 3208 / 3216
- Mediatrrix 3308 / 3316
- Mediatrrix 3716
- Mediatrrix 3731
- Mediatrrix 3732
- Mediatrrix 3741
- Mediatrrix 3742
- Mediatrrix 4100 Series
- Mediatrrix LP Series
- Mediatrrix C7 Series

This section describes configuration that is available only in the MIB parameters of the Mediatrrix 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 Mediatrrix unit listing how many new and old messages are available. The Mediatrrix 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 Mediatrrix 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 Mediatrix unit.
- ▶ Specific configurations that override the default configurations.

You can define specific configurations for each endpoint in your Mediatrix unit. For instance, you could enable a codec for all the endpoints of the Mediatrix 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.fxsDefaultMessageWaitingIndicatorActivation="Value"
```

where *Value* may be one of the following:

Table 354: 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"]="Value"
```

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 355: 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: <ul style="list-style-type: none"> • Mediatrix 4108, 4116 and 4124 • Mediatrix LP Series

Distinctive Call Waiting Tone

The distinctive call waiting tone configuration allows the administrator to modify the pattern of the tone.

Two variables are used:

- *ToneId*: Allows the identification of the distinctive call waiting tone. If the distinctive ring call-property matches the *ToneId*, the distinctive tone will be used.
- *Pattern*: Describes the tone pattern.

A tone pattern contains:

1. Frequencies

Up to 4 frequencies (f1 to f4) each with a power level can be defined. At least one frequency/power pair must be defined. Frequency range is from 10 to 4000 Hz and Power level range is from -99 to 3 dbm.

The syntax is: f1=<frequency>:<power>

2. States

Up to 8 states (s1 to s8) can be defined, each with an action, a set of frequencies, a duration and a next state. At least one state must be described if the tone-pattern is not empty.

- The action can be 'on', 'off' or 'CID' (for call waiting tones).
- The duration of the state is from 10 to 56000 ms.
- The tone is continuous if no time is specified.

The syntax is: s1=<action>:<frequency>:...:<frequency>:<duration>:<end-of-loop-indicator>:<next state>

3. Loops

A set of states can be enclosed in a loop.

- The starting state of a loop is marked with a loop counter (l=), the range is from 2 to 128.
- The ending state of a loop is marked with an end-of-loop indicator (l).

The syntax is: l=<loop count>,<state definition>,...,<state definition (with end-of-loop-indicator)>,<state definition>...

Examples:

- Germany dialtone (continuous): "f1=350:-17,f2=440:-17,s1=on:f1:f2"
- North America Recall dialtone (3 quick tones followed by a continuous tone): "f1=350:-17,f2=440:-17,l=3,s1=on:f1:f2:100:s2,s2=off:100:l:s1,s3=on:f1:f2"
- Australia ring back tone (on 400ms, off 200 ms, on 400 ms and off 2000 ms and replay): "f1=425:-17,f2=400:-5,f3=450:-5,s1=on:f1:f2:f3:400:s2,s2=off:200:s3,s3=on:f1:f2:f3:400:s4,s4=off:2000:s1"

Only two frequencies can be used by the Call Waiting tone.

The parameters can be set :

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

▶ **To set the distinctive call waiting tone:**

1. In the *Telf MIB* set :
 - *Telf.DistinctiveCallWaitingPattern* variable in the *CallWaitingToneGroup* table
 - *Telf.DistinctiveCallWaitingRingId* variable in the *CallWaitingToneGroup* table.
 - or
2. Use the CLI or a configuration script:
 - `Telf.DistinctiveCallWaiting[Index=value].Pattern=value`
 - `Telf.DistinctiveCallWaiting[Index=value].ToneId=value`

Index value can vary from 1 to 4.

Call Statistics

This section describes how to access data available only in the MIB parameters of the Mediatrix unit. You can display these parameters as follows:

- ▶ by using a MIB browser
- ▶ by using the CLI

The following are the call statistics the Mediatrix unit keeps. Statistics are updated at the end of each call.

Table 356: 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.

Table 356: Call Statistics

MIB Variable	Statistics Description
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[EpId=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[EpId=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 Mediatrix 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 357: 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.

CHAPTER

40

Tone Customization Parameters Configuration

This chapter describes how to override the pattern for a specific tone defined for the selected country. (For more details on Tone Definition, refer the Reference Guide at <http://www.media5corp.com/documentation>.)

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:

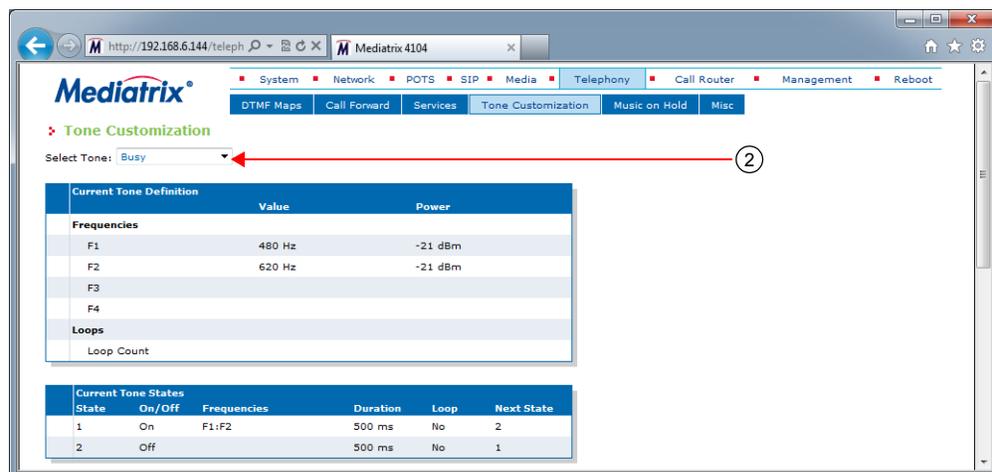
- ▶ Busy
- ▶ Call Waiting
- ▶ Confirmation
- ▶ Congestion
- ▶ Dial
- ▶ Hold
- ▶ Intercept
- ▶ Message Waiting
- ▶ Preemption
- ▶ Reorder
- ▶ Ringback
- ▶ Receiver Off Hook (ROH)
- ▶ Special Information Tone (SIT)
- ▶ Stutter

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 193: 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:

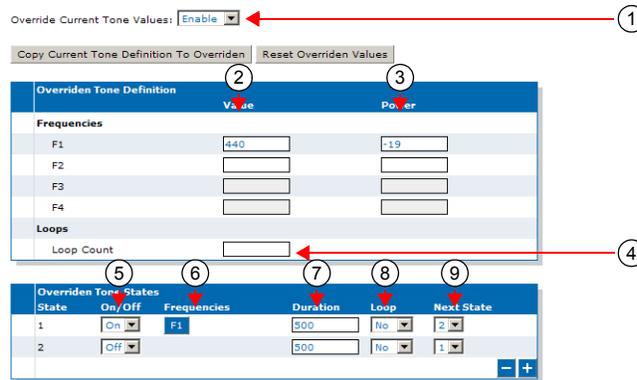
Table 358: Tone Override Sections

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 194: 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

41

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.

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 195: Telephony – Music on Hold Web Page

► **Music on Hold**

Status	
File Status:	No File
Last Transfer Result:	Success
Last Successful Transfer:	

Music on Hold Configuration	
Streaming:	Disable ▾

Transfer Configuration	
URL:	<input type="text"/> (2)
User Name:	<input type="text"/> (3)
Password:	<input type="password"/> (3)
Reload Interval:	<input type="text" value="0"/> (4)

Red arrows and circled numbers (2-5) indicate the fields mentioned in the steps: (2) points to the URL field, (3) points to the User Name and Password fields, (4) points to the Reload Interval field, and (5) points to the Streaming dropdown menu.

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 Mediatrix 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 537 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*.

CHAPTER

42

Country Parameters Configuration

This chapter describes how to

- ▶ configure the country information:
 - Select a specific country.
 - Additional country settings.
- ▶ set the input and output offset

Country Configuration

The *Misc* sub-page of the *Telephony* page allows you to configure the country in which the unit is located. It also allows the user to change the Input and Output Offset.

▶ To select a specific country:

1. In the Web interface, go to *Telephony / Misc*

Figure 196: Telephony – Misc Web Page

2. In the *Country* section, from the *Country Selection* drop-down menu, select the country in which the Mediatrix unit is located

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 Reference Guide for more information on these country-specific settings.

3. Click *Apply*.

▶ To set the Input Offset

1. In the Web interface, go to *Telephony/Misc*
2. From the *Select Endpoint* selection list, select an endpoint.
3. In the *User Gain* section, enter the Input Offset value in the *Input Offset* field.
4. Click *Apply*.

► To set the Output Offset

1. In the Web interface, go to *Telephony/Misc*
2. From the *Select Endpoint* selection list, select an endpoint.
3. In the *User Gain* section, enter the Output Offset value in the *Output Offset* field.
4. Click *Apply*.

Additional Country Settings

This section describes configuration that is available only in the MIB parameters of the Mediatrix 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 Mediatrix unit.
- ▶ Specific configurations that override the default configurations.

You can define specific configurations for each endpoint in your Mediatrix unit. For instance, you could enable a codec for all the endpoints of the Mediatrix 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 Mediatrix unit.



Caution: Use these settings with great care. Media5 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 Mediatrix 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 421](#).

▶ To set user gain variables:

1. In the *telIfMIB*, locate the *countryCustomizationUserGainGroup* folder.
2. On a call involving a SIP terminal and an FXS terminal, raising the output offset will raise the volume perceived on the FXS terminal. Define the default user output gain offset in dB 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. On a call involving a SIP terminal and an FXS terminal, raising the input offset will raise the volume perceived on the SIP terminal. Define the default user input gain offset in dB 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 Mediatrix unit dials numbers.

When selecting a country (see [“Country Configuration” on page 419](#) 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 421](#).

► 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 25 - E&M CAS Configuration” on page 223](#) 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="Interface"]="value"
```

11. Set the duration, in milliseconds, of a MFR1 when dialing on the interface in the `defaultCountryCustomizationDialingMFR1Duration` variable.
See [“Chapter 25 - E&M CAS Configuration” on page 223](#) 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 421](#).

► 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 Mediatix 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 Mediatix 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"
```

CHAPTER
43

Call Detail Record

This chapter describes how to configure call detail record:

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:**

- 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 197: CDR Call Detail Record Section



- 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 359: Control Character

Character	Value
%%	%
\n	Split message

Call detail record macros:

Table 360: 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.
%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)

Table 360: Call Detail Record Macros (Continued)

Macro	Value
%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)
%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

44

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.

Introduction

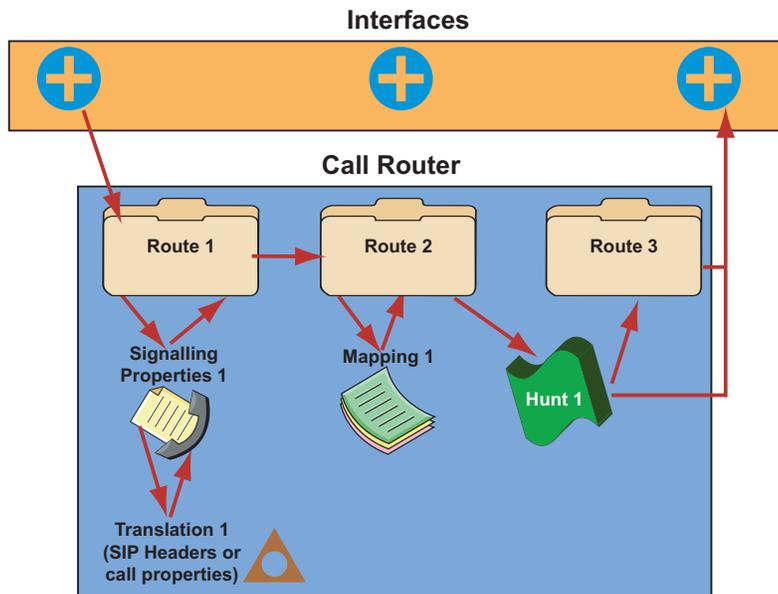
The Mediatrix unit's call router allows you to route calls between interfaces. Based on a set of routing criteria, the call router determines the destination (interface) for every incoming call. The forwarding decisions are based on the following tables:

Table 361: 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 449 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 455 for more details.
Call Signalling	Call signalling specifies how to set up a call to the destination Mediatrix unit or 3 rd 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 465 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 469 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 472 for more details.
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 475 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 483 for more details.

When a new call comes from one of the Mediatrix unit interfaces, it is redirected to the routing table. The following figure illustrates the Mediatrix unit call router:

Figure 198: 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.
- ▶ The call properties Called Bearer Channel and Calling Bearer Channel are limited to ISDN interfaces only.
- ▶ 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
- ▶ Maximum number of Call Properties Translations: 100

Regular Expressions

Some of the routing types described in [“Routing Type” on page 434](#) 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 Mediatrix 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 362: 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.

Table 362: Regular Expressions Wildcards (Continued)

Character	Description
*	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. <ul style="list-style-type: none"> 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 433 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 363: Groups Replacement Example

Replacement	Result
\0	9123456
\1	123456
\2	45

Table 363: Groups Replacement Example

Replacement	Result
\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

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 440](#).

Table 364: Routing Types Locations

Routing Type	Location
E164	"Called / Calling E164" on page 435
Type of Number (TON)	"Called / Calling TON" on page 435
Numbering Plan Indicator (NPI)	"Called / Calling NPI" on page 435
Name	"Called / Calling Name" on page 435
Host	"Called / Calling Host" on page 436
URI	"Called / Calling URI" on page 436
Presentation Indicator (PI)	"Calling PI" on page 436
Screening Indicator (SI)	"Calling SI" on page 436
Information Transfer Capability (ITC)	"Calling ITC" on page 436
Date and Time	"Date/Time" on page 437
Phone Context	"Called / Calling Phone Context" on page 438
SIP Username	"Called / Calling SIP Username" on page 438
Bearer Channel	"Called / Calling SIP Username" on page 438
Diverting Reason	"Last / Original Diverting Reason" on page 438
Diverting E.164	"Last / Original Diverting E.164" on page 438
Diverting Party Number Type	"Last / Original Diverting Party Number Type" on page 438
Diverting Public Type Of Number	"Last / Original Diverting Public Type Of Number" on page 439
Diverting Private Type Of Number	"Last / Original Diverting Private Type Of Number" on page 439
Diverting Number Presentation	"Last / Original Diverting Number Presentation" on page 439
SIP Privacy Type	"SIP Privacy Type" on page 439

Media5 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 440](#) 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 432](#). 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 Mediatrix 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 365: 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 366: 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 432](#) for more details on how to enter a proper expression.

The Mediatrix 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 367: 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 368: 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 369: 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 Mediatrix 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 Mediatrix 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 370: Date/Time Accepted Formats

Format	Description
Date/Time Period format	<ul style="list-style-type: none"> • '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	<ul style="list-style-type: none"> • 'DDD' • 'DDD,DDD...' • 'DDD/HH:MM:SS-HH:MM:SS' • 'DDD,DDD.../HH:MM:SS-HH:MM:SS' <p>DDD must be one of: SUN, MON, TUE, WED, THU, FRI, SAT.</p>

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 432](#).

Called / Calling SIP Username

Calling and called party SIP username. See [“Regular Expressions” on page 432](#) 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 432](#) for more details on how to enter a proper expression.

Last / Original Diverting Reason

This is the last or original diverting reason in ISDN setup and SIP INVITE messages. The following values are available:

Table 371: 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 314](#) 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 432](#). 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 Mediatrix 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 372: 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 373: 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 374: Diverting Private Type of Number Values

Value	Description
unknown	Unknown.
leg2-reg	Leg2 reg.
leg1-reg	Leg1 reg.
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 375: 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 376: 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 377: 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 378: Call Properties to SIP

SIP Field	Description
To	<p>The Mediatrix unit uses the calling URI to populate the <i>To</i> field if not undefined. Otherwise, the unit does the following:</p> <ul style="list-style-type: none"> • Uses the called <i>Name</i> for the friendly name if not undefined. • Uses the called <i>SipUsername</i> for the user name if not empty or undefined; otherwise, uses the called <i>E164</i> for the username. If it is empty or undefined, the Mediatrix unit rather uses the value defined in the <i>Default Username Value</i> field of the <i>SIP > Interop > SIP Interop</i> parameters as username (see “SIP Interop” on page 279 for more details). The unit uses the called <i>Phone Context</i> 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 <i>SIP URI User Parameter Value</i> field of the <i>SIP > Interop > SIP Interop</i> parameters. If empty, then the value 'phone' is used • Uses the called <i>Host</i> 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 <i>SIP URI User Parameter Value</i> field of the <i>SIP > Interop > SIP Interop</i> parameters is not empty, then the parameter is added with the value defined by the field.

Table 378: Call Properties to SIP (Continued)

SIP Field	Description
From	<p>The Mediatrix unit uses the called URI to populate the <i>From</i> field if not undefined. Otherwise, the unit does the following:</p> <ul style="list-style-type: none"> • Uses the calling <i>Name</i> for the friendly name if not undefined. • Uses the calling <i>SipUsername</i> for the user name if not empty or undefined; otherwise, uses the calling <i>E164</i> for the username. If it is empty or undefined, the Mediatrix unit rather uses the value defined in the <i>Default Username Value</i> field of the <i>SIP > Interop > SIP Interop</i> parameters as username (see “SIP Interop” on page 279 for more details). The unit uses the calling <i>Phone Context</i> 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 <i>SIP URI User Parameter Value</i> field of the <i>SIP > Interop > SIP Interop</i> parameters. If empty, then the value 'phone' is used. • Uses the calling <i>Host</i> 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 <i>SIP URI User Parameter Value</i> field of the <i>SIP > Interop > SIP Interop</i> parameters is not empty, then the parameter is added with the value defined by the field.
Request URI	The Mediatrix unit uses the same information as the <i>To</i> field.
Contact	The Mediatrix unit uses the same information as the <i>From</i> field, but with the current IP address/port for the host.

Table 378: Call Properties to SIP (Continued)

SIP Field	Description
Diversion	<p>A <i>Diversion</i> header is added if the <i>Last Diverting E.164</i> property is present and not empty. This <i>Diversion</i> header is constructed as follows:</p> <ul style="list-style-type: none"> The <i>username</i> of the URI is set to the value of the <i>Last Diverting E.164</i> property. The <i>host</i> of the URI is set to the configured home domain proxy host. The <i>reason</i> field is set according to value of the <i>Last Diverting Reason</i> property: <ul style="list-style-type: none"> cfu: "unconditional" cfb: "user-busy" cfnr: "no-answer" All other values or when undefined: "unknown". The field counter is set to the value of <i>DivertingCounter</i> if the <i>Original Diverting E.164</i> property is set to empty or undefined, otherwise it is set to <i>DivertingCounter</i> - 1. <p>A second <i>Diversion</i> header is added if the <i>Last Diverting E.164</i> and <i>Original Diverting E.164</i> properties are present and not empty. This <i>Diversion</i> header is constructed as follows:</p> <ul style="list-style-type: none"> The <i>username</i> of the URI is set to the value of the <i>Original Diverting E.164</i> property. The <i>host</i> of the URI is set to the configured home domain proxy host. The <i>reason</i> field is set according to the value of the <i>Original Diverting Reason</i> property: <ul style="list-style-type: none"> cfu: "unconditional" cfb: "user-busy" cfnr: "no-answer" All other values or when undefined: "unknown". <p>The field counter is set to 1.</p>

SIP to Call Properties

This section describes the SIP information the call router uses for the various call properties.

Table 379: SIP to Call Properties

Property	SIP Information
Called URI	The URL of the <i>To</i> field.
Calling URI	The URL of the <i>From</i> field.
Called Name	The friendly name in the <i>To</i> field. The property is undefined if there is no friendly name.
Calling Name	The friendly name in the <i>From</i> field. The property is undefined if there is no friendly name.
Called E164	The user name of the <i>Request-Uri</i> 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 <i>From</i> 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 <i>To</i> field.

Table 379: SIP to Call Properties (Continued)

Property	SIP Information
Calling Host	The host of the <i>Contact</i> field.
Called TON	Set to "international" if the <i>To</i> user name is an E.164 with the prefix "+"; otherwise, the property is undefined.
Calling TON	Set to "international" if the <i>From</i> 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 <i>To</i> 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 <i>From</i> if the user name is an E.164, otherwise the property is undefined.
Called SIP Username	Set to the username of the <i>Request-Uri</i> . Note that this does not include the username parameter like the "phone-context".
Calling SIP Username	Set to the username of the <i>From</i> . Note that this does not include the username parameter like the "phone-context".
Last Diverting Reason	If the INVITE contains at least one <i>Diversion</i> header, this value is set according to the <i>reason</i> field value of the first <i>Diversion</i> header: <ul style="list-style-type: none"> "user-busy": cfb "unconditional":cfu "no-answer": cfna All other values: unknown Otherwise, the property is undefined. The <i>reason</i> field comparison is not case sensitive.
Original Diverting Reason	If the INVITE contains more than one <i>Diversion</i> header, this value is set according to the <i>reason</i> field value of the last <i>Diversion</i> header: <ul style="list-style-type: none"> "user-busy": cfb "unconditional":cfu "no-answer": cfna All other values: unknown Otherwise, the property is undefined. The <i>reason</i> field comparison is not case sensitive.
Last Diverting E.164	If the INVITE contains at least one <i>Diversion</i> header, this value is set to the <i>username</i> of the URI (can be a SIP URI, SIPS URI or TEL URI) of the first <i>Diversion</i> 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 <i>Diversion</i> header, this value is set to the <i>username</i> of the URI (can be a SIP URI, SIPS URI or TEL URI) of the last <i>Diversion</i> 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 <i>Diversion</i> header, this value is set to the sum of the <i>counter</i> field of all <i>Diversion</i> headers. If a diversion header does not contain the <i>counter</i> 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 380: Call Properties to ISDN

Information Element	Description
Bearer Capabilities	If valid, the <i>calling ITC</i> 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 <i>calling E164</i> to fill the field “number digits” (octet 4). Uses the <i>calling TON</i> to fill the field “type of number” (octet 3 [7:5]). Uses the <i>calling PI</i> to fill the field “presentation indicator” (octet 3a [7:6]). Uses the <i>calling SI</i> to fill the field “screening indicator” (octet 3a [2:1]). Uses the <i>calling NPI</i> to fill the field “numbering plan identification” (octet 3 [4:1]).
Called Party Number	Uses the <i>called E164</i> to fill the field “number digits” (octet 4). Uses the <i>called TON</i> to fill the field “type of number” (octet 3 [7:5]). Uses the <i>called NPI</i> to fill the field “numbering plan identification” (octet 3 [4:1]).
Display	Uses the <i>calling E164</i> 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 381: 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 381: 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 382: 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 <i>E164</i> property (truncated to the first 20 characters). See "Auto-Routing" on page 487 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 <i>Name</i> property (truncated to the first 50 characters). See "Auto-Routing" on page 487 for details.

FXS to Call Properties

This section describes the information the call router uses for the various FXS to call properties.

Table 383: FXS to Call Properties

Caller ID	Description
Calling E164	If the auto routing is enabled and the <i>E164</i> field of the <i>Call Router > Auto-routing</i> page is not empty (see "Auto-Routing" on page 487 for details), the value of the <i>E164</i> field. Otherwise, the property is not present.
Calling Name	If the auto routing is enabled and the <i>Name</i> field of the <i>Call Router > Auto-routing</i> page is not empty (see "Auto-Routing" on page 487 for details), the value of the <i>Name</i> field. Otherwise, the property is not present.
Calling SIP Username	If the auto routing is enabled and the <i>SIP Username</i> field of the <i>Call Router > Auto-routing</i> page is not empty (see "Auto-Routing" on page 487 for details), the value of the <i>SIP Username</i> field. Otherwise, the property is not present.
Called E164	For automatic calls, the E.164 defined in the <i>Automatic Call Target</i> field of the <i>Telephony > Services</i> page (see "Automatic Call" on page 387 for more details). For other calls, the dialed digit after the transformation defined in the <i>Transformation</i> field of the <i>Allowed DTMF Map</i> section (<i>Telephony > DTMF Maps</i> page – see "Allowed DTMF Maps" on page 373 for more details).
Called Name	For automatic calls, the name specified in the <i>Automatic Call Target</i> field of the <i>Telephony > Services</i> page (see "Automatic Call" on page 387 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 383: FXS to Call Properties (Continued)

Caller ID	Description
Called Host	<p>For automatic calls, the host specified in the the <i>Automatic Call Target</i> field of the <i>Telephony > Services</i> page (see “Automatic Call” on page 387 for more details). The property is not present if the target address does not contain a host.</p> <p>For other calls, the host defined in the <i>Target</i> field of the <i>Allowed DTMF Map</i> section (<i>Telephony > DTMF Maps</i> page – see “Allowed DTMF Maps” on page 373 for more details). The property is not present if the target host is not configured for the matching DTMF map.</p>

Call Properties to FXO

This section describes the information the call router uses for the various call properties to FXO.

Table 384: Call Properties to FXO

Caller ID	Description
Dialled number	The <i>Called E164</i> property.

FXO to Call Properties

This section describes the information the call router uses for the various FXO to call properties.

Table 385: FXO to Call Properties

Caller ID	Description
Calling E164	<p>If the caller ID is detected, the numbers provided by the caller ID.</p> <p>If the auto routing is enabled and the <i>E164</i> field of the <i>Call Router > Auto-routing</i> page is not empty (see “Auto-Routing” on page 487 for details), the value of the <i>E164</i> field. Otherwise, the property is not present.</p>
Calling Name	<p>If the caller ID is detected, the name provided by the caller ID.</p> <p>If the auto routing is enabled and the <i>Name</i> field of the <i>Call Router > Auto-routing</i> page is not empty (see “Auto-Routing” on page 487 for details), the value of the <i>Name</i> field. Otherwise, the property is not present.</p>
Calling SIP Username	<p>If the caller ID is detected, the property is not present.</p> <p>If the auto routing is enabled and the <i>SIP Username</i> field of the <i>Call Router > Auto-routing</i> page is not empty (see “Auto-Routing” on page 487 for details), the value of the <i>SIP Username</i> field. Otherwise, the property is not present.</p>
Called E164	<p>For automatic calls, the E.164 defined in the <i>Automatic Call Target</i> field of the <i>Telephony > Services</i> page (see “Automatic Call” on page 387 for more details).</p> <p>For other calls, the dialed digit after the transformation defined in the <i>Transformation</i> field of the <i>Allowed DTMF Map</i> section (<i>Telephony > DTMF Maps</i> page – see “Allowed DTMF Maps” on page 373 for more details).</p>
Called Name	<p>For automatic calls, the name specified in the <i>Automatic Call Target</i> field of the <i>Telephony > Services</i> page (see “Automatic Call” on page 387 for more details). The property is not present if the target address does not contain a name.</p> <p>For other calls, the property is not present.</p>

Table 385: FXO to Call Properties (Continued)

Caller ID	Description
Called Host	<p>For automatic calls, the host specified in the the <i>Automatic Call Target</i> field of the <i>Telephony > Services</i> page (see “Automatic Call” on page 387 for more details). The property is not present if the target address does not contain a host.</p> <p>For other calls, the host defined in the <i>Target</i> field of the <i>Allowed DTMF Map</i> section (<i>Telephony > DTMF Maps</i> page – see “Allowed DTMF Maps” on page 373 for more details). The property is not present if the target host is not configured for the matching DTMF map.</p>

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 386: 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)	<ol style="list-style-type: none"> When the Calling Party Number E.164 is missing: interworking. In this case, this value overrides any value set by the call router. When CLIR is enabled (user-side only): restricted. In this case, this value overrides any value set by the call router. 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)	<p>Network-side: The SI in the incoming Calling Party information element is ignored and replaced by one of the following:</p> <ol style="list-style-type: none"> No calling IA5 digits received: network. NPI is not “unknown” nor “ISDN telephony”: network. TON is not “international” nor “national”: network, called IA5 digits are discarded. PI is set to “interworking”: network. Otherwise: passed. <p>User-side: not-screened.</p>

Table 386: SIP/ISDN Calls Default Values (Continued)

Parameter	Default Value
PI (calling)	<p>Network-side:</p> <ol style="list-style-type: none"> 1. CLIR enabled: restricted. The PI is set to <i>restricted</i> 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. <p>User-side:</p> <ol style="list-style-type: none"> 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 23 - ISDN Configuration” on page 149](#) 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.

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.

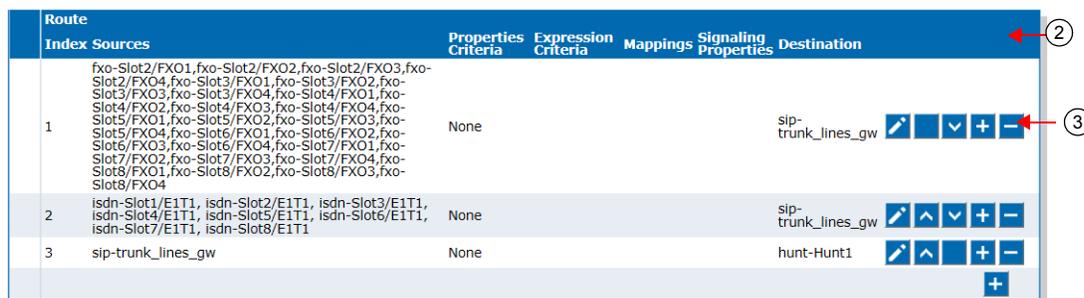
Creating/Editing a Route

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.

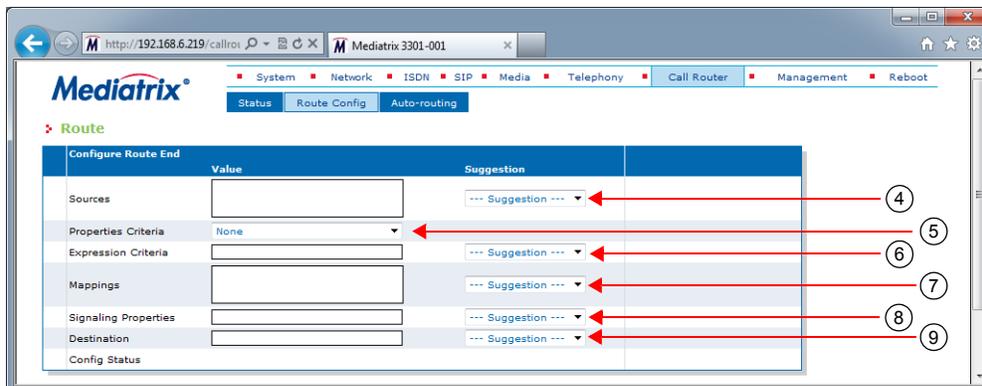
Figure 200: Call Router – Route Config Web Page



Route Index	Sources	Properties Criteria	Expression Criteria	Mappings	Signaling Properties	Destination
1	fxo-Slot2/FXO1,fxo-Slot2/FXO2,fxo-Slot2/FXO3,fxo-Slot2/FXO4,fxo-Slot3/FXO1,fxo-Slot3/FXO2,fxo-Slot3/FXO3,fxo-Slot3/FXO4,fxo-Slot4/FXO1,fxo-Slot4/FXO2,fxo-Slot4/FXO3,fxo-Slot4/FXO4,fxo-Slot5/FXO1,fxo-Slot5/FXO2,fxo-Slot5/FXO3,fxo-Slot5/FXO4,fxo-Slot6/FXO1,fxo-Slot6/FXO2,fxo-Slot6/FXO3,fxo-Slot6/FXO4,fxo-Slot7/FXO1,fxo-Slot7/FXO2,fxo-Slot7/FXO3,fxo-Slot7/FXO4,fxo-Slot8/FXO1,fxo-Slot8/FXO2,fxo-Slot8/FXO3,fxo-Slot8/FXO4	None				sip-trunk_lines_gw
2	isdn-Slot1/E1T1, isdn-Slot2/E1T1, isdn-Slot3/E1T1, isdn-Slot4/E1T1, isdn-Slot5/E1T1, isdn-Slot6/E1T1, isdn-Slot7/E1T1, isdn-Slot8/E1T1	None				sip-trunk_lines_gw
3	sip-trunk_lines_gw	None				hunt-Hunt1

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 **+** of this row.
 - If you want to add a route at the end of the existing rows, click **+** 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  . This brings you to the *Configure Route* panel.

Figure 201: Configure Route Panel



- 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.



Note: When using *endpoint* gateways, SIP interface names are composed of both the gateway name and a username; for example, a SIP source on an endpoint gateway may be: sip-default/5551212. When using *trunk* gateways, SIP interface names are based on the gateway name only.

- 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 387: 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.

Table 387: Routing Types (Continued)

Type	Description
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 <i>To-URI</i> .
Calling URI	Routes calls based on the <i>From-URI</i> .
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 <i>Expression criteria</i> field. Use it to easily configure the Date/Time type.
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.

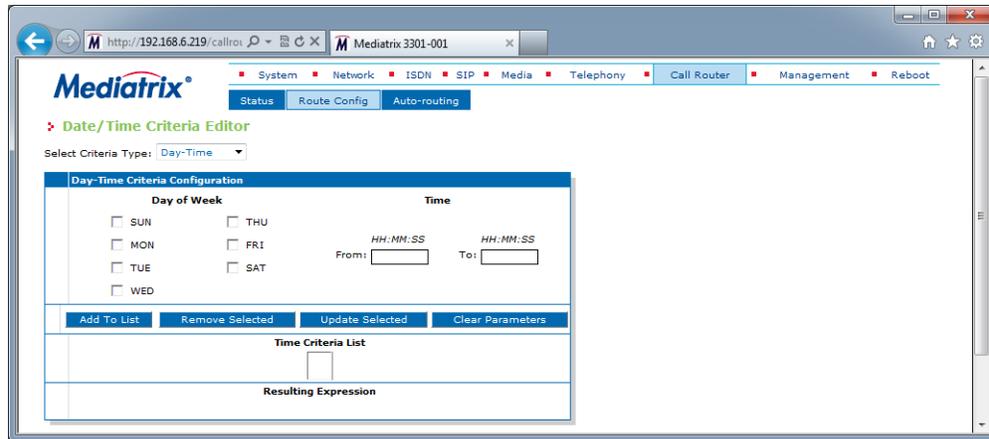
You can use the *Suggestion* column's drop-down menu to select between suggested values, if any. See ["Routing Type" on page 434](#) for a list of available values for each call property.

For instance, if the property is *Calling TON*, you could instruct the call router to look for the following expression:

```
international
```

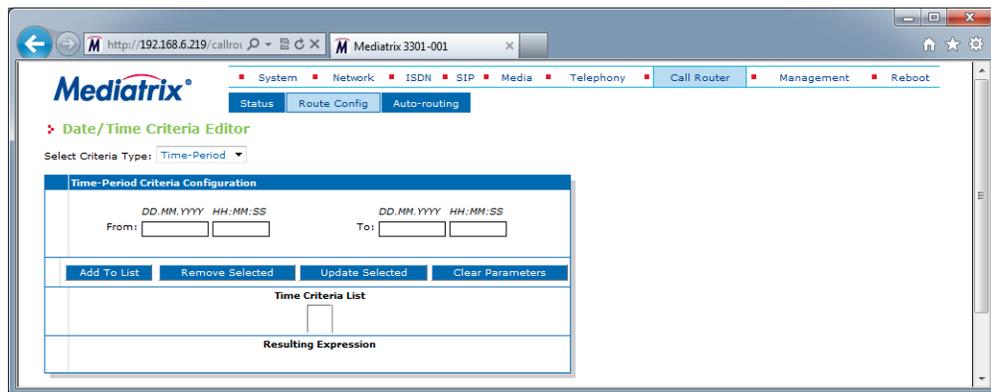
If you have selected the *Date/Time* property in the above step, you can click the **Time criteria editor** link and use the editor to easily configure the Date/Time parameters.

Figure 202: 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 203: Date/Time Criteria Editor (Time Period)



- Select or enter the parameters you want, then click **Add to List** . 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 **Remove Selected** .
- To update an existing parameter, select it in the *Time Criteria List* field, then click **Update Selected** .
- To remove all parameters, click **Clear Parameters** .
- When done, click **Save** .

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 455](#) 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 465](#). 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 483](#) or more details.

For instance, if you want to route calls to the hunt “CallCenter”, enter the following:

```
hunt-CallCenter
```



Note: When using *endpoint* gateways, SIP interface names are composed of both the gateway name and a username; for example, a SIP source on an endpoint gateway may be: sip-default/5551212. When using *trunk* gateways, SIP interface names are based on the gateway name only.

10. Click **Save**.

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 **Save** 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 204: 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  or  of the row you want to move until the entry is properly located.
2. Click **Save** 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  of the row you want to delete.
2. Click **Save** 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

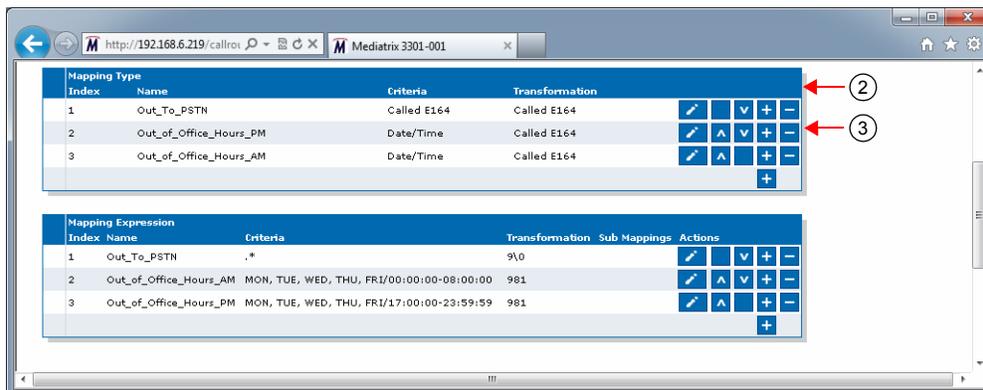
The *Mapping Type* part allows you to define the input call property to match and to define which call property to change. The mapping type then uses one or more corresponding mapping expressions that you can define in [“Creating/Editing a Mapping Expression” on page 457](#).

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.

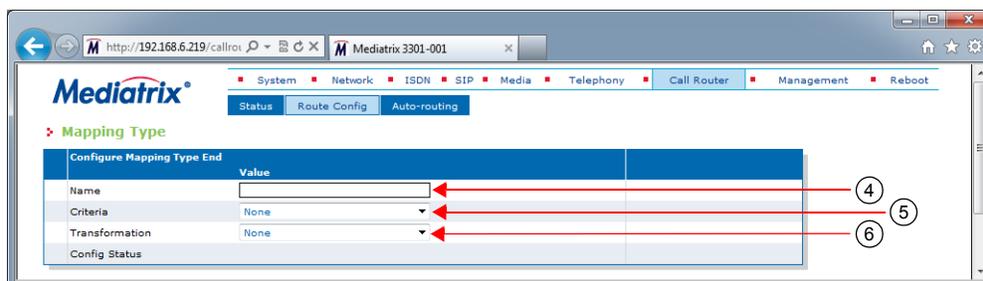
Figure 205: Call Router – Route Config Web Page



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 **+** of this row.
 - If you want to add a mapping type entry at the end of the existing rows, click **+** 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 **[edit]**.

This brings you to the *Configure Mapping Type* panel.

Figure 206: 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. Media5 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 457](#) 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 **Save** to go back to the main *Call Router > Route Config* web page. You can now define a corresponding mapping expression.
 - Click **Save and Insert Expression** to directly access the proper mapping expression dialog.

Creating/Editing a Mapping Expression

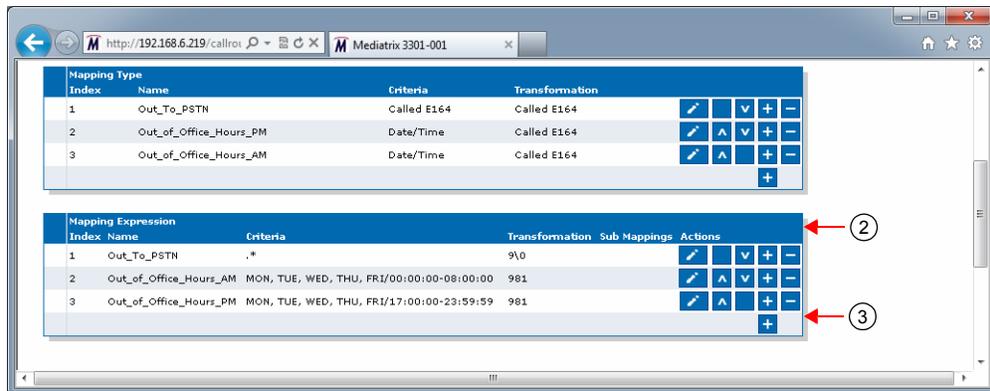
The *Mapping Expression* part defines the actual transformation to apply to the corresponding mapping type. Each mapping expression must match a mapping type as defined in “[Creating/Editing a Mapping Type](#)” on page 455.

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.

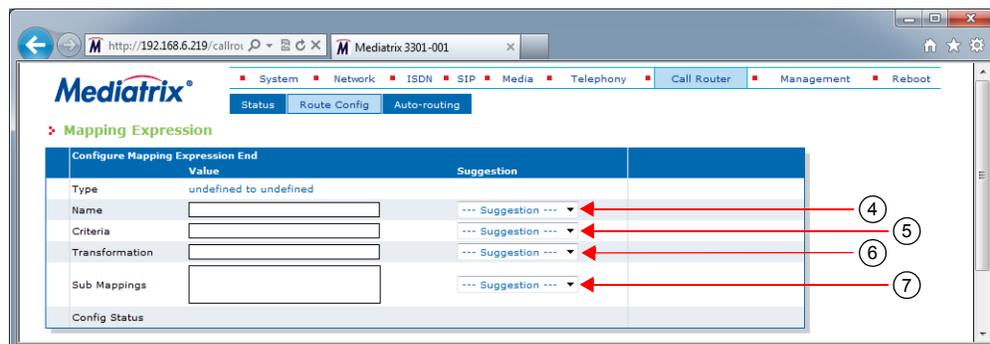
Figure 207: Call Router – Route Config Web Page



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 **+** of this row.
 - If you want to add a mapping expression entry at the end of the existing rows, click **+** 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 .

This brings you to the *Configure Mapping Expression* panel.

Figure 208: 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 455. 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 434](#) for a list of available transformation values.

Table 388: Input Type Criteria

Input Type	Criteria
None	No criteria, always matches.
E164	If the <i>Transformation</i> value of the <i>Mapping Type</i> part is also a generic property, this is applied to both this <i>Calling E164</i> and <i>Called E164</i> 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 435 .
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 435 .
Name	If the <i>Transformation</i> value of the <i>Mapping Type</i> part is also a generic property, this is applied to both this <i>Calling Name</i> and <i>Called Name</i> 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 435 .
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 435 .
TON	If the <i>Transformation</i> value of the <i>Mapping Type</i> part is also a generic property, this is applied to both this <i>Calling TON</i> and <i>Called TON</i> property.
Called TON	Selects an entry based on the called party type of number as per "Called / Calling TON" on page 435 .
Calling TON	Selects an entry based on the calling party type of number as per "Called / Calling TON" on page 435 .
NPI	If the <i>Transformation</i> value of the <i>Mapping Type</i> part is also a generic property, this is applied to both this <i>Calling NPI</i> and <i>Called NPI</i> property.
Called NPI	Selects an entry based on the called party numbering plan indicator as per "Called / Calling NPI" on page 435 .
Calling NPI	Selects an entry based on the calling party numbering plan indicator as per "Called / Calling NPI" on page 435 .
Host	If the <i>Transformation</i> value of the <i>Mapping Type</i> part is also a generic property, this is applied to both this <i>Calling Host</i> and <i>Called Host</i> 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 436 .
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 436 .
Calling PI	Selects an entry based on the presentation indicator as per "Calling PI" on page 436 .
Calling SI	Selects an entry based on the screening indicator as per "Calling SI" on page 436 .

Table 388: Input Type Criteria (Continued)

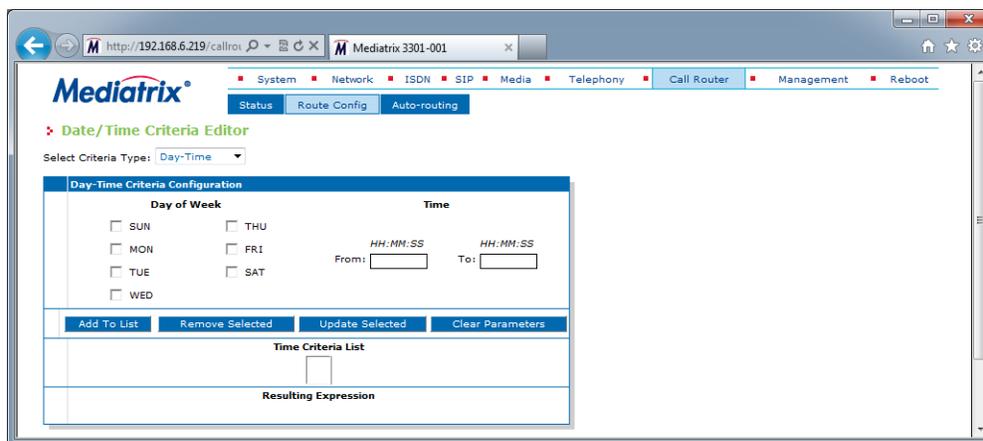
Input Type	Criteria
Calling ITC	Selects an entry based on the information transfer capability as per “Calling ITC” on page 436 .
URI	If the <i>Transformation</i> value of the <i>Mapping Type</i> part is also a generic property, this is applied to both this <i>Calling URI</i> and <i>Called URI</i> property.
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 436 .
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 436 .
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 437 .
Phone Context	Selects an entry based on the called or calling phone context properties as per “Called / Calling Phone Context” on page 438 .
Called Phone Context	Selects an entry based on the called phone context properties as per “Called / Calling Phone Context” on page 438 .
Calling Phone Context	Selects an entry based on the calling phone context properties as per “Called / Calling Phone Context” on page 438 .
SIP Username	Selects an entry based on the called or calling SIP username properties as per “Called / Calling SIP Username” on page 438 .
Called SIP Username	Selects an entry based on the called SIP username properties as per “Called / Calling SIP Username” on page 438 .
Calling SIP Username	Selects an entry based on the calling SIP username properties as per “Called / Calling SIP Username” on page 438 .
Last Diverting Reason	Selects an entry based on the last diverting reason properties as per “Last / Original Diverting Reason” on page 438 .
Last Diverting E164	Selects an entry based on the last diverting E.164 properties as per “Last / Original Diverting E.164” on page 438 .
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 438 .
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 439 .
Last Diverting Private Type Of Number	Selects an entry based on the private type of number of the last diverting number properties as per “Last / Original Diverting Private Type Of Number” on page 439 .
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 439 .
OriginalDiver tingReason	Selects an entry based on the original diverting reason properties as per “Last / Original Diverting Reason” on page 438 .

Table 388: Input Type Criteria (Continued)

Input Type	Criteria
OriginalDiver tingE164	Selects an entry based on the original diverting E.164 properties as per “Last / Original Diverting E.164” on page 438.
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 438.
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 439.
Called Bearer Channel	Selects an entry based on the called bearer channel properties as per “Called / Calling SIP Username” on page 438.
Calling Bearer Channel	Selects an entry based on the calling bearer channel properties as per “Called / Calling SIP Username” on page 438.
Calling SIP Privacyl	Selects an entry based on the calling SIP privacy properties as per “SIP Privacy Type” on page 439.

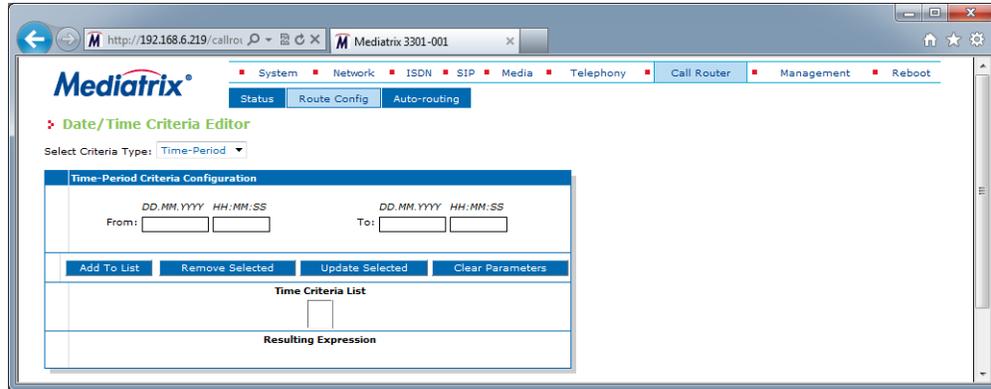
If you are editing a *Date/Time* property, you can click the **Time criteria editor** link and use the editor to easily configure the Date/Time parameters.

Figure 209: 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 210: Date/Time Criteria Editor (Time Period)



- Select or enter the parameters you want, then click **Add to List** . 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 **Remove Selected**.
 - To update an existing parameter, select it in the *Time Criteria List* field, then click **Update Selected**.
 - To remove all parameters, click **Clear Parameters**.
 - When done, click **Save**.
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 433 for more details. See “Routing Type” on page 434 for a list of available transformation values.

Table 389: Output Type Transformation

Output Type	Transformation
None	No transformation is applied.
E164	If the <i>Criteria</i> value of the <i>Mapping Type</i> part is also a generic property, this is applied to both the <i>Calling E164</i> and <i>Called E164</i> properties.
Called E164	Modifies the called party E.164 number as per “Called / Calling E164” on page 435.
Calling E164	Modifies the calling party E.164 number as per “Called / Calling E164” on page 435.
Name	If the <i>Criteria</i> value of the <i>Mapping Type</i> part is also a generic property, this is applied to both the <i>Calling Name</i> and <i>Called Name</i> properties.
Called Name	Sets the display name of the called party as per “Called / Calling Name” on page 435.
Calling Name	Sets the display name of the calling party as per “Called / Calling Name” on page 435.
TON	If the <i>Criteria</i> value of the <i>Mapping Type</i> part is also a generic property, this is applied to both the <i>Calling TON</i> and <i>Called TON</i> properties.
Called TON	Sets the called party type of number as per “Called / Calling TON” on page 435.
Calling TON	Sets the calling party type of number as per “Called / Calling TON” on page 435.

Table 389: Output Type Transformation (Continued)

Output Type	Transformation
NPI	If the <i>Criteria</i> value of the <i>Mapping Type</i> part is also a generic property, this is applied to both the <i>Calling NPI</i> and <i>Called NPI</i> properties.
Called NPI	Sets the called party numbering plan indicator as per “Called / Calling NPI” on page 435 .
Calling NPI	Sets the calling party numbering plan indicator as per “Called / Calling NPI” on page 435 .
Host	If the <i>Criteria</i> value of the <i>Mapping Type</i> part is also a generic property, this is applied to both the <i>Calling Host</i> and <i>Called Host</i> properties.
Called Host	Sets the remote IP address or domain name of the destination VoIP peer as per “Called / Calling Host” on page 436 .
Calling Host	Sets the remote IP address or domain name of the originating VoIP peer as per “Called / Calling Host” on page 436 .
Calling PI	Sets the presentation indicator as per “Calling PI” on page 436 .
Calling SI	Sets the screening indicator as per “Calling SI” on page 436 .
Calling ITC	Sets the information transfer capability as per “Calling ITC” on page 436 .
URI	If the <i>Criteria</i> value of the <i>Mapping Type</i> part is also a generic property, this is applied to both the <i>Calling URI</i> and <i>Called URI</i> properties.
Called URI	Sets the called URI as per “Called / Calling URI” on page 436 .
Calling URI	Sets the calling URI as per “Called / Calling URI” on page 436 .
Phone Context	If the <i>Criteria</i> value of the <i>Mapping Type</i> part is also a generic property, this is applied to both the <i>Calling Phone Context</i> and <i>Called Phone Context</i> properties.
Called Phone Context	Sets the called Phone Context as per “Called / Calling Phone Context” on page 438 .
Calling Phone Context	Sets the calling Phone Context as per “Called / Calling Phone Context” on page 438 .
SIP Username	If the <i>Criteria</i> value of the <i>Mapping Type</i> part is also a generic property, this is applied to both the <i>Calling SIP Username</i> and <i>Called SIP Username</i> properties.
Called SIP Username	Sets the called SIP Username as per “Called / Calling SIP Username” on page 438 .
Calling SIP Username	Sets the calling SIP Username as per “Called / Calling SIP Username” on page 438 .
Last Diverting Reason	Sets the last diverting reason properties as per “Last / Original Diverting Reason” on page 438 .
Last Diverting E164	Sets the last diverting E.164 properties as per “Last / Original Diverting E.164” on page 438 .
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 438 .

Table 389: Output Type Transformation (Continued)

Output Type	Transformation
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 439.
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 439.
Last Diverting Number Presentation	Sets the presentation of the last diverting number properties as per “Last / Original Diverting Number Presentation” on page 439.
Original Diverting Reason	Sets the original diverting reason properties as per “Last / Original Diverting Reason” on page 438.
Original Diverting E.164	Sets the original diverting E.164 properties as per “Last / Original Diverting E.164” on page 438.
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 438.
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 439.
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 439.
Original Diverting Number Presentation	Sets the Presentation of the original diverting number properties as per “Last / Original Diverting Number Presentation” on page 439.
Called Bearer Channel	Sets the called bearer channel properties as per “Called / Calling SIP Username” on page 438.
Calling Bearer Channel	Sets the calling bearer channel properties as per “Called / Calling SIP Username” on page 438.
Debug	Reserved for debug configuration.

You cannot use Date/Time as an output type transformation.

- 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 **Save** 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 **Save and Insert Expression** button to create another expression for the same type.
9. Click **Save** 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 211: 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  or  of the row you want to move until the entry is properly located.
 2. Click **Save** 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  of the row you want to delete.
 2. Click **Save** to update the *Call Router > Status* web page.

Signalling Properties

Call signalling specifies how to set up a call to the destination Mediatrix 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 449.

► **To create or edit a signalling property:**

1. In the web interface, click the *Call Router* link, then the *Route Config* sub-link.

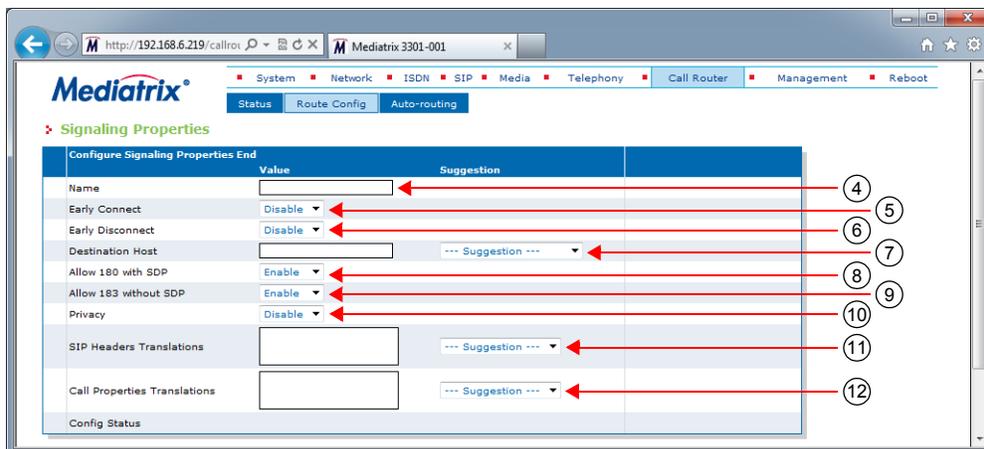
Figure 212: Call Router – Route Config Web Page



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 **+** of this row.
 - If you want to add a signalling property entry at the end of existing rows, click **+** 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 .

This brings you to the *Configure Signaling Properties* panel.

Figure 213: 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 449.
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 390: 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.

Table 390: 180 with SDP Parameters (Continued)

Parameter	Description
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.

- Define whether or not to enable the 183 without SDP allowed feature in the *Allow 183 No SDP* drop-down menu.

Table 391: 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.

- Set the privacy level of the call in the *Privacy* drop-down menu.

Table 392: Privacy Levels

Level	Description	Effects on incoming SIP call	Effects on outgoing SIP call
Disable	No privacy is used.	None	None
None	Use P-Asserted Identity privacy.	None	Adds two headers: <ul style="list-style-type: none"> Privacy: none P-Asserted-Identity: p_asserted_identity_value <p><i>p_asserted_identity_value</i> is the call's From URI unless a SIP header translation has been added to the Signaling Properties for the <i>Identity-header</i>.</p>
Id	Use P-Preferred Identity privacy.	The <i>calling-name</i> is empty and the PI is set to restricted .	Always adds one header: <ul style="list-style-type: none"> P-Preferred-Identity: p_preferred_identity_value <p><i>p_preferred_identity_value</i> is the call's From URI unless a SIP header translation has been added to the Signaling Properties for the <i>Identity-header</i>.</p> <p>If the incoming call's PI property is <i>restricted</i>, another header is added:</p> <ul style="list-style-type: none"> Privacy: id

Table 392: Privacy Levels (Continued)

Level	Description	Effects on incoming SIP call	Effects on outgoing SIP call
Rpid	Use Remote-Party-ID privacy.	None	<p>One header always added :</p> <ul style="list-style-type: none"> Remote-Party-ID: remote_party_id_value <p>"Optional Friendly Name"<sip:410202@10.4.125.12>;party=calling</p> <p>Where <i>remote_party_id_value</i> should be set by the SIP Headers Translation. It consists of an optional friendly name followed by the SIP URI and the party direction.</p> <p>Example:</p> <pre>Remote-Party-ID: "John Doe"<sip:410202@10.4.125.12>;party=calling</pre>

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 469](#). 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 472](#). 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 **Save** 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 **Save** 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 214: Signalling Properties Examples

Signalling 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 ▲ or ▼ of the row you want to move until the entry is properly located.
 2. Click the **Save** 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 - of the row you want to delete.
 2. Click **Save** 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.

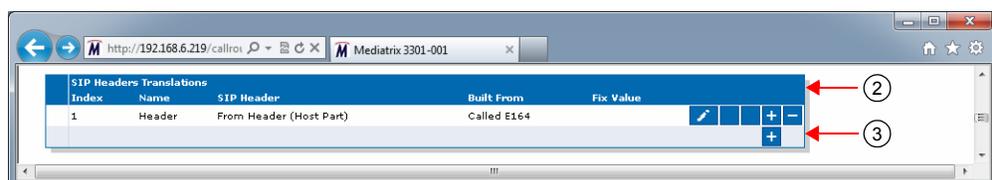
You can add up to 100 SIP Headers Translations.

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 465.

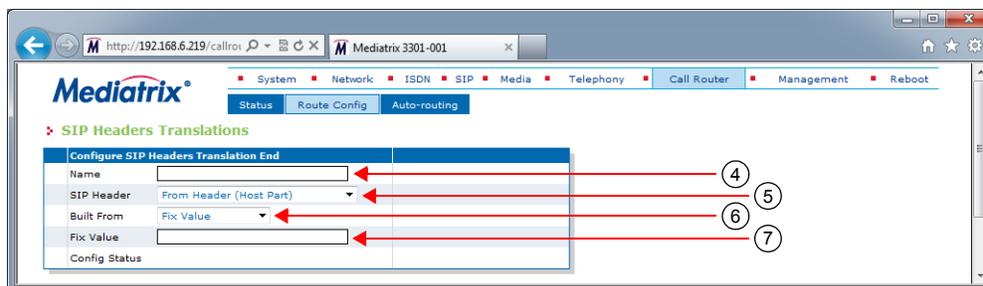
- ▶ **To create or edit a SIP headers translation:**
 1. In the web interface, click the *Call Router* link, then the *Route Config* sub-link.

Figure 215: 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 **+** of this row.
 - If you want to add a SIP headers translation at the end of existing rows, click **+** 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 **✎**.
- This brings you to the *Configure SIP Headers Translation* panel.

Figure 216: 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 393: SIP Headers

SIP Header	Description
From Header (Host Part)	Host part of the <i>From</i> header's URI.
From Header (User Part)	User part of the <i>From</i> header's URI.
Identity Header (Host Part)	Host part of the <i>Identity</i> header's URI.
Identity Header (User Part)	User part of the <i>Identity</i> header's URI.
Identity Header (Phone Number)	Phone number in the <i>Identity</i> 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 <i>To</i> header's URI.
To Header (User Part)	User part of the <i>To</i> header's URI.

6. Set what information is used to build the selected SIP header in the *Built From* drop-down menu.

Table 394: 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 <i>Fix Value</i> field (see Step 7).
Host Name	Use the host name configured in the unit.

Table 394: Built From Information (Continued)

Built From	Description
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 **Save** 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 **Save** 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 217: 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  or  of the row you want to move until the entry is properly located.
2. Click **Save** 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  of the row you want to delete.
2. Click **Save** 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.

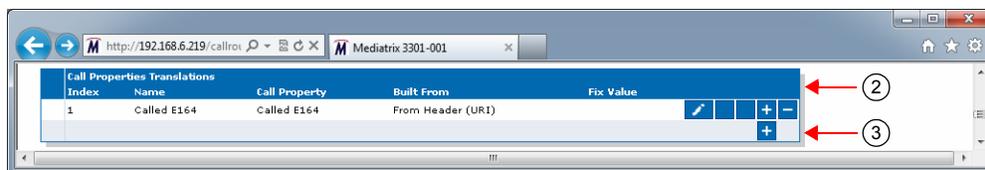
Creating/Editing a Call Properties Translation

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 465.

► **To create or edit a call properties translation:**

1. In the web interface, click the *Call Router* link, then the *Route Config* sub-link.

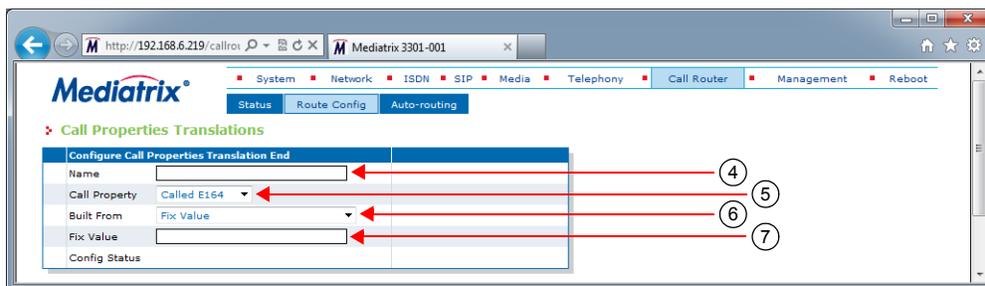
Figure 218: Call Router – Route Config Web Page



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 **+** of this row.
 - If you want to add a call properties translation at the end of existing rows, click **+** 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 **✎**.

This brings you to the *Configure Call Properties Translation* panel.

Figure 219: Configure Call Properties Translation Panel



4. Enter the name of the call properties translation in the *Name* field.

- Set which call property is modified by this translation in the *Call Property* drop-down menu.

Table 395: 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.

- Set what information is used to build the selected call property in the *Built From* drop-down menu.

Table 396: 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 <i>Fix Value</i> field (see Step 7).
From Header (Uri)	Use the <i>From</i> header's URI.
From Header (Friendly Name)	Use the friendly name part of the <i>From</i> header.
From Header (User Part)	Use the user part of the <i>From</i> header's URI.
Identity Header (Uri)	Use the <i>Identity</i> header's URI.
Identity Header (User Part)	Use the user part of the <i>Identity</i> header's URI.
Identity Header (Phone Number)	Use the phone number in the <i>Identity</i> 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: <ul style="list-style-type: none"> 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 <i>Identity</i> 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 <i>To</i> header's URI.
To Header (Friendly Name)	Use the friendly name part of the <i>To</i> header.
To Header (User Part)	Use the user part of the <i>To</i> header's URI.

- 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.

- Click the **Save** 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.

- Click the **Save** 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 220: 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:

- Either click  or  of the row you want to move until the entry is properly located.
- Click **Save** 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:

- Click  of the row you want to delete.
- Click **Save** 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 221: *Call Router – Route Config Web Page*

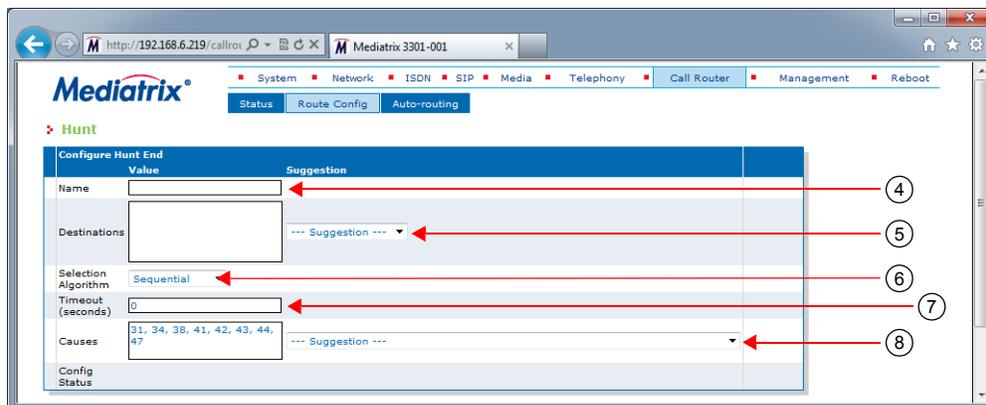
Hunt			
Index	Name	Destinations	Causes
1	Hunt1	isdn-Slot1/E1T1,isdn-Slot2/E1T1,isdn-Slot3/E1T1,isdn-Slot4/E1T1,isdn-Slot5/E1T1,isdn-Slot6/E1T1,isdn-Slot7/E1T1,isdn-Slot8/E1T1,fxo-Slot2/FXO1,fxo-Slot2/FXO2,fxo-Slot2/FXO3,fxo-Slot2/FXO4,fxo-Slot3/FXO1,fxo-Slot3/FXO2,fxo-Slot3/FXO3,fxo-Slot3/FXO4,fxo-Slot4/FXO1,fxo-Slot4/FXO2,fxo-Slot4/FXO3,fxo-Slot4/FXO4,fxo-Slot5/FXO1,fxo-Slot5/FXO2,fxo-Slot5/FXO3,fxo-Slot5/FXO4,fxo-Slot6/FXO1,fxo-Slot6/FXO2,fxo-Slot6/FXO3,fxo-Slot6/FXO4,fxo-Slot7/FXO1,fxo-Slot7/FXO2,fxo-Slot7/FXO3,fxo-Slot7/FXO4,fxo-Slot8/FXO1,fxo-Slot8/FXO2,fxo-Slot8/FXO3,fxo-Slot8/FXO4	31, 34, 38, 41, 42, 43, 44, 47
		Sequential	0

✎
+
-
+

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 + of this row.
 - If you want to add a hunt entry at the end of existing rows, click + 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 ✎.

This brings you to the *Configure Hunt* panel.

Figure 222: 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).
For instance:
isdn-Slot2/Pri1, route-test (Mediatrix 3000 Series)
isdn-Bri1, route-test (Mediatrix 4400 Series)
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 Mediatrix 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 223: Hunt Timeout Example

Hunt						
Index	Name	Destinations	Selection Algorithm	Timeout (seconds)	Causes	Actions
1	isdn-to-sip	sip-default, isdn-slot3/bri2	Sequential	5	31, 34, 38, 41, 42, 43, 44, 47	<input type="button" value="Edit"/> <input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="+"/>

The Mediatrix 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 Mediatrix 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 279).

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 478 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 **Save**.

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 .

10. In the main *Call Routing Config* web page, click **Save** 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 224: 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 Mediatrix 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 397: 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: <ul style="list-style-type: none"> • 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 398: 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 399: 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 400: 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 400: 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 401: 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 402: 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 402: 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 403: 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  or  of the row you want to move until the entry is properly located.
2. Click **Save** 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  of the row you want to move.
2. Click **Save** 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.

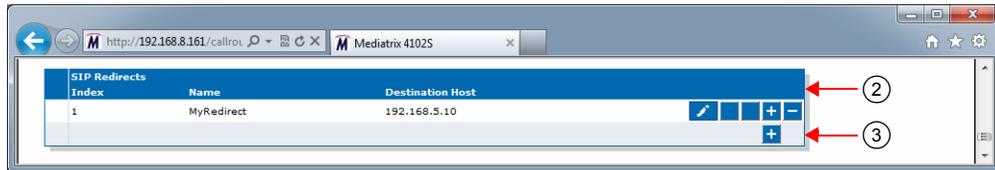
Creating/Editing a SIP Redirect

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.

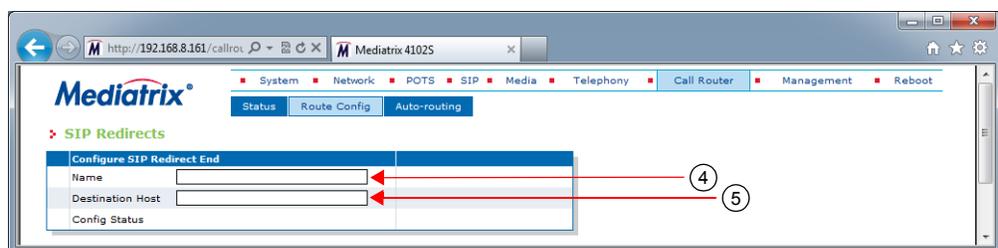
Figure 225: *Call Router – Route Config Web Page*



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 **+** of this row.
 - If you want to add a SIP Redirect entry at the end of existing rows, click **+** 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 **[edit]**.

This brings you to the *Configure SIP Redirect* panel.

Figure 226: *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 **Save** 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 **Save** 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 227: 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  or  of the row you want to move until the entry is properly located.
2. Click **Save** 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  of the row you want to move.
2. Click **Save** to update the *Call Router > Status* web page.

Hairpinning

Hairpinning is defined as a call between two telephony endpoints without using SIP.

Hairpinning is only supported between ISDN and R2 endpoints.

The Call Router does not produce an error when configuring a route between telephony interfaces that do not support the hairpinning, but the call will fail if it uses the configured route. This is not limited to direct routes in the route table configuration, but also for calls that use multiple routes and hunts where the source and the final destination are telephony interfaces that do not support hairpinning.

Calls between the following telephony interfaces are allowed:

- ▶ ISDN <-> ISDN
- ▶ ISDN<-> SIP
- ▶ E&M<-> E&M
- ▶ E&M<->SIP
- ▶ R2 <-> R2
- ▶ R2 <-> SIP
- ▶ FXS <-> SIP
- ▶ FXO <-> SIP

Hairpinning is thus possible with the Mediatrix 440x, Mediatrix 34xx, Mediatrix 35xx, and Mediatrix 36xx models.

Hairpinning is not possible with the Mediatrix 41xx, C7 and Mediatrix 33xx models.

The Mediatrix 37xx models partially support hairpinning with their ISDN card.

You can still make a loopback call on the same unit between two interfaces that do not support hairpinning by performing a SIP loopback. To do this, you need to:

- ▶ make a route from the source telephony interface to a SIP interface ([“Routes” on page 449](#))
- ▶ associate a “Signalling Properties” to override the SIP destination ([“Signalling Properties” on page 465](#))
- ▶ make a route from the SIP interface to the destination telephony interface ([“Routes” on page 449](#))

Configuration Examples

For configuration examples refer to the

CHAPTER

45

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 490](#) for more details.

▶ **To activate auto-routing:**

1. In the web interface, click the *Call Router* link, then the *Auto-routing* sub-link.

Figure 228: 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 4) 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 404: 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 455](#) 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 455](#) 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 465](#) 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 465](#) 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.

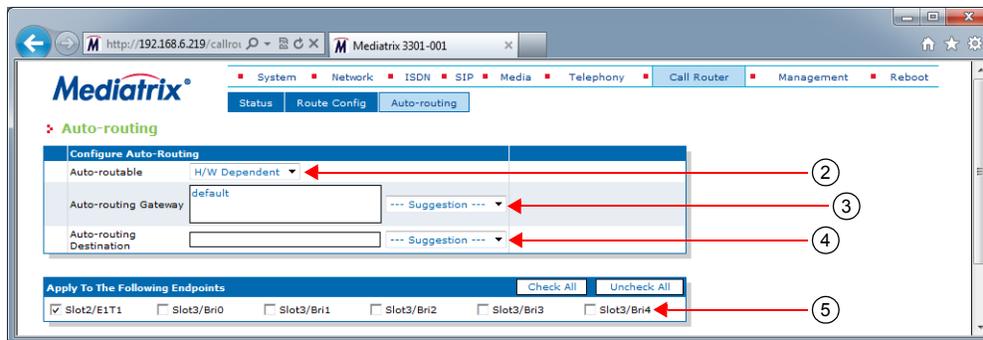
Endpoints Auto-Routing

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  button.
 The Configure Auto-Routing page displays:

Figure 229: 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 405: 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.

Please 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 255 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 Mediatrix 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 287](#) 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 230](#) gives an example of manual routes for an endpoint using "5550001_parameter" as user.

Figure 230: 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 v + -
2	fxs-Port02	None		Port2_username, destination_suffix	sip-default	Edit ^ v + -
3	sip-default	Called URI	sip:5550001_*		fxs-Port01	Edit ^ v + -
4	sip-default	Called URI	sip:5550002_*		fxs-Port02	Edit ^ v + -
+						

Mapping Type				
Index	Name	Criteria	Transformation	Actions
1	destination_suffix	Called E164	Called E164	Edit v + -
2	Port1_username	Calling E164	Calling E164	Edit ^ v + -
3	Port2_username	Calling E164	Calling E164	Edit ^ v + -
+				

Mapping Expression					
Index	Name	Criteria	Transformation	Sub Mappings	Actions
1	Port1_username		5550001_parameter		Edit v + -
2	Port2_username		5550002_parameter		Edit ^ v + -
3	destination_suffix	(.+)	\\1_parameter		Edit ^ v + -
+					

Management Parameters

Page Left Intentionally Blank

CHAPTER

46

Configuration Script

This chapter describes the configuration script download feature, which allows updating the Mediatrix unit configuration by transferring a configuration script from a remote server or from the local file system. The Mediatrix unit is the session initiator, which allows NAT traversal. You can also configure the Mediatrix unit to automatically update its configuration.

For complete details, refer to the Configuration Scripts Import and Export technical bulletin at <http://www.media5corp.com/documentation>.

CHAPTER

47

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 Mediatrix unit into a configuration image file located on a remote server or to the local file system.

For complete details refer to the Configuration Backup and Restore technical bulletin at <http://www.media5corp.com/documentation>.

CHAPTER

48

Firmware Download

This chapter describes how to install, uninstall and update software components on the Mediatrix unit by using the web interface, according to a supplied Firmware Pack selection.

For complete details, refer to the Firmware Dowload technical bulletin at <http://www.media5corp.com/documentation>.

CHAPTER

49

Certificates Management

This chapter describes how to transfer and manage certificates into the Mediatrix unit.

Introduction

The Mediatrix 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 Mediatrix unit uses two types of certificates:

Table 406: 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 Media5 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.

HTTPS Transfer Cipher Suite Settings

This section describes configuration that is available only in the MIB parameters of the Mediatrix 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 allowed cipher suites for the network security settings when using the HTTPS transfer protocol. When the device initiates an HTTPS connection to a server it will negotiate the cipher suite according to its configuration.

Table 407: Cipher Suites Configuration Parameters

Parameter	Description
CS1	<p>This is the default value and represents the cipher suites configuration prior to this variable being introduced. This should be changed if additional network security is required. The Web server only accepts the following cipher suites:</p> <ul style="list-style-type: none"> • TLS_DHE_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_DSS_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA • TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA • TLS_RSA_WITH_3DES_EDE_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_DSS_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_RC4_128_SHA • TLS_RSA_WITH_RC4_128_MD5 • TLS_DHE_RSA_WITH_DES_CBC_SHA • TLS_DHE_DSS_WITH_DES_CBC_SHA • TLS_RSA_WITH_DES_CBC_SHA • TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA • TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA • TLS_RSA_EXPORT_WITH_DES40_CBC_SHA • TLS_RSA_EXPORT_WITH_RC4_40_MD5
CS2	<p>This represents a secure configuration using SHA-1. The Web server only accepts requests using cipher suites:</p> <ul style="list-style-type: none"> • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_3DES_EDE_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

Table 407: Cipher Suites Configuration Parameters

Parameter	Description
CS3	<p>This represents the most secure configuration using SHA-2. Only the most secure cipher suites are allowed when using this value.</p> <ul style="list-style-type: none"> • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_128_GCM_SHA256 - • TLS_RSA_WITH_AES_128_CBC_SHA256

► **To set the HTTPS transfer cipher suite configuration parameter:**

1. In the *cert MIB*, locate the *transferGroup* folder.
2. Set the HTTPS transfer cipher suite configuration in the `TransferHttpsCiphersuite` variable.

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

```
cert.TransferHttpsCiphersuite="value"
```

where *Value* may be as follows:

Table 408: Cipher Suites Configuration Values

Value	Meaning
100	CS1
200	CS2
300	CS3

HTTPS Transfer Tls Version Settings

You can define the allowed TLS version for the network security settings when using the HTTPS transfer protocol. When the device initiates an HTTPS connection to a server it will negotiate the TLS version according to its configuration.

You can configure this parameter as follows:

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

Table 409: Tls Version Configuration Settings

Parameter	Description
SSLv3	Allow SSL version 3 and all TLS versions.
TLSv1	Allow TLS versions 1 and up.
TLSv1_1	Allow TLS versions 1.1 and up.
TLSv1_2	Allow TLS versions 1.2 and up.

The device will always send its highest supported TLS version in the ClientHello message.

The server will select the highest supported TLS version it supports from the ClientHello message.

The device will then validate that the selected version is allowed. If the version is not allowed the device will close the connection.

The default value is TLSv1.

► **To set the HTTPS transfer Tls Version configuration parameter:**

1. In the *cert MIB*, locate the *transferGroup* folder.

Set the HTTPS transfer Tls version configuration in the `TransferHttpsTlsVersion` variable.

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

```
Cert.TransferHttpsTlsVersion = "value"
```

where value may be:

Table 410: Tls Version Configuration Values

Value	Meaning
100	SSLv3
200	TLSv1
300	TLSv1_1
400	TLSv1_2

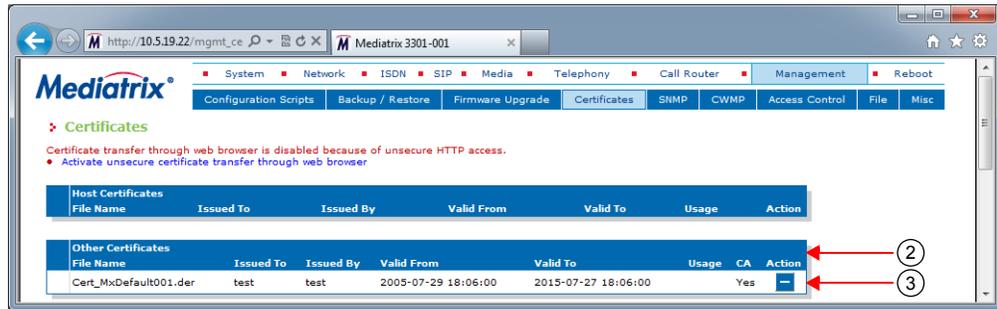
Managing Certificates

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 231: 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 232: 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 233: 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 Mediatrix 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 23](#)) 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 Mediatrix 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. Refer to the Scripting Language Configuration Notes at <http://www.media5corp.com/documentation> for more details on the Media5 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 411: Certificate Transfer Values

Value	Description
Fileurl	<p>URL to a Certificate file that is loaded upon executing the execution of Download command. The transfer protocols supported are:</p> <ul style="list-style-type: none"> • HTTP • HTTPS • TFTP • FTP <p>Examples of valid URLs:</p> <ul style="list-style-type: none"> • <code>http://www.myserver.com/Cert_MxDefault001.der</code> • <code>tftp://myserver.com:69/myfolder/Cert_MxDefault001.der</code> <p>When the port is not included in the URL, the default port for the chosen protocol is used.</p> <p>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:</p> <ul style="list-style-type: none"> • <code>%mac%</code> - the MAC address of the unit. • <code>%product%</code> - 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	<p>Type of certificate to transfer.</p> <ul style="list-style-type: none"> • 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 234: Host Certificate Associations Section

Host Certificate Associations							
File Name	SIP	Web	EAP	Conf	Fpu	File	Cert

Table 412: 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 412: Host Certificate Associations Parameters (Continued)

Parameter	Description
EAP	Specifies if this certificate can be used for EAP security.
Conf	Specifies if this certificate can be used for Conf security.
Fpu	Specifies if this certificate can be used for Fpu security.
File	Specifies if this certificate can be used for File security.
Cert	Specifies if this certificate can be used for Cert security.

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

CHAPTER

50

SNMP Configuration

This chapter describes how to set the SNMP parameters of the Mediatrix unit.

Introduction

All parameters available in the Mediatrix unit web interface may also be configured via SNMP. The Mediatrix unit SNMP feature offers the following options:

- ▶ Password-protected access
- ▶ Remote management
- ▶ Simultaneous management

The Mediatrix unit SNMP feature allows you to configure all the MIB services by using a SNMP browser to contact the MIBs of the Mediatrix unit. It is assumed that you have basic knowledge of TCP/IP network administration.



Note: The Mediatrix unit's SNMP settings do not support IPv6. See [“IPv4 vs. IPv6 Availability” on page 49](#) for more details.

You can use the MIB browser built in the Media5' 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 Mediatrix 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.

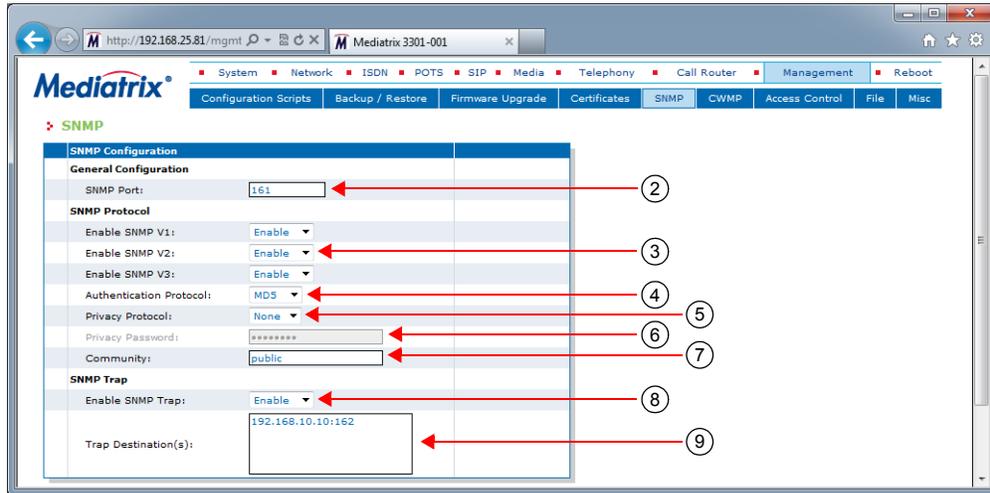
SNMP Configuration Section

The SNMP Configuration section allows you to configure the SNMPv3 privacy information that allows securing the Mediatrix unit, as well as defining where the Mediatrix unit must send traps.

► To set SNMP parameters:

1. In the web interface, click the *Management* link, then the *Snmp* sub-link.

Figure 235: 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 413: 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 Mediatrix 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.

- If SNMPv3 is enabled, set the *Authentication Protocol* drop-down menu with the authentication protocol to use with SNMPv3.

Table 414: 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 537 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 52 - Access Control Configuration” on page 537).

- If SNMPv3 is enabled, set the privacy protocol to use with SNMPv3 in the *Privacy Protocol* drop-down menu.

Table 415: SNMP Privacy Protocol

Protocol	Description
None	No encryption is used. The <i>Privacy Password</i> 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 537 for more details.

- 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 537 for more details.

- 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 Mediatrix for non-authenticated SNMP access (SNMPv1 and SNMPv2). See “Additional SNMP Parameters” on page 513 for more information.

- Specify that traps can be sent by setting the *Enable SNMP Traps* drop-down menu to **enable**.

There are five conditions that the Mediatrix 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 Mediatrix unit sends the traps. If any of those conditions is false, the Mediatrix 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 416: 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 7 for details on how to work with the CLI.

The Mediatrix unit handles five different types of trap:

Table 417: Trap Types

Trap	Description
coldStart	<p>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.</p> <p>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.</p> <p>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.</p>
warmStart	<p>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.</p> <p>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.</p> <p>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.</p>
linkDown	<p>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.</p> <p>The Trap-PDU of type linkDown includes ifIndex, ifAdminStatus, ifOperStatus (as of RFC 2233) of the interface that generated the trap.</p>

Table 417: 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 Mediatrix 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 Mediatrix 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**.

For more details refer to *Performing a Partial Reset* Technical Bulletin at <http://www.media5corp.com/documentation>.

SNMP Statistics

The following are the statistics the Mediatrix unit keeps.

Table 418: 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

51

CWMP Configuration

This chapter describes how to set the CWMP parameters of the Mediatrix unit. The CPE WAN Management Protocol (Cwmp) service is an optional feature that may be added to a Mediatrix unit at purchase time. For more details, contact your sales representative.

Introduction

The CPE WAN Management Protocol service allows configuring the Mediatrix unit via the TR-069 protocol. The supported data models are a subset of Internet Gateway Device (TR-098) and Device (TR-106) and includes Mediatrix proprietary data models.

Using TR-069, the Mediatrix unit can get in contact with an Auto Configuration Server (ACS) to initiate a configuration script transfer/execution and a firmware upgrade. The periodic informs are also supported to allow the unit to contact the ACS when behind a NAT.

See [“ACS Access to the Local Log Table” on page 534](#) for the list of supported methods and parameters.



Note: The Mediatrix unit's CWMP settings do not support IPv6. See [“IPv4 vs. IPv6 Availability” on page 49](#) for more details.

Licence Key Activation of TR-069

You can enable the TR-069 feature on units that are already deployed via an encrypted licence key. See [“Activate Licence” on page 552](#) for more details.

CWMP Configuration Section

The *CWMP Configuration* section allows you to configure the CWMP general parameters, as well as the ACS and Periodic Inform parameters.

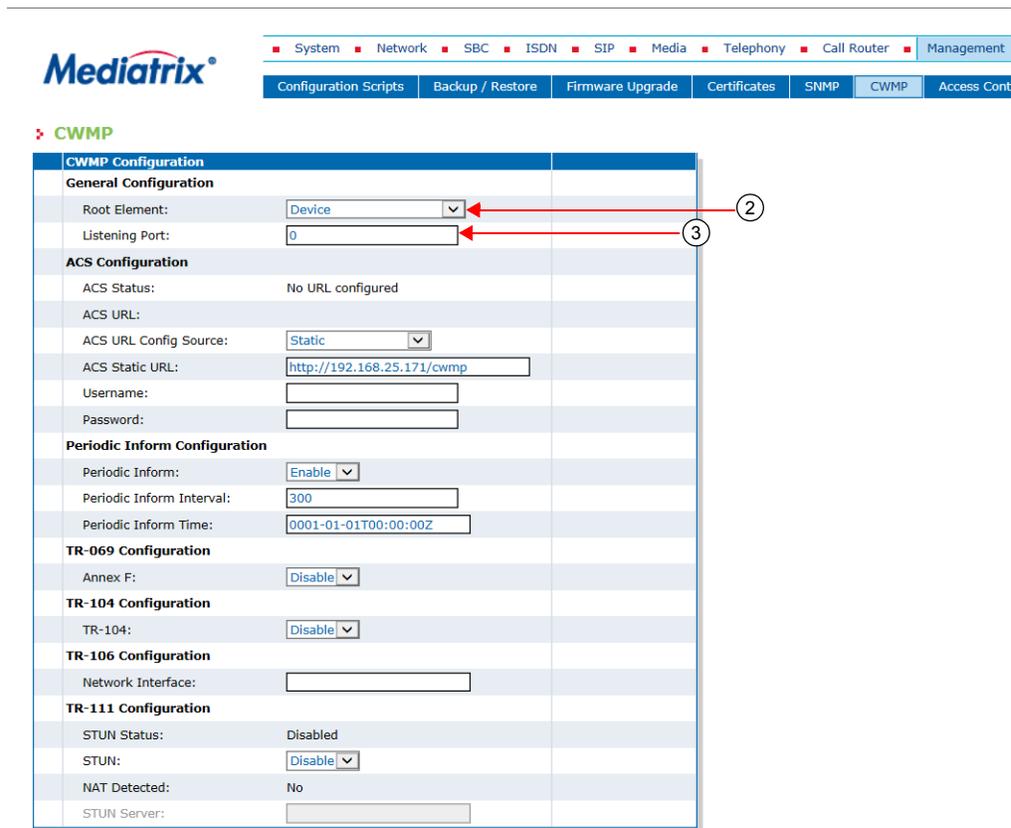
General Configuration

The *General Configuration* part allows you to set the basic CWMP parameters.

► **To set general CWMP parameters:**

1. In the web interface, click the *Management* link, then the *CWMP* sub-link.

Figure 236: Management – CWMP Web Page



2. In the *General Configuration* part, set the *Root Element* drop-down menu with the data model used for the configuration.

Table 419: Root Element Parameters

Parameter	Description
Device	The Mediatrix unit uses the Device data model as defined in TR-106.
Internet Gateway Device	The Mediatrix unit uses the Internet Gateway Device data model as defined in TR-098.

3. Set the *Listening Port* field with the port number on which the unit listens for incoming CPE WAN Management Protocol connections.

If you set the field to **0**, the Mediatrix unit uses the default CPE WAN Management Protocol port 7547.

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

ACS Configuration

The *ACS Configuration* part allows you to set how to contact the ACS server.

The ACS Status field displays the status of the connection with the ACS.

Table 420: ACS Status

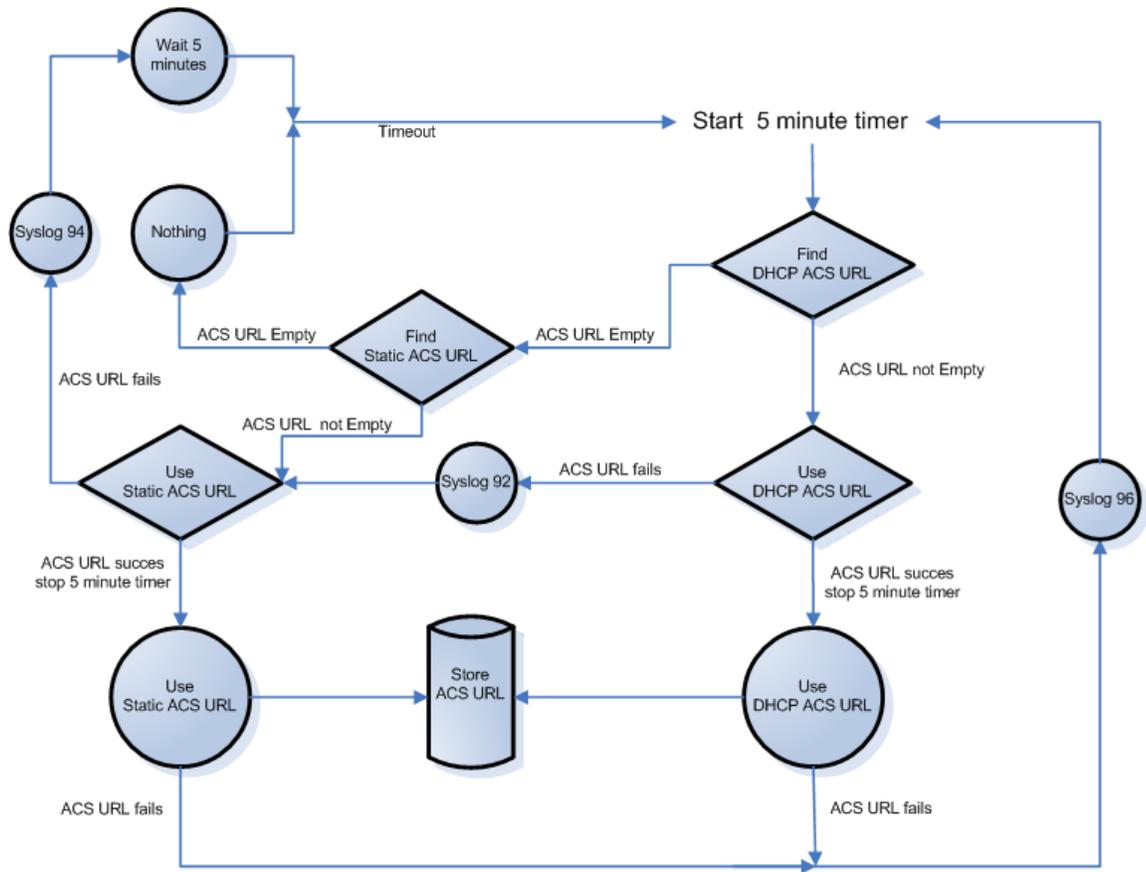
Status	Description
Starting	Cwmp service is starting and no connection attempt have been made so far.
Connected	The Cwmp service is connected to the ACS.
NoUrl	The Cwmp service cannot connect with the ACS because no ACS URL is configured.
ErrorCannotResolve	The Cwmp service cannot connect with the ACS because the FQDN cannot be resolved.
ErrorNotResponding	The Cwmp service cannot connect with the ACS because the ACS is not responding.
ErrorAuthFailure	The Cwmp service failed authenticating to the ACS.
ErrorOther	The Cwmp service cannot connect to the ACS for unspecified reason. See device and ACS logs.

► **To define the ACS parameters:**

1. In the *ACS Configuration* part, set the *ACS URL Config Source* field with the method to obtain the URL of the ACS.

Table 421: ACS URL Config Source Parameters

Parameter	Description
DHCP	<p>If the ACS Config Source field is set to DHCP, the unit will use the ACS URL obtained from the DHCP.</p> <p>If the ACS fails to respond, the unit will send periodic DHCP Informs every 5 minutes to get a new ACS URL.</p>
Static	<p>If the ACS Config Source is set to Static, the unit will use the configured static URL.</p> <p>If the static ACS URL fails to respond, the unit will try the ACS URL obtained from the DHCP only and only if the ACS was already contacted by the unit.</p> <p>If the ACS URL fails to respond, the unit will send periodic DHCP Informs every 5 minutes to get a new ACS URL. This is possible if the unit was originally configured using ACS Config Source to DHCP and the ACS server changed the ACS Config Source to Static and provisioned an invalid ACS static URL.</p>
DHCP with Failover	<p>If the ACS Config Source field is set to DHCP with Failover, the unit will use the URL obtained via the DHCP.</p> <p>If no ACS URL is found, the unit will try using the Static URL.</p> <p>If no static URL is found, the unit will reattempt to use the ACS URL of the DHCP. The attempts to use the DHCP or the ACS static URL will be carried out every 5 minutes until an URL is found.</p>



Cwmp: 3900-CPE WAN Management Protocol: 92-ACS URL provisioning fall back to static configuration
 Cwmp: 3900-CPE WAN Management Protocol: 94-ACS URL provisioning fails with both DHCP and static configuration
 Cwmp: 3900-CPE WAN Management Protocol: 96-ACS URL lost connection with the unit

Figure 237: The following figure describes only the DHCP with Failover scenario.

Figure 238: Management – CWMP Web Page, ACS Part

The screenshot displays the Mediatrix CWMP Configuration web page. The navigation menu includes System, Network, SBC, ISDN, SIP, Media, Telephony, Call Router, and Management. The CWMP configuration page is divided into several sections:

- General Configuration:** Root Element (Device), Listening Port (0).
- ACS Configuration:** ACS Status (No URL configured), ACS URL, ACS URL Config Source (Static), ACS Static URL (http://192.168.25.171/cwmp), Username, Password.
- Periodic Inform Configuration:** Periodic Inform (Enable), Periodic Inform Interval (300), Periodic Inform Time (0001-01-01T00:00:00Z).
- TR-069 Configuration:** Annex F (Disable).
- TR-104 Configuration:** TR-104 (Disable).
- TR-106 Configuration:** Network Interface.
- TR-111 Configuration:** STUN Status (Disabled), STUN (Disable), NAT Detected (No), STUN Server.

2. If the configuration source is set to *Static* or *DHCP with Failover*, set the *ACS Static URL* field with the URL used by the unit to connect to the ACS.

This parameter must be a valid HTTP or HTTPS URL.

Example:

`http://somewhere.com`

`https://somewhere.secure.com`

3. Set the *Username* field with the username used to authenticate the unit when making a connection to the ACS.



Caution: The *Username* field is not accessible if you have the User or Observer access right. See “Users” on page 537 for more details.

4. Set the *Password* field with the password used to authenticate the unit when making a connection to the ACS.



Caution: The *Password* field is not accessible if you have the User or Observer access right. See “Users” on page 537 for more details.

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

ACS Configuration Parameters

This section describes configuration that is available only in the MIB parameters of the Mediatrix 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 a username and password to authenticate an ACS making a connection request to the CPE.

▶ **To set the ACS connection request username and password:**

1. In the *cwmpMIB*, locate the *AcsGroup* folder.
2. Define the username to authenticate an ACS making a connection request to the CPE in the *connectionRequestUsername* variable.

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

```
cwmp.ConnectionRequestUsername="value"
```

The default *Value* is *admin*.

3. Define the password to authenticate an ACS making a connection request to the CPE in the *connectionRequestPassword* variable. This variable contains a secret value.

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

```
cwmp.ConnectionRequestPassword="value"
```

The default *Value* is *administrator*.

Periodic Inform Configuration

The *Periodic Inform Configuration* part allows you to configure the parameters related to the Inform method call.

When *Periodic Inform* is enabled, the Mediatix unit periodically notifies the ACS of parameter changes and the ACS can then execute commands on the unit. This method allows the unit to contact the ACS when behind a NAT or firewall. Notifications to the ACS are also sent if there are no parameter changes.

▶ **To define the Periodic Inform parameters:**

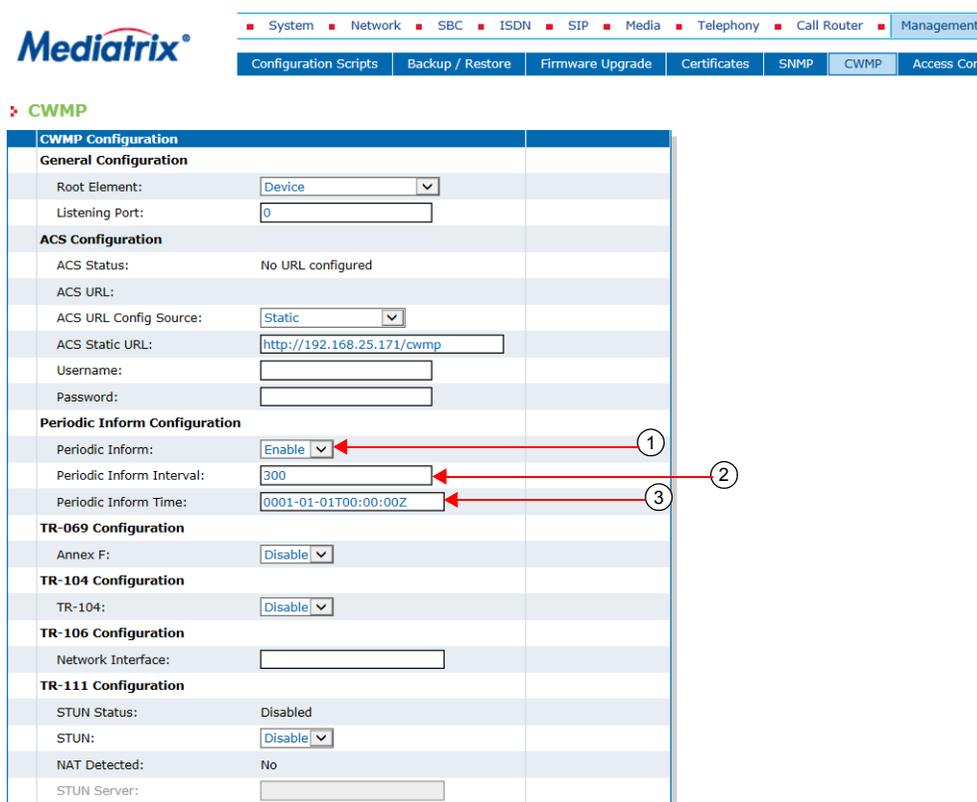
1. In the *Periodic Inform Configuration* part, set the *Periodic Inform Enable* drop-down menu with the proper behaviour.

This defines whether or not the unit needs to periodically send CPE information to the ACS using the Inform method call.

Table 422: Periodic Inform Parameters

Parameter	Description
Disable	The unit does not send periodic inform.
Enable	The unit sends periodic inform.

Figure 239: Management – CWMP Web Page, Periodic Inform Part



2. Set the *Periodic Inform Interval* field with the duration, in seconds, of the interval for which the unit needs to attempt to connect with the ACS and call the Inform method.
3. Set the *Periodic Inform Time* field with an absolute time reference in UTC format to determine when the unit initiates the periodic Inform method calls.

Each Inform call MUST occur at this reference time plus or minus an integer multiple of the *Periodic Inform Interval* parameter (Step 2).

The *Periodic Inform Time* parameter is used only to set the "phase" of the periodic Informs. The actual value of the *Periodic Inform Time* field can be arbitrarily far into the past or future.

For example, if *Periodic Inform Interval* is 86400 (a day) and if *Periodic Inform Time* is set to UTC midnight on some day (in the past, present, or future), then periodic Informs will occur every day at UTC midnight. These MUST begin on the very next midnight, even if *Periodic Inform Time* refers to a day in the future.

The Unknown Time value indicates that no particular time reference is specified. That is, the unit locally chooses the time reference and needs only to follow the specified *Periodic Inform Interval*. If absolute time is not available to the unit, its periodic Inform behavior is the same as if the *Periodic Inform Time* parameter was set to the Unknown Time value.

The format of the value is:

CCYY-MM-DDThh:mm:ssZ

where:

- CCYY: Year number.
- MM: Month number in the year.
- DD: Day number in the month.
- hh: Hour number in the day.

- mm: Minute number in the hour.
- ss: Second number in the minute.

Example:

1969-07-21T02:28:00Z

The Unknown Time value is defined as:

0001-01-01T00:00:00Z

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

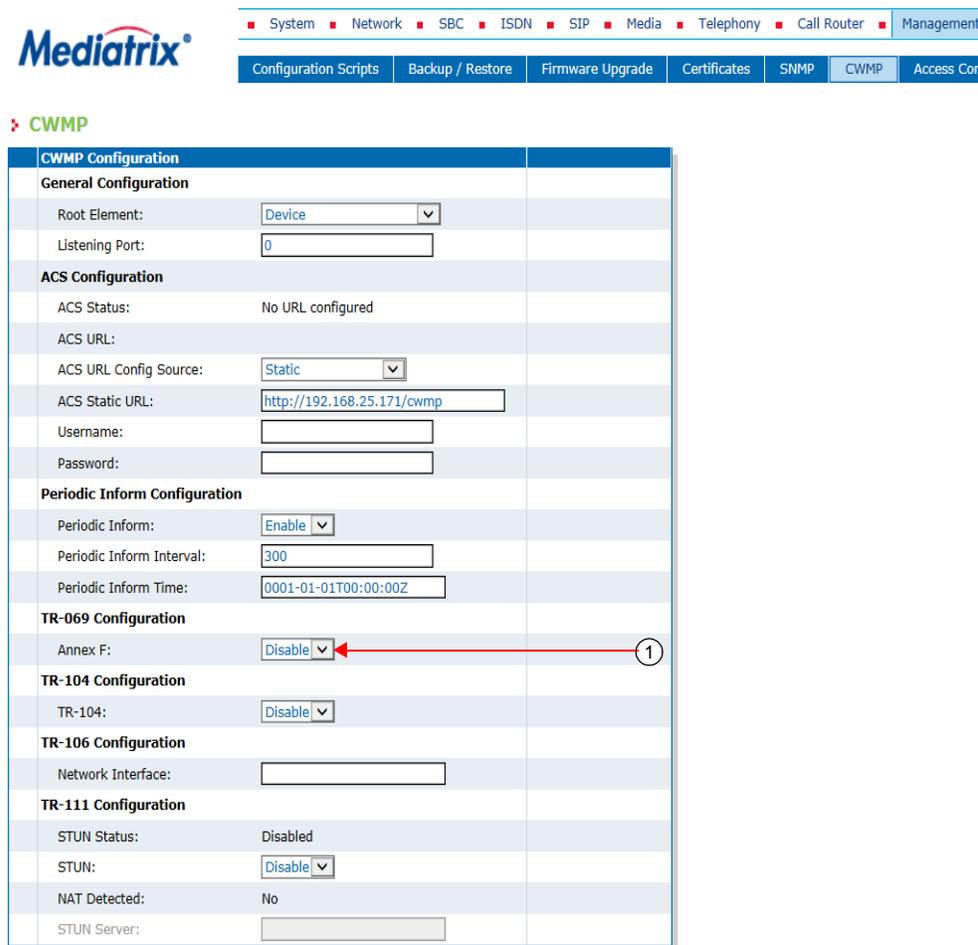
TR-069 Configuration

The *TR-069 Configuration* part allows you to enable or disable the support of variables under the TR-069 Device.GatewayInfo tree.

► **To set the TR-069 configuration:**

1. In the *TR-069 Configuration* part, set the *Annex-F* drop-down menu with the proper behaviour. This parameter enables/disables the support of variables under the TR-069 Device.GatewayInfo tree.

Figure 240: Management – CWMP Web Page, TR-069 Configuration Part



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

TR-104 Configuration



Note: This feature is available on the following models:

- Mediatrix 3208 / 3216
- Mediatrix 3308 / 3316
- Mediatrix 3716 / 3731 / 3732 / 3741 / 3742
- Mediatrix 4102S
- Mediatrix 4104
- Mediatrix 4108/4116/4124
- Mediatrix LP series
- Mediatrix C7 Series

The *TR-104 Configuration* part allows you to enable or disable the provisioning parameters for VoIP CPE.

► To set the TR-104 configuration:

1. In the *TR-104 Configuration* part, set the *TR-104 Enable* drop-down menu with the proper behaviour.

This parameter enables/disables the support of variables under the TR-069 Device.Services.VoiceService tree.

Figure 241: Management – CWMP Web Page, TR-104 Configuration Part

CWMP Configuration	
General Configuration	
Root Element:	Device
Listening Port:	0
ACS Configuration	
ACS Status:	No URL configured
ACS URL:	
ACS URL Config Source:	Static
ACS Static URL:	http://192.168.25.171/cwmp
Username:	
Password:	
Periodic Inform Configuration	
Periodic Inform:	Enable
Periodic Inform Interval:	300
Periodic Inform Time:	0001-01-01T00:00:00Z
TR-069 Configuration	
Annex F:	Disable
TR-104 Configuration	
TR-104:	Disable
TR-106 Configuration	
Network Interface:	
TR-111 Configuration	
STUN Status:	Disabled
STUN:	Disable
NAT Detected:	No
STUN Server:	

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

TR-104 Implementation Limitations

- The Media5 implementation of TR-104 is limited to the SIPEndpoint profile:1 for the

VoiceService :1 object.

- ▶ Active notifications are not supported for all objects except when explicitly mentioned under the Notification field in the mapping table in section [“ACS Access to the Local Log Table” on page 534](#).
- ▶ Only FXS lines can be managed by the TR-104 profile. BRI, PRI or FXO lines are not supported but can be configured with configuration variables.
- ▶ A single voice profile is supported, it is instantiated by default. No creation or deletion of voice profile is allowed.
- ▶ Only a subset of variables is currently supported. Refer to section [“ACS Access to the Local Log Table” on page 534](#).
- ▶ When TR-104 is used, it is highly recommended not to use other means of configuration (since TR-104 assumes some configuration).

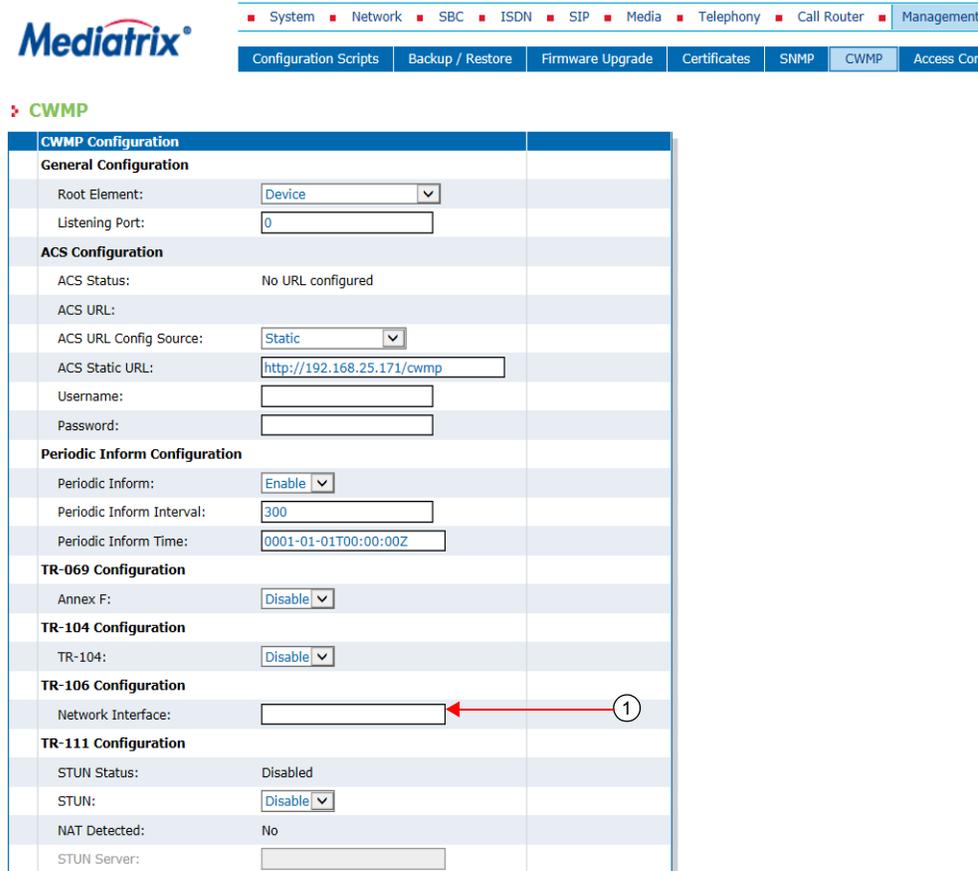
TR-106 Configuration

The *TR-106 Configuration* part allows you to set the network interface referred by the TR-106 LAN profile.

▶ To select a specific profile:

1. In the *TR-106 Configuration* part, set the *Network Interface* drop-down menu with the network interface referred by the TR-106 LAN profile.
If the menu is empty, the Mediatrix unit uses the network interface configured in [“Management Interface Configuration” on page 551](#). If this network interface is set to **All**, the Mediatrix unit uses the network interface used for contacting the ACS.

Figure 242: Management – CWMP Web Page, TR-106 Configuration Part



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

TR-111 Configuration

The *TR-111* part allows you to set the TR-111 parameters for connection request via NAT Gateway. The STUN Status field displays the status of the connection with the STUN server.

Table 423: STUN Server Status

Status	Description
Disabled	TR-111 is disabled.
Starting	Cwmp service is starting and no connection attempt have been made so far.
Connected	The Cwmp service is connected to the STUN server.
ErrorCannotResolve	The Cwmp service cannot connect with the STUN server because the FQDN cannot be resolved.
ErrorNotResponding	The Cwmp service cannot connect with the STUN server because the server is not responding.
ErrorOther	The Cwmp service cannot connect to the STUN server for unspecified reason or because no ACS URL is configured. See device and ACS logs.

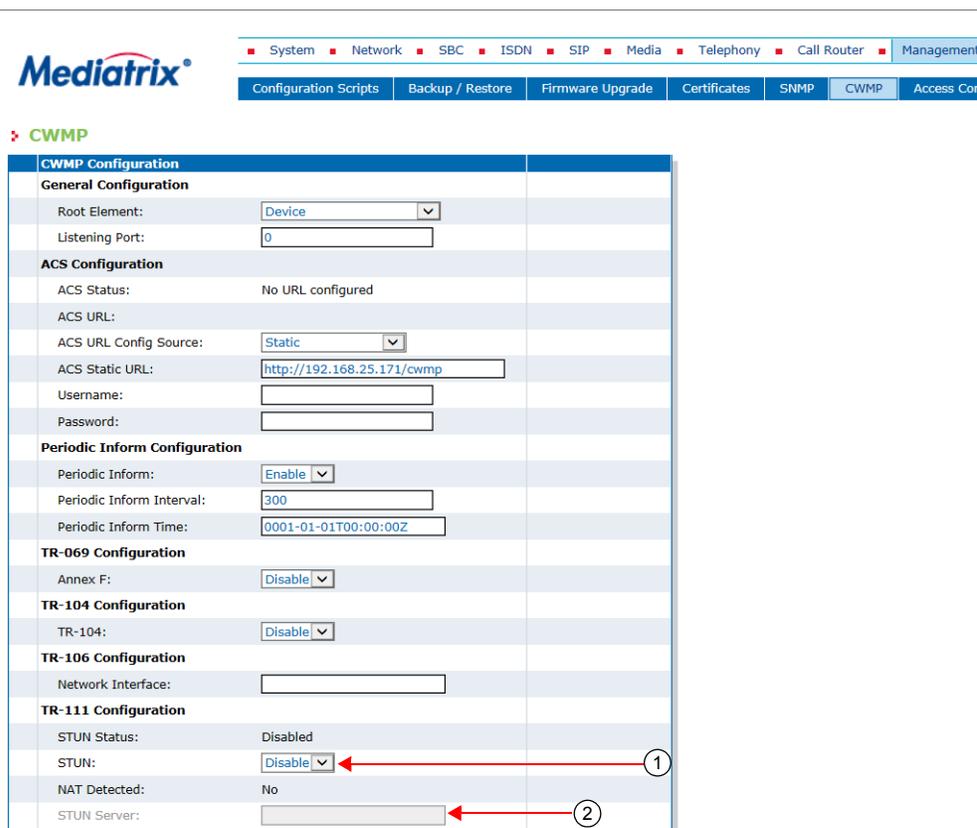
► To set TR-111 parameters:

1. In the *TR-111* part, enable or disable the use of STUN binding requests to discover the unit's external IP address and port in the *STUN Enable* drop-down menu. This also sets the *ManagementServer.UDPConnectionRequestAddress* value accordingly. The ACS can then send UDP connection requests to the unit at that IP address and port.

Table 424: STUN Parameters

Parameter	Description
Enable	Enables the use of STUN by the unit.
Disable	Disables the use of STUN by the unit.

Figure 243: Management – CWMP Web Page, TR-111 Configuration Part



When TR-111 STUN is enabled, the *NAT Detected* status parameter indicates whether or not the unit has detected the address and/or port mapping in use.

Table 425: NAT Detected Parameters

Parameter	Description
Yes	TR-111 STUN is enabled and the unit has detected the address and/or port mapping.
No	TR-111 STUN is disabled or the unit has not detected the address and/or port mapping.

2. If TR-111 STUN is enabled, set the host name or IP address of the STUN server for the unit to send Binding Requests in the *STUN Server* field.

If the *STUN server* field is empty and TR-111 STUN is enabled, the unit uses the address of the ACS extracted from the host portion of the ACS URL.

If the port is not specified or set to 0, the default STUN port (3478) is used.

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

Additional TR-111 Parameters

This section describes configuration that is available only in the MIB parameters of the Mediatix 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 STUN username and STUN keep alive parameters. These parameters are effective only if the *STUN Enable* drop-down menu is set to **Enable** (see “[TR-111 Configuration](#)” on page 526 for more details).

▶ To set additional TR-111 parameters:

1. In the *cwmpMIB*, set the period range, in seconds, at which STUN Binding Requests must be sent by the unit for the purpose of maintaining the STUN connection in the *tr111StunKeepAlivePeriod* variable.

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

```
cwmp.tr111StunKeepAlivePeriod="value"
```

The timeouts must be entered in the format 'minimum-maximum'.

The value must be less than or equal to 3600 seconds.



Note: The current implementation does not allow a range. The minimum and maximum values must be the same.

2. Set the value of the STUN username attribute to be used in Binding Requests in the *tr111StunUsername* variable.

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

```
cwmp.tr111StunUsername="value"
```

Transport HTTPS Cipher Suite Settings

This section describes configuration that is available only in the MIB parameters of the Mediatix 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 allowed cipher suites for the network security settings when using the HTTPS protocol to connect to the ACS. When the device initiates an HTTPS connection to the ACS, it will negotiate the cipher suite according to its configuration.

Table 426: Cipher Suites Configuration Parameters

Parameter	Description
CS1	<p>This is the default value and represents the cipher suites configuration prior to this variable being introduced. This should be changed if additional network security is required. This value includes the following cipher suites:</p> <ul style="list-style-type: none"> • TLS_DHE_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_DSS_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA • TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA • TLS_RSA_WITH_3DES_EDE_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_DSS_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_RC4_128_SHA • TLS_RSA_WITH_RC4_128_MD5 • TLS_DHE_RSA_WITH_DES_CBC_SHA • TLS_DHE_DSS_WITH_DES_CBC_SHA • TLS_RSA_WITH_DES_CBC_SHA • TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA • TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA • TLS_RSA_EXPORT_WITH_DES40_CBC_SHA • TLS_RSA_EXPORT_WITH_RC4_40_MD5
CS2	<p>This represents secure configuration using SHA-1. This value includes the following cipher suites:</p> <ul style="list-style-type: none"> • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_3DES_EDE_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

Table 426: Cipher Suites Configuration Parameters

Parameter	Description
CS3	<p>This represents the most secure configuration using SHA-2. Only the most secure cipher suites are allowed when using this value.</p> <ul style="list-style-type: none"> • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_128_GCM_SHA256

► **To set the HTTPS transport cipher suite configuration parameter:**

1. In the *cwmpMIB*, locate the *transportGroup* folder.
2. Set the HTTPS transport cipher suite configuration in the *TransportHttpsCipherSuite* variable.

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

```
cwmp.TransportHttpsCipherSuite="value"
```

where *Value* may be as follows:

Table 427: Cipher Suites Configuration Values

Value	Meaning
100	CS1
200	CS2
300	CS3

HTTPS Transport Tls Version Settings

Allows a user to define the allowed TLS versions for the network security settings when using the HTTPS protocol to connect to the ACS. When the device initiates an HTTPS connection to the ACS, it will negotiate the TLS version according to its configuration.

You can configure this parameter as follows:

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

Table 428: Tls Version Configuration Settings

Parameter	Description
SSLv3	Allow SSL version 3 and all TLS versions.
TLSv1	Allow TLS versions 1 and up.
TLSv1_1	Allow TLS versions 1.1 and up.
TLSv1_2	Allow TLS versions 1.2 and up.

The device will always send its highest supported TLS version in the ClientHello message.

The server will select the highest supported TLS version it supports from the ClientHello message.

The device will then validate that the selected version is allowed. If the version is not allowed the device will close the connection.

The default value is TLSV1.

► **To set the HTTPS Transport Tls Version configuration parameter:**

1. In the *cwmpMIB*, locate the *TransferGroup* folder.
2. Set the HTTPS Transport Tls Version configuration in the `TransportHTTPSTlsVersion` parameter.

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

```
Cwmp.TransportHTTPSTlsVersion = "value"
```

where value may be:

Table 429: Tls Version Configuration Values

Value	Meaning
100	SSLv3
200	TLSv1
300	TLSv1_1
400	TLSv1_2

Transport Certificate Validation

This section describes configuration that is available only in the MIB parameters of the Mediatrix 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 level of security to use when validating the server's certificate when connecting to the ACS using HTTPS. The following values are available:

Table 430: Transport Certificate Validation Parameters

Parameter	Description
NoValidation	Allows 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.

Table 430: Transport Certificate Validation Parameters (Continued)

Parameter	Description
HostName	Allows 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. This is the default setting.

► **To set the level of security to use when validating the server's certificate when connecting to the ACS using HTTPS:**

1. In the *cwmpMIB*, locate the *TransportGroup* folder.
2. Set the level of security to use in the `TransportCertificateValidation` variable.

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

```
cwmp.TransportCertificateValidation="value"
```

where *Value* may be as follows:

Table 431: Transport Certificate Validation Values

Value	Meaning
100	NoValidation
200	HostName

Allow Unauthenticated UDP Connection Requests

This section describes configuration that is available only in the MIB parameters of the Mediatix 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 CPE behaviour when receiving a UDP connection request message. The following values are available:

Table 432: Allow Unauthenticated UDP Connection Requests Parameters

Parameter	Description
Enable	Allows any UDP connection request without authentication. This behaviour goes against the UDP Connection Request described by TR-069 Amendment-2 specification.
Disable	Forces the authentication of a UDP connection request.

► **To set the CPE behaviour when receiving a UDP connection request message:**

1. In the *cwmpMIB*, set the behaviour when receiving a UDP connection request message in the `InteropAllowUnauthenticatedUDPConnectionRequests` variable.

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

```
cwmp.InteropAllowUnauthenticatedUDPConnectionRequests="value"
```

where *Value* may be as follows:

Table 433: Allow Unauthenticated UDP Connection Requests Values

Value	Meaning
0	disable

Table 433: Allow Unauthenticated UDP Connection Requests Values (Continued)

Value	Meaning
1	enable

Parameter Type Validation

This section describes configuration that is available only in the MIB parameters of the Mediatrix 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 parameter type validation when the ACS assigns a value to a parameter. The following values are available:

Table 434: Parameter Type Validation Parameters

Parameter	Description
Tolerant	The client target type is evaluated and conversion is done (if possible): i.e., string to boolean, string to int, string to unsigned int, string to datetime, etc.
Strict	The ACS and the client must have matching xsd:type otherwise the client rejects the parameter value.

▶ To set the parameter type validation:

1. In the *cwmpMIB*, set the parameter type validation when the ACS assigns a value to a parameter in the `interopParameterTypeValidation` variable.

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

```
cwmp.interopParameterTypeValidation="value"
```

where *Value* may be as follows:

Table 435: Parameter Type Validation Values

Value	Meaning
100	Tolerant
200	Strict

MAC Address Format

This section describes configuration that is available only in the MIB parameters of the Mediatrix 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 LAN MAC address display format. The following values are available:

Table 436: MAC Address Format Parameters

Parameter	Description
LowerCase	MAC address is in lower case format. Ex.: 0090f80d5b4a
UpperCaseWithColon	MAC address is in upper case format, each octet separated by a colon. Ex.: 00:90:F8:0D:5B:4A

► **To set the parameter type validation:**

1. In the *cwmpMIB*, set the MAC address format in the `interopMacAddressFormat` variable.

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

```
cwmp.interopMacAddressFormat="value"
```

where *Value* may be as follows:

Table 437: MAC Address Format Values

Value	Meaning
100	LowerCase
200	UpperCaseWithColon

ACS Access to the Local Log Table

This section describes configuration that is available only in the MIB parameters of the Mediatix 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 enable or disable access to the local log table from the ACS. The following values are available:

Table 438: Allow ACS Access to Local Log Table Parameters

Parameter	Description
Enable	Allow access to the local log table from the ACS.
Disable	Disallow access to the local log table from the ACS.

► **To set the access mode to the local log table from the ACS:**

1. In the *cwmpMIB*, set access to the local log table in the `N1mLocalLogLogEnable` variable.

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

```
cwmp.N1mLocalLogLogEnable="value"
```

where *Value* may be `Enable` or `Disable` (default)



Warning: Enabling access will require significant CPU resources and impact performance of your unit when notifications are sent frequently to the local log.

Supported TR-069 Methods and Parameters

For more details on TR-069 methods and parameters, request from our technical support team either the Tr-069 Data Model Support or TR-069 Notification Messages documents.

CHAPTER

52

Access Control Configuration

This chapter describes how to set the Access Control parameters of the Mediatrix unit.



Caution: The *Access Control* page is not accessible if you have the User or Observer access right. See “Users” on page 537 for more details.

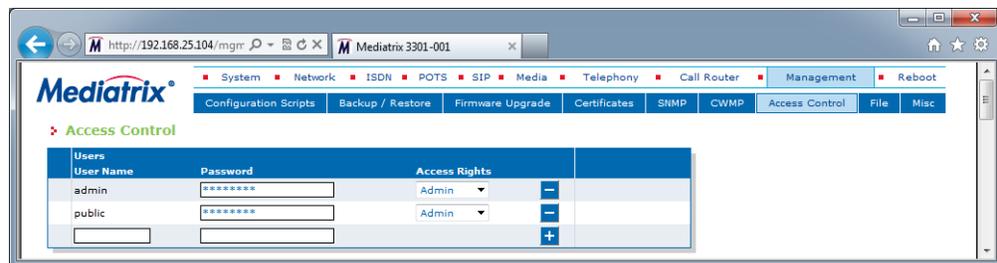
Users

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 244: 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 439: 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.

Table 439: Access Rights (Continued)

Access Right	Description
Observer	User is only allowed to read variables that are not passwords or secrets.

See “Access Rights Description” on page 541 for more details on the various operations allowed with each access right.

- 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 (For more details, refer to *Performing a Partial Reset* Technical Bulletin at <http://www.media5corp.com/documentation>).

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:**

- 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 440: 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 537 for more details).
Radius	Incoming authentication attempts are validated against the first responding Radius server configured in the <i>Radius Servers</i> section (“Radius Servers” on page 539). 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 537 for more details). Note: This type is not available for the SNMP interface.

Figure 245: Access Control – Services Access Control Type Section



- 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 441: Accounting Types

Type	Description
None	Accounting is disabled.
Radius	Accounting is done by the first responding Radius server configured in the <i>Radius Servers</i> section (“ Radius Servers ” on page 539).

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 (For more details refer to *Performing a Partial Reset* Technical Bulletin at <http://www.media5corp.com/documentation>).

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 Mediatrix unit’s Radius server settings do not support IPv6. See “[IPv4 vs. IPv6](#)” on page 49 for more details.

Radius Authentication occurs when the *Authentication Type* column of the *Services Access Control Type* section (“[Services Access Control Type](#)” on page 538) 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 538) 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 Mediatrix 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 246: 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 442: 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 541 for more 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 537](#) and [“Radius Servers” on page 539](#)).

The following table describes the various operations allowed with each access right.

Table 443: 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

53

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.

It also allows you to see the default and user-defined configuration presets for the ISDN, R2 CAS and E&M protocols. They differ depending on the Mediatrix unit you are using. Depending on your unit's profile, it may be possible that no preset files are available.



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.

► Deleting a file from the file management system:

1. In the web interface, click the *Management* link, then the *File* sub-link.
2. Click  located on the row of the file you wish to delete.

Figure 247: Management – File Web Page

File transfer through web browser is disabled because of unsecure HTTP access.
 • [Activate unsecure file transfer through web browser](#)

Internal files		
Name	Description	Size
conf/Gateway_Configuration.cfg	Configures the Sentinel with Gateway-style default settings.	10 KB
conf/main.exe	Mon Oct 19 10:26:57 2015	16.5 MB
conf/PRI_China-DSS1.cfg	China DSS1	3 KB
conf/PRI_Default.cfg	PRI default configuration	3 KB
conf/PRI_NorthAmerica-NI1.cfg	North America NI1	3 KB
conf/PRI_NorthAmerica-NI2.cfg	North America NI2	3 KB
sbc/rulesets/main.exe	Mon Oct 19 10:28:19 2015	16.5 MB
7 file(s)		Total: 33 MB / Max: 57.7 GB

Import File Through URL

Last Import File Result: Success

Import File Parameters

Destination:

URL:

Username:

Password:

Import File Through Web Browser

Path

► Importing a file through the web browser:

1. In the web interface, click the *Management* link, then the *File* sub-link.

Figure 248: Management – File Web Page

► **File**

File transfer through web browser is disabled because of unsecure HTTP access.
 • [Activate unsecure file transfer through web browser](#)

Internal files Name	Description	Size
conf/Gateway_Configuration.cfg	Configures the Sentinel with Gateway-style default settings.	10 KB
conf/main.exe	Mon Oct 19 10:26:57 2015	16.5 MB
conf/PRI_China-DSS1.cfg	China DSS1	3 KB
conf/PRI_Default.cfg	PRI default configuration	3 KB
conf/PRI_NorthAmerica-NI1.cfg	North America NI1	3 KB
conf/PRI_NorthAmerica-NI2.cfg	North America NI2	3 KB
sbc/rulesets/main.exe	Mon Oct 19 10:28:19 2015	16.5 MB
7 file(s)	Total: 33 MB / Max: 57.7 GB	

Import File Through URL

Last Import File Result: Success

Import File Parameters Import

Destination:

URL:

Username:

Password:

Import File Through Web Browser

Path File

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 *Import 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 *Import 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 **Import**.

► Importing a file through a URL:

You must use the http and https protocols to import larger files.

1. In the web interface, click the *Management* link, then the *File* sub-link.

Figure 249: Management – File Web Page

File

File transfer through web browser is disabled because of unsecure HTTP access.
 • [Activate unsecure file transfer through web browser](#)

Internal files		
Name	Description	Size
conf/Gateway_Configuration.cfg	Configures the Sentinel with Gateway-style default settings.	10 KB
conf/main.exe	Mon Oct 19 10:26:57 2015	16.5 MB
conf/PRI_China-DSS1.cfg	China DSS1	3 KB
conf/PRI_Default.cfg	PRI default configuration	3 KB
conf/PRI_NorthAmerica-NI1.cfg	North America NI1	3 KB
conf/PRI_NorthAmerica-NI2.cfg	North America NI2	3 KB
sbc/rulesets/main.exe	Mon Oct 19 10:28:19 2015	16.5 MB
7 file(s)	Total: 33 MB / Max: 57.7 GB	

Import File Through URL	
Last Import File Result:	Success
Import File Parameters	
Destination:	<input type="text" value="conf/"/> Import 6
URL:	<input type="text" value="http://www.myserver.com/myfile"/> 3
Username:	<input type="text" value="username"/> 4
Password:	<input type="password" value="*****"/> 5

Import File Through Web Browser	
Path	File
<input type="text"/>	<input type="text"/> Parcourir... Import

2. In the *Destination* field, enter the destination directory on the device where to save the file.
3. In the *URL* field, enter the URL of the file to download. For example: `http://www.myserver.com/myfile` or `ftp://myserver.com:69/myfolder/myfile`
4. If authentication is required by the remote file server, enter the user name in the *Username* field.
5. If authentication is required by the remote file server, enter the password in the *Password* field.

If you are currently using an unsecure HTTP access, the *Upload File Through URL* 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.

6. Click *Import*.

Partial Reset

When a partial reset is triggered, the user-defined presets are deleted.

Transfer Protocols

Table 444:

Name	Status
HTTP	Upload and download. Basic and digest authentication supported.
HTTPS	Upload and download. Requires a valid trusted certificate matching the remote server's certificate to be available through Cert. Basic and digest authentication supported.
TFTP	Download only.
FTP	Download only.

Security Certificates

This service makes use of security certificates as configured in the Certificate Manager service (Cert). It retrieves the certificates from Cert and then uses them as needed to authenticate remote servers.

HTTPS Transfer Settings

If the TLS server requests a certificate from the client (with a **CertificateRequest** message), the connection must be mutually authenticated by sending a message containing the client's certificate during the TLS handshake. The corresponding certificate is retrieved from the Cert.HostCertificateAssociation table.

When the transfer method is HTTPS, the negotiated network security settings depend on the CipherSuite configuration. The current cipher suite choices:

- ▶ CS1: This is the default value and represents the cipher suites configuration prior to this variable introduction. This should be changed if additional network security is required.
- ▶ CS2: This represents a secure configuration using SHA-1.
- ▶ CS3: This represents the most secure configuration using SHA-2. Only the most secure cipher suites are allowed when using this value.

HTTPS Transfer Cipher Suite Settings

This section describes configuration that is available only in the MIB parameters of the Mediatrix 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 allowed cipher suites for the network security settings when using the HTTPS transfer protocol. When the device initiates an HTTPS connection to a server it will negotiate the cipher suite according to its configuration.

Table 445: Cipher Suites Configuration Parameters

Parameter	Description
CS1	<p>This is the default value and represents the cipher suites configuration prior to this variable being introduced. This should be changed if additional network security is required. This value includes the following cipher suites:</p> <ul style="list-style-type: none"> • TLS_DHE_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_DSS_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA • TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA • TLS_RSA_WITH_3DES_EDE_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_DSS_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_RC4_128_SHA • TLS_RSA_WITH_RC4_128_MD5 • TLS_DHE_RSA_WITH_DES_CBC_SHA • TLS_DHE_DSS_WITH_DES_CBC_SHA • TLS_RSA_WITH_DES_CBC_SHA • TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA • TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA • TLS_RSA_EXPORT_WITH_DES40_CBC_SHA <p>TLS_RSA_EXPORT_WITH_RC4_40_MD5</p>
CS2	<p>This represents a secure configuration using SHA-1. This value includes the following cipher suites:</p> <ul style="list-style-type: none"> • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_3DES_EDE_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

Table 445: Cipher Suites Configuration Parameters

Parameter	Description
CS3	<p>This represents the most secure configuration using SHA-2. Only the most secure cipher suites are allowed when using this value.</p> <ul style="list-style-type: none"> • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256

► **To set the HTTPS transfer cipher suite configuration parameter:**

1. In the file *MIB*, locate the *transferGroup* folder.
2. Set the HTTPS transfer cipher suite configuration in the `TransferHttpsCiphersuite` variable.

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

```
file.TransferHttpsCiphersuite="value"
```

where *Value* may be as follows:

Table 446: Cipher Suites Configuration Values

Value	Meaning
100	CS1
200	CS2
300	CS3

HTTPS Transfer Tls Version Settings

You can define the allowed TLS version for the network security settings when using the HTTPS transfer protocol. When the device initiates an HTTPS connection to a server it will negotiate the TLS version according to its configuration.

You can configure this parameter as follows:

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

Table 447: Tls Version Configuration Settings

Parameter	Description
SSLv3	Allow SSL version 3 and all TLS versions.
TLSv1	Allow TLS versions 1 and up.
TLSv1_1	Allow TLS versions 1.1 and up.
TLSv1_2	Allow TLS versions 1.2 and up.

The device will always send its highest supported TLS version in the ClientHello message.

The server will select the highest supported TLS version it supports from the ClientHello message.

The device will then validate that the selected version is allowed. If the version is not allowed the device will close the connection.

the default value is TLSv1.

► **To set the HTTPS transfer Tls Version configuration parameter:**

1. In the *fileMIB*, locate the *TransferGroup* folder.
2. Set the HTTPS transfer Tls Version configuration in the `TransferHttpsTlsVersion` variable.

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

```
File.TransferHttpsTlsVersion = "value"
```

where value may be:

Table 448: Tls Version Configuration Values

Value	Meaning
100	SSLv3
200	TLSv1
300	TLSv1_1
400	TLSv1_2

CHAPTER 54

Miscellaneous

This chapter describes how to set various parameters used to manage the Mediatrix unit.

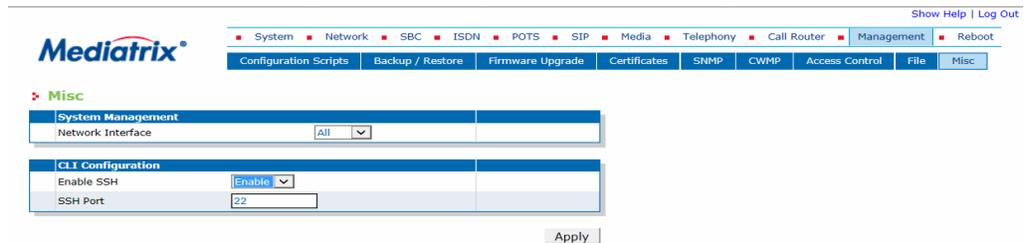
Management Interface Configuration

The *Miscellaneous* page allows you to specify which one of the existing network interfaces is used to manage the Mediatrix unit. It also allows you to enable or disable the access to the unit by SSH and through which port the SSH service should listen for incoming SSH requests.

► **To set the system management interface:**

1. In the web interface, got to *Management / Misc*

Figure 250: 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 Mediatrix unit.

The special value "All" means to bind all network interfaces.

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

► **To enable the access to the unit by SSH:**

1. In the Web Interface, go to *Management / Misc*.
2. In the *CLI Configuration* table, select *Enable* from the *Enable SSH* selection list.
3. In the *SSH Port* field, enter the port number on which the SSH port should listen to for SSH requests.
4. Click *Apply*.

► **To disable the access to the unit by SSH:**

1. In the Web Interface, go to *Management / Misc*.
2. In the *CLI Configuration* table, select *Disable* from the *Enable SSH* selection list.
3. Click *Apply*.

Activate Licence

The *Activate Licence* section allows you to activate a feature via an encrypted licence key. Once decrypted, the licence key will contain the feature to activate.

This functionality currently allows you to enable the TR-069 feature on units that are already deployed (see [“Chapter 51 - CWMP Configuration” on page 515](#) for more details on TR-069).

► **To use the Feature Activation:**

1. In the *Activate Licence* section of the *Misc* page, enter the licence key in the *Licence Key* field.

Figure 251: Management – Activate Licence Section



2. Click *Submit & Activate Now* to activate the feature.

Index

Numerics

802.1q, in local QoS [81](#)

A

AAA, service
 user access [4](#), [5](#)
 access control
 RADIUS [538](#)
 accounting type [538](#)
 authentication type [538](#)
 servers configuration [539](#)
 type [538](#)
 user
 access rights [537](#)
 add [537](#)
 delete [537](#)
 modify [537](#)
 access rights [537](#)
 description [541](#)
 RADIUS servers [540](#)
 accounting type, in RADIUS [538](#)
 ACK branch matching, in SIP [296](#)
 activate licence [552](#)
 A-Law [321](#)
 answering on caller ID, on FXO port [140](#)
 AOC-E support, ISDN interface [187](#)
 audience, intended [xix](#)
 authentication information [267](#)
 creating [268](#)
 deleting [270](#)
 editing [268](#)
 moving [270](#)
 authentication type, in RADIUS [538](#)
 auto cancel timeout, ISDN interface [182](#)
 auto-configuration
 E&M interfaces [224](#)
 ISDN interfaces [152](#)
 R2 interfaces [193](#)
 automatic
 call [387](#)
 auto-routing
 auto-routable parameter [489](#)
 enabling [487](#)
 introduction [487](#)
 SIP gateway [489](#)

B

base ports [365](#)
 bearer capabilities mapping, vs. codec [326](#)
 preferred codec choice [285](#)
 BRI interface configuration
 bypass connection [177](#)
 calling name max length [172](#)
 channel allocation strategy [171](#)
 clock mode [169](#)
 connection type [169](#)
 copy config to all interfaces [168](#)
 encoding scheme, fallback [170](#)

encoding scheme, preferred [170](#)
 endpoint type [168](#)
 exclusive B-channel selection [172](#)
 inband DTMF dialing [171](#)
 inband tone generation [171](#)
 maximum active calls [171](#)
 network location [170](#)
 overlap dialing [172](#)
 restart on startup [172](#)
 select interface [168](#)
 sending complete information [172](#)
 signal information element [171](#)
 signalling protocol [170](#)

bypass

activation [135](#)
 activation DTMF map [136](#)
 deactivation timeout [136](#)
 Bypass connection [1](#)
 bypass connection, in BRI [177](#)

C

call

automatic [387](#)
 completion
 CCBS [387](#)
 CCBS, using [390](#)
 CCNR [387](#)
 CCNR, using [390](#)
 emergency
 enabling [375](#)
 emergency override [409](#)
 forward
 on busy [377](#), [379](#)
 on no answer [380](#), [381](#)
 unconditional [382](#), [383](#)
 hold [403](#)
 direction attributes [289](#)
 putting on hold [394](#), [404](#)
 second [404](#), [405](#)
 transfer
 attended [391](#), [393](#)
 blind [391](#), [392](#)
 waiting [393](#)
 disabling [395](#)
 enabling [395](#)
 IMS-3GPP Communication Waiting [395](#)
 using [394](#)
 Call Detail Record [425](#)
 call failure timeout, on FXO port [144](#)
 call properties translation, in call routing
 built from [473](#)
 creating [472](#)
 defined [472](#)
 deleting [474](#)
 editing [472](#)
 modified property [473](#)
 moving [474](#)
 name [472](#)
 call rejection (drop) causes [478](#)
 call router
 call properties translation
 built from [473](#)
 creating [472](#)
 defined [472](#)
 deleting [474](#)

- editing [472](#)
 - modified property [473](#)
 - moving [474](#)
 - name [472](#)
- hairpinning [485](#)
- hunts
 - call rejection (drop) causes [478](#)
 - creating [475](#)
 - defined [475](#)
 - deleting [482](#)
 - destinations [476](#)
 - editing [475](#)
 - moving [482](#)
 - selection algorithm [476](#)
 - timeout [476](#)
- introduction [431](#)
- limitations [432](#)
- mappings
 - defined [455](#)
- mappings, expression
 - accessing [457](#)
 - criteria [458](#)
 - deleting [464](#)
 - moving [464](#)
 - sub mappings [463](#)
 - transformation [461](#)
- mappings, type
 - accessing [455](#)
 - input call property [456](#)
 - moving [464](#)
 - transformation [456](#)
- regular expression [432](#)
- routes
 - call property to compare [451](#)
 - creating [450](#)
 - defined [449](#)
 - deleting [455](#)
 - destination, of call [454](#)
 - editing [450](#)
 - expression to compare [452](#)
 - mapping, apply [453](#)
 - moving [454](#)
 - signalling, of call [453](#)
 - source to compare [451](#)
- routing type
 - Called Bearer Channel [438](#)
 - Called E164 [435](#)
 - Called Host [436](#)
 - Called Name [435](#)
 - Called NPI [435](#)
 - Called Phone Context [438](#)
 - Called SIP username [438](#)
 - Called TON [435](#)
 - Called URI [436](#)
 - Calling Bearer Channel [438](#)
 - Calling E164 [435](#)
 - Calling Host [436](#)
 - Calling ITC [436](#)
 - Calling Name [435](#)
 - Calling NPI [435](#)
 - Calling Phone Context [438](#)
 - Calling PI [436](#)
 - Calling SI [436](#)
 - Calling SIP username [438](#)
 - Calling TON [435](#)
 - Calling Uri [436](#)
- Date/Time [437](#)
- Last Diverting E.164 [438](#)
- Last Diverting Number Presentation [439](#)
- Last Diverting Party Number Type [438](#)
- Last Diverting Private Type of Number [439](#)
- Last Diverting Public Type of Number [439](#)
- Last Diverting Reason [438](#)
- Original Diverting E.164 [438](#)
- Original Diverting Number Presentation [439](#)
- Original Diverting Party Number Type [438](#)
- Original Diverting Private Type of Number [439](#)
- Original Diverting Public Type of Number [439](#)
- Original Diverting Reason [438](#)
- special tags [440](#)
- signalling properties
 - 180 with SDP [466](#)
 - 183 without SDP [467](#)
 - call properties translation [468](#)
 - creating [465](#)
 - defined [465](#)
 - deleting [469](#)
 - destination host [466](#)
 - early connect [466](#)
 - early disconnect [466](#)
 - editing [465](#)
 - moving [469](#)
 - name [466](#)
 - privacy level [467](#)
 - SIP headers translation [468](#)
- SIP headers translation
 - built from [470](#)
 - creating [469](#)
 - defined [469](#)
 - deleting [471](#)
 - editing [469](#)
 - modified header [470](#)
 - moving [471](#)
 - name [470](#)
- SIP redirects
 - creating [483](#)
 - defined [483](#)
 - deleting [484](#)
 - editing [483](#)
 - moving [484](#)
- status information [448](#)
- call waiting
 - private number for SIP INFO [288](#)
- Called Bearer Channel, routing type [438](#)
- Called E164, routing type [435](#)
- Called Host, routing type [436](#)
- Called Name, routing type [435](#)
- Called NPI, routing type [435](#)
- Called Phone Context, routing type [438](#)
- Called SIP username, routing type [438](#)
- Called TON, routing type [435](#)
- Called URI, routing type [436](#)
- caller ID
 - customization, in POTS [128](#)
 - DTMF signalling [130](#)
 - FSK generation [130](#)
 - generation [130](#)
- Calling Bearer Channel, routing type [438](#)
- Calling E164, routing type [435](#)
- Calling Host, routing type [436](#)
- Calling ITC, routing type [436](#)
- calling name max length, ISDN interface

- BRI configuration [172](#)
- PRI configuration [162](#)
- Calling Name, routing type [435](#)
- Calling NPI, routing type [435](#)
- Calling Phone Context, routing type [438](#)
- Calling PI, routing type [436](#)
- Calling SI, routing type [436](#)
- Calling SIP username, routing type [438](#)
- Calling TON, routing type [435](#)
- Calling Uri, routing type [436](#)
- CAS. *see* [R2 configuration](#)
- CCBS
 - setting up [387](#)
 - using [390](#)
- CCNR
 - setting up [387](#)
 - using [390](#)
- CDR (Call Detail Record) [425](#)
- CED tone detection [364](#)
 - behaviour [365](#)
- certificate
 - validation, in TLS [286](#)
- certificates
 - deleting [504](#)
 - transferring [507](#)
 - upload through web browser [506](#)
- channel allocation strategy
 - E&M interface, configuration [228](#)
 - ISDN interface
 - BRI configuration [171](#)
 - PRI configuration [161](#)
 - R2 interface, configuration [196](#)
- channel range
 - E&M interface, configuration [227](#)
 - ISDN interface
 - PRI configuration [160](#)
 - R2 interface, configuration [196](#)
- Clear Channel
 - defined [323](#)
 - enabling
 - for data transmission [335](#)
 - for voice transmission [335](#)
 - packetization time [335](#)
 - payload type [335](#)
 - priority
 - for data codecs [335](#)
 - for voice codecs [335](#)
- clear channel fax
 - call flow [339](#)
 - limitation [339](#)
- Clear Mode
 - defined [323](#)
 - enabling
 - for data transmission [334](#)
 - for voice transmission [334](#)
 - packetization time [334](#)
 - payload type [334](#)
 - priority
 - for data codecs [334](#)
 - for voice codecs [334](#)
- CLI
 - accessing via Console port [8](#)
 - accessing via SSH [10](#)
 - accessing via Telnet [9](#)
 - contexts [11](#)
 - defined [7](#)
- CLIP, ISDN interface [184](#)
- CLIR, ISDN interface [184](#)
 - override [185](#)
- clock mode
 - E&M interface, configuration [226](#)
 - ISDN interface
 - BRI configuration [169](#)
 - PRI configuration [158](#)
 - R2 interface, configuration [195](#)
- CNG tone detection [364](#), [424](#)
- codec
 - bearer capabilities mapping [326](#)
 - preferred codec choice [285](#)
- Clear Channel
 - defined [323](#)
 - enabling
 - for data transmission [335](#)
 - for voice transmission [335](#)
 - packetization time [335](#)
 - payload type [335](#)
 - priority
 - for data codecs [335](#)
 - for voice codecs [335](#)
- Clear Mode
 - defined [323](#)
 - enabling
 - for data transmission [334](#)
 - for voice transmission [334](#)
 - packetization time [334](#)
 - payload type [334](#)
 - priority
 - for data codecs [334](#)
 - for voice codecs [334](#)
- G.711
 - defined [321](#)
 - enabling
 - for data transmission [328](#)
 - for voice transmission [328](#)
 - packetization time [328](#)
 - priority
 - for data transmission [328](#)
 - for voice transmission [328](#)
- G.723
 - bit rate [330](#)
 - defined [322](#)
 - enabling for voice transmission [330](#)
 - packetization time [331](#)
 - priority for voice codecs [330](#)
- G.726
 - defined [322](#)
 - enabling
 - for data transmission [331](#)
 - for voice transmission [331](#)
 - packetization time [332](#)
 - payload type [332](#)
 - priority
 - for data transmission [331](#)
 - for voice transmission [331](#)
- G.729
 - defined [322](#)
 - enabling for voice transmission [333](#)
 - packetization time [333](#)
 - priority for voice codecs [333](#)
 - voice activity detection [334](#)
- T.38
 - defined [324](#)

- enabling [340](#)
- number of redundancy packets [340](#)
- priority [340](#)
- X-CCD Clear Channel
 - defined [324](#)
 - enabling
 - for data transmission [337](#)
 - for voice transmission [337](#)
 - packetization time [337](#)
 - payload type [337](#)
 - priority
 - for data codecs [337](#)
 - for voice codecs [337](#)
- COLP, ISDN interface [185](#)
- COLR, ISDN interface [185](#)
 - override [186](#)
- conference call
 - limitation [397](#)
- configuration backup image
 - backing up [497](#)
 - decryption [497](#)
 - location path [497](#)
 - privacy key [497](#)
 - restoring [497](#)
 - server, IP address [497](#)
 - transfer protocols [497](#)
- connection type, ISDN interface
 - BRI configuration [169](#)
- Console port
 - accessing CLI via [8](#)
- contact domain, in SIP [256](#)
- Content-type, unsupported [299](#)
- Country [134](#)
- country selection, R2 interface [197](#)
- country-specific parameters
 - CNG tone detection [424](#)
 - country [419](#)
 - custom tone configuration [411](#)
 - dialing settings [422](#)
 - user gain
 - input [421](#)
 - output [421](#)
- custom tones, configuring [411](#)
- CWMP
 - ACS parameters [517](#)
 - Allow Unauthenticated UDP Connection Requests [532](#)
 - general configuration [516](#)
 - parameter type validation [533](#), [534](#)
 - periodic inform parameters [521](#)
 - profile creation [525](#)
 - TR-069 configuration [523](#)
 - TR-104 configuration [524](#)
 - TR-106 configuration [525](#)
 - TR-111 [526](#)

D

- Date/Time, routing type [437](#)
- decryption
 - configuration backup image [497](#)
- default gateway
 - client, setting [55](#)
 - server, in embedded DHCP server [116](#)
- default router. see *default gateway*
- delayed hot line [401](#)
- detection custom repetition, on FXO port [146](#)

- DHCP connection type [64](#)
- DHCP server
 - configuring [73](#)
 - embedded
 - default gateway [116](#)
 - defined [113](#)
 - DNS servers [117](#)
 - domain name server [116](#)
 - lease time [115](#)
 - leases [120](#)
 - NBNS servers [119](#)
 - NTP servers [118](#)
 - subnets, managing [115](#)
- DHCPv4 classless static route option [95](#)
- diagnostic traces, enabling [35](#)
 - PCM capture [38](#)
- dial tone detection mode, on FXO port [139](#)
- dial tone detection timeout, on FXO port [140](#)
- dialing
 - settings
 - delay between MFR1s [423](#)
 - DTMF duration value [423](#)
 - inter-digit dial delay [423](#)
- Differentiated Services (DS) Field, in local QoS [79](#)
- direct IP address
 - call [402](#)
- direction attribute "sendonly" [285](#), [291](#)
- direction attributes, in SIP [289](#)
- disabling endpoints [31](#)
- DNS
 - client [56](#)
 - server, in embedded DHCP server [117](#)
 - supported queries [315](#)
- DNS SRV
 - record lock, in SIP [294](#)
- document
 - conventions [xx](#), [xxi](#)
 - intended audience [xix](#)
- domain name
 - server, in embedded DHCP server [116](#)
- DTMF
 - base ports [365](#)
 - detection [360](#)
 - duration value [423](#)
 - machine detection
 - CED tone detection [364](#)
 - CED tone detection, behaviour [365](#)
 - CNG tone detection [364](#)
 - V.21 modulation detection [365](#)
 - out-of-band [359](#)
 - signalling, caller ID [130](#)
 - transport type
 - over the SIP protocol [360](#)
- DTMF map
 - allowed [373](#)
 - defined
 - # and * characters [371](#)
 - combining two expressions [370](#)
 - special characters [370](#)
 - timer [371](#)
 - using [370](#)
 - validating [371](#)
 - definition [369](#)
 - general parameters [372](#)
 - refused [375](#)

E

E&M

- partial reset [226](#)

E&M configuration

- auto-configuration [224](#)
- channel allocation strategy [228](#)
- channel range [227](#)
- clock mode [226](#)
- digit timers [234](#)
- encoding scheme [228](#)
- encoding scheme, preferred [228](#)
- introduction [223](#)
- line coding [227](#)
- line framing [227](#)
- link timers [236](#)
- maximum active calls [228](#)
- preset [225](#)
- PRI statistics [239](#)
- selecting signalling protocol [223](#)
- signalling [229](#)
 - B bit setting [230](#)
 - C bit setting [230](#)
 - D bit setting [230](#)
 - override default settings [230](#)
- timers [232](#)
- tones [237](#)

emergency call

- enabling [375](#)

enabling endpoints [31](#)

encoding scheme

- E&M interface, configuration [228](#)
- R2 interface, configuration [197](#)

encoding scheme, ISDN interface

- fallback
 - BRI configuration [170](#)
 - PRI configuration [160](#)
- preferred
 - BRI configuration [170](#)
 - PRI configuration [160](#)

encoding scheme, preferred

- E&M interface, configuration [228](#)
- R2 interface, configuration [197](#)

endpoint

- administration [32](#)
- locking/unlocking [31](#)
- unit shutting down behaviour [33](#)
- unregistered, behaviour when [262](#)

endpoint services

- automatic call [387](#)
- call completion
 - CCBS [387](#)
 - CCNR [387](#)
- call forward
 - on busy [377](#)
 - on no answer [380](#)
 - unconditional [382](#)
- call transfer
 - attended transfer [391](#)
 - blind transfer [391](#)
- call waiting [393](#)
- conference call [397](#)
 - limitation [397](#)
- direct IP address call [402](#)
- emergency call override [409](#)
- hold [403](#)

- direction attributes [289](#)

- hook-flash processing [386](#)

- second call [404](#)

endpoint type, ISDN interface

- BRI configuration [168](#)
- PRI configuration [157](#)

error causes mapping, setting [302](#)

- cause to SIP [306](#)
- SIP to cause [304](#)

Ethernet connection

- setting speed of [75](#)

Ethernet, link configuration [72](#)event handling, in SIP [315](#)

events

- monitoring parameters
 - monitoring parameters, in events [41](#)
- notification
 - notification events [39](#)
- rule
 - deleting [41](#)

exclusive B-channel selection, ISDN interface

- BRI configuration [172](#)
- PRI configuration [162](#)

F

facility ISDN services

- enabling [183](#)

fax

- call waiting tone, disabling [395](#)

- calling tone detection, enabling [424](#)

clear channel

- call flow [339](#)
- limitation [339](#)

T.38

- defined [324](#)
- enabling [340](#)
- number of redundancy packets [340](#)
- priority [340](#)
- user gain vs communication quality [421](#)

file manager [543](#)

firewall, local

- default policy [85](#)
- disabling [89](#)
- partial reset [85](#)
- rule, creating [86](#)
- rule, deleting [89](#)
- rule, editing [86](#)
- rule, moving [88](#)
- status information [88](#)

firewall, network

- default policy [99](#)
- disabling [103](#)
- rule, creating [100](#)
- rule, deleting [103](#)
- rule, editing [100](#)
- rule, moving [103](#)
- status information [103](#)

flash hook detection range [134](#)force end of call on call failure, on FXO port [144](#)forced end of call on silence detection mode, on FXO port [144](#)forced end of call on tone detection mode, on FXO port [145](#)forked provisional responses behaviour, in SIP [311](#)FSK generation, caller ID [130](#)

FXO configuration

- answering on caller ID [140](#)

- call failure timeout [144](#)
- detection custom repetition [146](#)
- dial tone detection mode [139](#)
- dial tone detection timeout [140](#)
- force end of call on call failure [144](#)
- forced end of call on silence detection mode [144](#)
- forced end of call on tone detection mode [145](#)
- link state verification [143](#)
- link state verification timeout [144](#)
- not allowed behavior [142](#)
- pre dial delay [139](#)
- silence detection timeout [145](#)
- tone detection custom cadence [146](#)
- tone detection custom frequency [146](#)
- wait before answering delay [140](#)
- wait for callee to answer [141](#)

FXS

- auto cancel timeout [131](#)
- bypass
 - activation [135](#)
 - activation DTMF map [136](#)
 - deactivation timeout [136](#)
- country override
 - flash hook detection range [134](#)
 - loop current [134](#)
- disconnect delay [131](#)
- inband ringback [132](#)
- line supervision mode [131](#)
- override country customization [133](#)
- power drop on disconnect duration [132](#)
- service activation [132](#)
- shutdown behavior [132](#)

G

G.711

- defined [321](#)
- enabling
 - for data transmission [328](#)
 - for voice transmission [328](#)
- packetization time [328](#)
- priority
 - for data transmission [328](#)
 - for voice transmission [328](#)

G.723

- bit rate [330](#)
- defined [322](#)
- enabling for voice transmission [330](#)
- packetization time [331](#)
- priority for voice codecs [330](#)

G.726

- defined [322](#)
- enabling
 - for data transmission [331](#)
 - for voice transmission [331](#)
- packetization time [332](#)
- payload type [332](#)
- priority
 - for data transmission [331](#)
 - for voice transmission [331](#)

G.729

- defined [322](#)
- enabling for voice transmission [333](#)
- packetization time [333](#)
- priority for voice codecs [333](#)
- voice activity detection [334](#)

- gateways, multiple SIP
 - adding [243](#)
 - keep alive destinations [253](#)
 - messaging servers [250](#)
 - proxy servers [251](#)
 - registrar servers [249](#)
 - removing [243](#)
- group port management [31](#)

H

- hairpinning [485](#)
- hardware configuration
 - PRI interface
 - line type [192](#), [224](#)
 - signaling [192](#), [224](#)
- header, SIP user agent
 - sending [265](#)
- hold, putting a call on [394](#), [403](#), [404](#)
 - direction attributes [289](#)
- home domain proxy override [313](#)
- hook-flash processing [386](#)
- HTTP
 - remote server, configuring [415](#)
- hunts, in call routing
 - call rejection (drop) causes [478](#)
 - creating [475](#)
 - defined [475](#)
 - deleting [482](#)
 - destinations [476](#)
 - editing [475](#)
 - moving [482](#)
 - selection algorithm [476](#)
 - timeout [476](#)

I

- IEEE 802.1q, in local QoS [81](#)
- IMS-3GPP Communication Waiting [395](#)
- inband DTMF dialing, ISDN interface
 - BRI configuration [171](#)
 - PRI configuration [161](#)
- inband tone generation, ISDN interface
 - BRI configuration [171](#)
 - PRI configuration [161](#)
- InformationFollowing operation, ISDN interface
 - PRI configuration [166](#)
- intended audience [xix](#)
- inter-digit dial delay [423](#)
- IP address
 - configuration backup server [497](#)
 - LAN, setting for [64](#)
 - messaging server host [249](#)
 - reserving in network server [63](#)
 - SIP outbound proxy [249](#)
 - SIP proxy [249](#)
 - SIP registrar [249](#)
 - syslog daemon [35](#)
 - unit, setting for [64](#)
 - vocal identification of [129](#)
- IP address call [402](#)
- IP routing
 - DHCPv4 classless static route option [95](#)
 - IPv4 forwarding [91](#)
 - rule, creating [92](#)
 - rule, deleting [93](#)

- rule, editing [92](#)
- rule, moving [93](#)
- static IPv4 routes [94](#)
- status information [93, 94](#)
- IPv4
 - forwarding [91](#)
- IPv4, static routes [94](#)
- ISDN
 - partial reset [153, 545](#)
- ISDN configuration
 - auto cancel timeout [182](#)
 - auto-configuration [152](#)
 - BRI interface
 - bypass connection [177](#)
 - calling name max length [172](#)
 - channel allocation strategy [171](#)
 - clock mode [169](#)
 - connection type [169](#)
 - copy config to all interfaces [168](#)
 - encoding scheme, fallback [170](#)
 - encoding scheme, preferred [170](#)
 - endpoint type [168](#)
 - exclusive B-channel selection [172](#)
 - inband DTMF dialing [171](#)
 - inband tone generation [171](#)
 - maximum active calls [171](#)
 - network location [170](#)
 - overlap dialing [172](#)
 - restart on startup [172](#)
 - select interface [168](#)
 - sending complete information [172](#)
 - signal information element [171](#)
 - signalling protocol [170](#)
 - interop parameters
 - copy config to all interfaces [178, 182, 183](#)
 - maximum facility waiting delay [179](#)
 - Progress Indicator in Alerting [179](#)
 - Progress Indicator in Call Proceeding [178](#)
 - Progress Indicator in Connect [179](#)
 - Progress Indicator in Progress [179](#)
 - Progress Indicator in Setup [178](#)
 - Progress Indicator in Setup ACK [178](#)
 - select interface [178](#)
 - introduction [149](#)
 - Layer 1 Timer 3 [182](#)
 - preset [153](#)
 - PRI interface
 - calling name max length [162](#)
 - channel allocation strategy [161](#)
 - channel range [160](#)
 - clock mode [158](#)
 - copy config to all interfaces [157, 490](#)
 - encoding scheme, fallback [160](#)
 - encoding scheme, preferred [160](#)
 - endpoint type [157](#)
 - exclusive B-channel selection [162](#)
 - inband DTMF dialing [161](#)
 - inband tone generation [161](#)
 - InformationFollowing operation [166](#)
 - line coding [159](#)
 - line framing [159](#)
 - line type [152](#)
 - link establishment [162, 172](#)
 - maximum active calls [161](#)
 - network location [159](#)
 - overlap dialing [162](#)
 - restart on startup [162](#)
 - select interface [157](#)
 - sending complete information [162](#)
 - signal information element [161](#)
 - signalling protocol [159](#)
 - statistics [153](#)
 - services
 - AOC-E support [187](#)
 - CLIP [184](#)
 - CLIR [184](#)
 - CLIR override [185](#)
 - COLP [185](#)
 - COLR [185](#)
 - COLR override [186](#)
 - facility services, enabling [183](#)
 - Maintenance Service Call Termination [186](#)
 - MSN [188](#)
 - select interface [183](#)
 - supplementary services, enabling [183](#)

J

- jitter buffer protection [355](#)

K

- keep alive, in SIP [252](#)

L

- Lan1, network interface [64](#)
- Last Diverting E.164, routing type [438](#)
- Last Diverting Number Presentation, routing type [439](#)
- Last Diverting Party Number Type, routing type [438](#)
- Last Diverting Private Type of Number, routing type [439](#)
- Last Diverting Public Type of Number, routing type [439](#)
- Last Diverting Reason, routing type [438](#)
- Layer 1 Timer 3, ISDN interface [182](#)
- lease times in embedded DHCP server [115](#)
- leases in embedded DHCP server [120](#)
- licence, activate [552](#)
- line coding
 - E&M interface, configuration [227](#)
 - ISDN interface
 - PRI configuration [159](#)
 - R2 interface, configuration [196](#)
- line framing
 - E&M interface, configuration [227](#)
 - ISDN interface
 - PRI configuration [159](#)
 - R2 interface, configuration [196](#)
- line signalling protocol
 - R2 interface, configuration [197](#)
- line type
 - PRI configuration [152, 192, 224](#)
- link establishment, ISDN interface
 - PRI configuration [162, 172](#)
- link state verification timeout, on FXO port [144](#)
- link state verification, on FXO port [143](#)
- LLDP configuration, network interface [71](#)
- local ring behaviour, in SIP [292](#)
- locking endpoints [31](#)
- loop current [134](#)

M

MAC address [63](#)
 vocal identification of [129](#)

machine detection
 CED tone detection [364](#)
 CED tone detection, behaviour [365](#)
 CNG tone detection [364](#)
 V.21 modulation detection [365](#)

Maintenance Service Call Termination, ISDN interface [186](#)

management interface
 selecting [551](#)

mappings, in call routing
 defined [455](#)
 expression
 accessing [457](#)
 criteria [458](#)
 deleting [464](#)
 moving [464](#)
 sub mappings [463](#)
 transformation [461](#)

type
 accessing [455](#)
 input call property [456](#)
 moving [464](#)
 transformation [456](#)

Max-Forwards header, in SIP [288](#)

maximum active calls
 E&M interface, configuration [228](#)
 ISDN interface
 BRI configuration [171](#)
 PRI configuration [161](#)
 R2 interface, configuration [197](#)

maximum facility waiting delay, ISDN interface [179](#)

message waiting indicator [405](#)
 visual type [407](#)

messaging subscription, in SIP [317](#)

MFR1
 dialling delay between [423](#)

MSN, ISDN interface [188](#)

MTU
 configuring [72](#)

Mu (μ)-Law [321](#)

music on hold
 configuring [415](#)
 remote server
 HTTP server, configuring [415](#)
 TFTP server, configuring [415](#)

N

NAT
 disabling [112](#)
 partial reset [105](#)

NAT, destination
 rule, creating [109](#)
 rule, deleting [112](#)
 rule, editing [109](#)
 rule, moving [112](#)

NAT, source
 rule, creating [105](#)
 rule, deleting [112](#)
 rule, editing [105](#)
 rule, moving [112](#)

NBNS server, in embedded DHCP server [119](#)

network interfaces

connection type [64](#)
 defining [64](#)

DHCP client identifier presentation
 DHCP
 client identifier presentation [70](#)

Ethernet link configuration [72](#)

Lan1 [64](#)

LLDP configuration [71](#)
 partial reset [63](#)

PPP configuration [69](#)
 PPP negotiation [70](#)

priority [68](#)

Rescue [64](#)

Uplink [64](#)

network location, ISDN interface
 BRI configuration [170](#)
 PRI configuration [159](#)

network parameters
 automatic configuration interface [53](#)
 default gateway client [55](#)
 DNS client [56](#)
 host [53](#)
 SNTP client [57](#)
 syslocation, updating [61](#)
 sysname, updating [61](#)
 time zone, defining custom [58](#)

network traffic control
 in QoS [82](#)

not allowed behavior, on FXO port [142](#)

NTP server, in embedded DHCP server [118](#)

O

Offer/Answer model [280](#), [283](#), [287](#)

Original Diverting E.164, routing type [438](#)

Original Diverting Number Presentation, routing type [439](#)

Original Diverting Party Number Type, routing type [438](#)

Original Diverting Private Type of Number, routing type [439](#)

Original Diverting Public Type of Number, routing type [439](#)

Original Diverting Reason, routing type [438](#)

outbound proxy server, configuring [248](#)

out-of-band DTMF [359](#)

overlap dialing, ISDN interface
 BRI configuration [172](#)
 PRI configuration [162](#)

P

packetization time
 Clear Channel [335](#)
 Clear Mode [334](#)
 G.711 [328](#)
 G.723 [331](#)
 G.726 [332](#)
 G.729 [333](#)
 X-CCD Clear Channel [337](#)

partial reset
 E&M preset [226](#)
 ISDN preset [153](#), [545](#)
 local firewall service [85](#)
 NAT service [105](#)
 network interfaces [63](#)
 R2 preset [194](#)
 RADIUS authentication [539](#)
 SNMP [509](#), [513](#)
 user password [538](#)

- password
 - modify [543, 551](#)
 - payload type
 - Clear Channel [335](#)
 - Clear Mode [334](#)
 - G.726 [332](#)
 - using the one found in answer [363](#)
 - X-CCD Clear Channel [337](#)
 - PCM capture [38](#)
 - penalty box, in SIP [301](#)
 - port number
 - configuration backup server [497](#)
 - messaging server host [249](#)
 - SIP outbound proxy [249](#)
 - SIP proxy [249](#)
 - SIP registrar [249](#)
 - POTS
 - auto cancel timeout [131](#)
 - caller ID customization [128](#)
 - FXO configuration
 - answering on caller ID [140](#)
 - call failure timeout [144](#)
 - detection custom repetition [146](#)
 - dial tone detection mode [139](#)
 - dial tone detection timeout [140](#)
 - force end of call on call failure [144](#)
 - forced end of call on silence detection mode [144](#)
 - forced end of call on tone detection mode [145](#)
 - link state verification [143](#)
 - link state verification timeout [144](#)
 - not allowed behavior [142](#)
 - pre dial delay [139](#)
 - silence detection timeout [145](#)
 - tone detection custom cadence [146](#)
 - tone detection custom frequency [146](#)
 - wait before answering delay [140](#)
 - wait for callee to answer [141](#)
 - FXS bypass
 - activation [135](#)
 - activation DTMF map [136](#)
 - deactivation timeout [136](#)
 - FXS Country Override Flash Hook Detection Range [134](#)
 - FXS Country Override Loop Current [134](#)
 - FXS Disconnect Delay [131](#)
 - FXS Inband Ringback [132](#)
 - FXS Line Supervision Mode [131](#)
 - FXS Override Country Customization [133](#)
 - FXS power drop on disconnect duration [132](#)
 - FXS service activation [132](#)
 - FXS shutdown behavior [132](#)
 - status information [127](#)
 - PPP configuration, network interface [69](#)
 - PPP negotiation [70](#)
 - PPPoE connection type [64](#)
 - PRACK, support [310](#)
 - pre dial delay, on FXO port [139](#)
 - preset
 - E&M interfaces [225](#)
 - ISDN interfaces [153](#)
 - R2 interfaces [193](#)
 - PRI interface configuration
 - calling name max length [162](#)
 - channel allocation strategy [161](#)
 - channel range [160](#)
 - clock mode [158](#)
 - copy config to all interfaces [157, 490](#)
 - encoding scheme, fallback [160](#)
 - encoding scheme, preferred [160](#)
 - endpoint type [157](#)
 - exclusive B-channel selection [162](#)
 - inband DTMF dialing [161](#)
 - inband tone generation [161](#)
 - InformationFollowing operation [166](#)
 - line coding [159](#)
 - line framing [159](#)
 - line type [152, 192, 224](#)
 - link establishment [162, 172](#)
 - maximum active calls [161](#)
 - network location [159](#)
 - overlap dialing [162](#)
 - restart on startup [162](#)
 - select interface [157](#)
 - sending complete information [162](#)
 - signal information element [161](#)
 - signaling [192, 224](#)
 - signalling protocol [159](#)
 - priority, of network interfaces [68](#)
 - privacy key
 - configuration backup image [497](#)
 - privacy level of calls [467](#)
 - Progress Indicator in Alerting, ISDN interface [179](#)
 - Progress Indicator in Call Proceeding, ISDN interface [178](#)
 - Progress Indicator in Connect, ISDN interface [179](#)
 - Progress Indicator in Progress, ISDN interface [179](#)
 - Progress Indicator in Setup ACK, ISDN interface [178](#)
 - Progress Indicator in Setup, ISDN interface [178](#)
 - proxy server
 - SNMP, configuring via
 - override [294](#)
 - proxy server, configuring [248](#)
- ## Q
- QoS
 - network traffic control [82](#)
 - VLAN [81](#)
 - QoS, local
 - 802.1q [81](#)
 - Differentiated Services (DS) Field [79](#)
 - QSIG
 - signalling protocol [159, 170](#)
- ## R
- R2
 - partial reset [194](#)
 - R2 configuration
 - auto-configuration [193](#)
 - channel allocation strategy [196](#)
 - channel range [196](#)
 - clock mode [195](#)
 - country selection [197](#)
 - encoding scheme [197](#)
 - encoding scheme, preferred [197](#)
 - introduction [191](#)
 - line coding [196](#)
 - line framing [196](#)
 - line signalling protocol [197](#)
 - maximum active calls [197](#)
 - preset [193](#)
 - PRI statistics [218](#)
 - R2 digit timers [207](#)

- R2 link timers [209](#)
 - R2 signaling [198](#)
 - C bit setting [199](#)
 - D bit setting [199](#)
 - override default country settings [199](#)
 - R2 timers [202](#)
 - R2 tones backward groups [214](#)
 - R2 tones forward groups [213](#), [238](#)
 - register signalling protocol [197](#)
 - selecting R2 signaling protocol [192](#)
 - RADIUS
 - accounting type [538](#)
 - authentication type [538](#)
 - servers access rights [540](#)
 - servers configuration [539](#)
 - Reason header [309](#)
 - Referred-by header [309](#)
 - register home domain override, in SIP [294](#)
 - register signalling protocol
 - R2 interface [197](#)
 - registrar server, configuring [248](#)
 - registration
 - delay value, in SIP [265](#)
 - expiration value, in SIP [261](#)
 - expiration, in SIP [258](#), [261](#)
 - refresh, in SIP [258](#), [260](#)
 - regular expression, defined [432](#)
 - related documentation [xix](#)
 - Require header, ignoring, in SIP [296](#)
 - Rescue, network interface [64](#)
 - resolve route header, in SIP [295](#)
 - restart
 - unit [19](#), [23](#)
 - restart on startup, ISDN interface
 - BRI configuration [172](#)
 - PRI configuration [162](#)
 - routes, in call routing
 - call property to compare [451](#)
 - creating [450](#)
 - defined [449](#)
 - deleting [455](#)
 - destination, of call [454](#)
 - editing [450](#)
 - expression to compare [452](#)
 - mapping, apply [453](#)
 - moving [454](#)
 - signalling, of call [453](#)
 - source to compare [451](#)
 - RTCP [79](#)
 - RTP
 - enforcing symmetric [347](#)
 - RTP statistics
 - collection period [351](#)
 - end-of-connection notification [351](#)
 - end-of-period notification [352](#)
 - statistics displayed [349](#)
 - RTP, early
 - listening to [294](#)
 - rule, in events
 - deleting [41](#)
- S**
- SDP
 - direction attribute level [292](#)
 - SDP detect peer direction attribute, in SIP [290](#)
 - SDP on hold connection address, in SIP [290](#)
 - second call, service [405](#)
 - secure communication
 - secure media [345](#)
 - secure signalling [272](#)
 - select interface [182](#)
 - sending complete information, ISDN interface
 - BRI configuration [172](#)
 - PRI configuration [162](#)
 - services, ISDN
 - AOC-E support [187](#)
 - CLIP [184](#)
 - CLIR [184](#)
 - override [185](#)
 - COLP [185](#)
 - COLR [185](#)
 - override [186](#)
 - enabling [183](#)
 - Maintenance Service Call Termination [186](#)
 - MSN [188](#)
 - select interface [183](#)
 - services, managing [23](#)
 - session ID/number in Origin field, in SIP [293](#)
 - session refresh [311](#)
 - session timers [311](#)
 - signal information element, ISDN interface
 - BRI configuration [171](#)
 - PRI configuration [161](#)
 - signaling
 - PRI configuration [192](#), [224](#)
 - signalling properties, in call routing
 - 180 with SDP [466](#)
 - 183 without SDP [467](#)
 - call properties translation [468](#)
 - creating [465](#)
 - defined [465](#)
 - deleting [469](#)
 - destination host [466](#)
 - early connect [466](#)
 - early disconnect [466](#)
 - editing [465](#)
 - moving [469](#)
 - name [466](#)
 - privacy level [467](#)
 - SIP headers translation [468](#)
 - signalling protocol
 - ISDN interface
 - BRI configuration [170](#)
 - PRI configuration [159](#)
 - silence detection timeout, on FXO port [145](#)
 - SIP headers translation, in call routing
 - built from [470](#)
 - creating [469](#)
 - defined [469](#)
 - deleting [471](#)
 - editing [469](#)
 - modified header [470](#)
 - moving [471](#)
 - name [470](#)
 - SIP INFO
 - call waiting private number for [288](#)
 - SIP INFO without content answer [298](#)
 - SIP redirects, in call routing
 - creating [483](#)
 - defined [483](#)
 - deleting [484](#)

- editing [483](#)
- moving [484](#)
- SIP, setting
 - ACK branch matching [296](#)
 - allow audio and image negotiation [284](#)
 - allow less media in response [284](#)
 - allow media reactivation in answer [284](#)
 - authentication information
 - creating [268](#)
 - deleting [270](#)
 - editing [268](#)
 - moving [270](#)
 - call waiting private number for SIP INFO [288](#)
 - calling party name of the caller ID [134](#)
 - certificate trust level for TLS connections [272](#)
 - default registration value in registrations [259](#)
 - default username value [280](#)
 - direction attribute "sendonly" [285](#), [291](#)
 - direction attributes [289](#)
 - direction attributes present [289](#)
 - DNS SRV record lock [294](#)
 - early RTP, listening to [294](#)
 - error causes mapping [302](#)
 - cause to SIP [306](#)
 - SIP to cause [304](#)
 - escape pound (#) in SIP URI Username [287](#)
 - event handling [315](#)
 - expiration value in registration [261](#)
 - force DNS NAPTR in TLS [276](#)
 - forked provisional reponses behaviour [311](#)
 - gateways
 - adding [243](#)
 - auto-routing, setting for [489](#)
 - keep alive destinations [253](#)
 - messaging servers [250](#)
 - proxy servers [251](#)
 - registrar servers [249](#)
 - removing [243](#)
 - home domain proxy override [313](#)
 - Ignore OPTIONS on no usable endpoints [281](#)
 - ignore plus (+) character in username [287](#)
 - ignore Require header [296](#)
 - keep alive [252](#)
 - local ring behaviour [292](#)
 - map plus to TON International [287](#)
 - Max-Forwards header [288](#)
 - messaging subscription [317](#)
 - Offer/Answer model [280](#), [283](#), [287](#)
 - on hold SDP connection address [290](#)
 - OPTIONS Method Support [280](#)
 - outbound proxy server [248](#)
 - loose router status [253](#)
 - payload type in answer, using [363](#)
 - penalty box [301](#)
 - persistent TLS connection port [272](#)
 - PRACK [310](#)
 - proxy server [248](#)
 - quantity of RTP packets [363](#)
 - Reason header [309](#)
 - Referred-by header [309](#)
 - register home domain override [294](#)
 - registrar server [248](#)
 - registration configuration [258](#)
 - registration contact matching [282](#)
 - registration delay value [265](#)
 - registration expiration [258](#), [261](#)
 - registration refresh [258](#), [260](#)
 - reject code for unsupported SDP offer [297](#), [298](#)
 - resolve route header [295](#)
 - SDP detect peer direction attribute [290](#)
 - SDP direction attribute level [292](#)
 - secure header [280](#)
 - session ID/number in Origin field [293](#)
 - session refresh [311](#)
 - session timers [311](#)
 - SIP INFO without content answer [298](#)
 - supported DNS queries [315](#)
 - symmetric RTP, enforcing [347](#)
 - TCP/TLS connect timeout [272](#), [314](#)
 - TLS certificate validation [286](#)
 - TLS client authentication [276](#)
 - TLS persistent connections status [248](#)
 - transmission timeout [282](#)
 - transport type [271](#)
 - TCP [271](#)
 - UDP [271](#)
 - UDP source port behaviour [275](#)
 - unit registration [257](#)
 - unsupported Content-Type [299](#)
 - UPDATE [310](#)
 - user agents
 - authentication information [267](#)
 - contact domain [256](#)
 - friendly user name [255](#)
 - header, enabling to send [265](#)
 - main user name [255](#)
 - User-Agent Header
 - format [297](#)
 - voiceband data mode, call in [358](#)
- SipEp, service
 - endpoint behaviour when unregistered [262](#)
 - registration parameters [260](#)
 - user behaviour when unregistered [263](#)
- SNMP
 - partial reset [509](#), [513](#)
 - SNMPv3 privacy [509](#)
 - statistics [514](#)
 - traps, sending [509](#)
- SNMP, service
 - sending traps [509](#)
 - statistics [514](#)
- SNTP
 - client [57](#)
 - time zone, defining custom [57](#)
- Spanning Tree Protocol
 - IPv6 stateless autoconfiguration [67](#)
- special tags, in routing types values [440](#)
- special vocal features
 - IP address [129](#)
 - MAC address [129](#)
- SSH
 - accessing CLI via [10](#)
 - standards supported [xx](#)
 - Static connection type [64](#)
 - statistics
 - SNMP [514](#)
- subnets
 - managing in embedded DHCP server [115](#)
- supplementary ISDN services
 - enabling [183](#)
- syslocation, updating [61](#)
- syslog daemon

- configuring the application [38](#)
- diagnostic traces [35](#)
 - PCM capture [38](#)
- IP address [35](#)
- messages level [35](#)
- sysname, updating [61](#)

T

- T.38
 - defined [324](#)
 - enabling [340](#)
 - number of redundancy packets [340](#)
 - priority [340](#)
- TCP
 - connect timeout [272](#), [314](#)
 - transport type [271](#)
- Telnet
 - accessing CLI via [9](#)
- TFTP
 - remote server, configuring [415](#)
- time zone, configuring [57](#), [58](#)
- TLS
 - certificate trust levels for connections in [272](#)
 - certificate validation [286](#)
 - client authentication [276](#)
 - connect timeout [272](#), [314](#)
 - force DNS NAPTR in [276](#)
 - persistent connection port [272](#)
 - persistent connections status [248](#)
- tone detection custom cadence, on FXO port [146](#)
- tone detection custom frequency, on FXO port [146](#)
- TR-069 configuration [523](#)
- TR-104 configuration [524](#)
- transfer protocols
 - configuration backup image [497](#)
- transferring a call
 - attended transfer [393](#)
 - blind [392](#)
- transmission timeout, setting [282](#)
- traps, where to send in SNMP [509](#)

U

- U [72](#)
- UDP
 - source port behaviour [275](#)
 - transport type [271](#)
- unit
 - locking/unlocking endpoints [31](#)
 - restarting [19](#), [23](#)
 - shutting down behaviour [33](#)
- unlocking endpoints [31](#)
- UPDATE, support [310](#)
- Uplink, network interface [64](#)
- user
 - add [537](#)
 - delete [537](#)
 - modify [537](#)
 - unregistered, behaviour when [263](#)
- user access, setting [4](#)
 - secure password policies [5](#)
- user gain
 - input [421](#)
 - output [421](#)
- User-Agent Header

- SIP format [297](#)
- using this manual [xx](#), [xxi](#)

V

- V.21 modulation detection [365](#)
- VLAN
 - in QoS [81](#)
 - vocal features, special
 - IP address [129](#)
 - MAC address [129](#)
 - vocal unit information [129](#)
 - voice activity detection
 - G.729 [334](#)
 - voiceband data mode
 - starting a call in [358](#)

W

- wait before answering delay, on FXO port [140](#)
- wait for calle to answer, on FXO port [141](#)
- web interface
 - automatic call [387](#)
 - call completion
 - CCBS [387](#)
 - CCNR [387](#)
 - call forward
 - on busy [377](#)
 - on no answer [380](#)
 - unconditional [382](#)
 - call hold [403](#)
 - call transfer
 - attended [391](#)
 - blind [391](#)
 - call waiting [393](#)
 - conference call [397](#)
 - introduction [13](#)
 - second call [404](#)
 - using [18](#)
- Web, service
 - TCP port [13](#)

X

- X-CCD Clear Channel
 - defined [324](#)
 - enabling
 - for data transmission [337](#)
 - for voice transmission [337](#)
 - packetization time [337](#)
 - payload type [337](#)
 - priority
 - for data codecs [337](#)
 - for voice codecs [337](#)